

Australian Security Intelligence Organisation

REPORT TO PARLIAMENT 2004–2005

ISSN 0815-4562
ISBN 0-9751485-2-4

© Commonwealth of Australia

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 Government

**Australian Security
Intelligence Organisation**

Director-General of Security

Reference Number: eA952309

19 September 2005

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 2005.

The distribution of this classified Annual Report is limited. I also present to you an unclassified version for tabling in the Parliament.

Yours sincerely

Paul O'Sullivan
Director-General of Security

ASIO

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

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



CONTENTS

ASIO and its <i>Annual Report</i>	vii
Part 1: Overview	1
The Year in Review	3
Agency Overview	7
Outcome and Output Structure	9
ASIO's Funding and Performance	11
Part 2: Output Performance	13
Output 1: Security Intelligence Analysis and Advice.....	15
Output 2: Protective Security Advice	29
Output 3: Security Intelligence Investigation and Capability	35
Output 4: Foreign Intelligence.....	49
Part 3: Management and Accountability.....	51
Corporate Governance	53
Accountability and External Scrutiny	55
Accessibility to the Public.....	57
Our People	58
Information Management	64
Security of ASIO	65
Building Management.....	67
Purchasing	68
Part 4: Financial Statements.....	71
Part 5: Appendices.....	105
A. Membership of the Parliamentary Joint Committee on ASIO, ASIS & DSD	107
B. Critical Infrastructure and Nationally Vital Assets.....	108
C. Workplace Diversity Statistics	109
D. ASIO Salary Classification Structure	110
Glossary	111
Compliance Index	112
General Index	113



The Hon. Philip Ruddock, MP
Attorney-General



Paul O'Sullivan
Director-General of Security

ASIO AND ITS ANNUAL REPORT

WHAT ASIO DOES

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

ASIO's role is to advise government on security threats to Australians and Australian interests in Australia and abroad. The ASIO Act defines security as the protection of Australia and its people from:

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

ASIO also carries out Australia's responsibilities to any foreign country in relation to these matters.

ASIO has an important role in Australia's counter-terrorism arrangements, including:

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

ASIO obtains information from published sources, interviews, surveillance, human

sources, other Australian and approved international liaison partners and through the use of special powers authorised by legislation. We analyse and assess this information and produce security intelligence and advice to inform and support government decision-making. ASIO does not investigate lawful protest activity, nor does it undertake criminal investigations. ASIO officers have no power of arrest.

ASIO also collects foreign intelligence within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence.

ASIO's corporate vision, mission and values are contained in its *Corporate Plan 2002–2006*, available on www.asio.gov.au.

THIS REPORT

Section 94 of the ASIO Act requires the Director-General, as soon as practicable after 30 June, to furnish the Minister with a report on the activities of the Organisation. The Minister is required to table an unclassified copy of this report in the Parliament within 20 sitting days of receipt.

ASIO produces a classified and unclassified version of its *Annual Report*.

- The *Annual Report* to the Minister is classified. It is provided to the Attorney-General, the Prime Minister, members of the National Security Committee and the Leader of the Opposition.
- The unclassified *Report to Parliament* is an abridged version excluding classified information in accordance with Section 94 of the ASIO Act.



PART 1: OVERVIEW



THE YEAR IN REVIEW

Australian interests were again the target of terrorist attacks – in Jakarta in September 2004 and Baghdad in January 2005. Statements by al-Qai'da leaders Abu Mus'ab al-Zarqawi and Ayman al-Zawahiri and Abu Bakar Ba'asyir in Indonesia specifically named Australia as a target.

And we know from our own investigations and those of our international liaison partners that Australia has been of interest to terrorists every year for the last six years.

OUR ROLE

Within this security environment, where further attacks could well occur, ASIO's counter-terrorism focus embraces:

- the prevention of terrorist attacks in Australia and against Australian interests abroad;
- the identification of people in Australia and elsewhere involved with terrorism;
- the provision of threat assessment and protective security advice, including for Australian interests abroad and national critical infrastructure here;
- providing support to terrorism-related prosecutions; and
- contributing to Australia's counter-terrorism response capability.

The task of detecting planning for terrorist acts is difficult and it cannot be guaranteed that there will always be prior intelligence which can enable prevention. Attacks without prior warning are feasible.

SECURITY INTELLIGENCE OUTCOMES

In 2004–05 ASIO continued to build cooperative arrangements with other Australian agencies and with international liaison partners to ensure our effectiveness in protecting Australians from the threat of terrorism and in taking action against those who would do harm to Australia or our friends and allies.

Our terrorism investigations were tightly focused on identifying activity prejudicial to the security of Australia or other countries and, where appropriate, working with others to disrupt it.

We continued to identify Australians who have undertaken terrorist training or engaged in militant jihad.

We identified more people in Australia linked to extremist individuals or groups abroad and questioned 10 people under warrant. None was detained.

We worked with liaison partners in connection with Australians detained overseas on terrorism-related charges.

Further adverse security assessments were issued resulting in the cancellation or denial of Australian passports, taking the total to 32 since November 2001.

We completed 48 194 visa assessments, resulting in the denial of visas to 12 people seeking entry to Australia. Two were unauthorised arrivals.

We issued 2003 threat assessments including in connection with threats to Australian interests abroad.

We investigated leads generated by the National Security Hotline and other sources.

We conducted security checking for the re-issue of Aviation Security Identity Cards and around 8000 assessments of flight crew and people requiring access to ammonium nitrate.

We recommended the proscription of the al-Zarqawi group and the re-listing of a further 13 groups as terrorist organisations, to bring the total to 18.

OTHER INTELLIGENCE OUTCOMES

ASIO contributed to whole-of-government efforts on counter-proliferation directed at preventing the exploitation of Australian products, resources and knowledge by foreign governments or terrorist groups for weapons of mass destruction programs.

Government also provided additional resources to bolster ASIO's counter-espionage function.

ASIO continued to make a valuable contribution to the collection of foreign intelligence in Australia at the request of the Minister for Foreign Affairs or the Minister for Defence.

CAPABILITY ENHANCEMENTS

Following the watershed of the 11 September terrorist attacks government increased funding to ASIO – our budget grew from \$62.935m in 2000–01 to \$142.852m in 2004–05.

This additional funding has allowed ASIO to grow from 584 staff at 30 June 2001 to 955 at 30 June 2005, with funding committed that will see staffing grow to around 1150 in 2005–06.

In 2004–05 we:

- expanded our international liaison network by posting additional officers abroad and establishing liaison with additional security, intelligence and law enforcement agencies, taking the total to 266 agencies in 112 countries;
- increased our cooperation with regional partners, including by laying the ground-work for a joint counter-terrorism training program to build

counter-terrorism capabilities in South East Asia and the Pacific; and

- extended our training and development opportunities with a particular focus on leadership, investigative and analytical skills, language and cross-cultural training, as well as administrative and information technology training.

Legislative amendments further refined Australia's counter-terrorism legal framework, facilitated the provision of ASIO advice to Federal, State and Territory agencies concerning access to ammonium nitrate, put measures in place to protect classified information in legal proceedings, and streamlined the provisions for intercepting stored communications.

ACCOUNTABILITY AND OVERSIGHT

ASIO's activities continued to attract high levels of media, community, business and parliamentary attention. The former Director-General appeared before the Parliamentary Joint Committee on ASIO, ASIS and DSD on four occasions and before the Senate Legal and Constitutional Committee twice. He also gave three public speeches, while the Deputy Director-General gave one public address to the Security in Government Conference.

The Inspector-General of Intelligence and Security's program of monitoring and reviewing ASIO's activities did not detect any instances of illegal or improper activity by the Organisation.

LOOKING AHEAD

After 8 ½ years as Director-General Dennis Richardson left ASIO on 27 May to take up the position of Australia's Ambassador to Washington. As Director-General, Dennis Richardson led the Organisation through a time of unprecedented growth in response to challenges in the security environment.

In 2005–06 ASIO will continue to grow at a rapid rate and will face the simultaneous challenges of responding to a volatile and demanding security environment while ensuring new and recently recruited staff are properly trained and integrated into the Organisation.

ASIO will contribute to the security of the Commonwealth Games in Melbourne and will also establish a Business Liaison Unit.

From October 2005, ASIO will conduct security checking of Maritime Security Identity Card (MSIC) holders.

Paul O'Sullivan
Director-General



AGENCY OVERVIEW

ORGANISATIONAL STRUCTURE

ASIO's organisational structure was further refined in 2004 with the establishment of a Counter-Espionage Branch and a Property and Services Branch to better support the work of the Organisation.

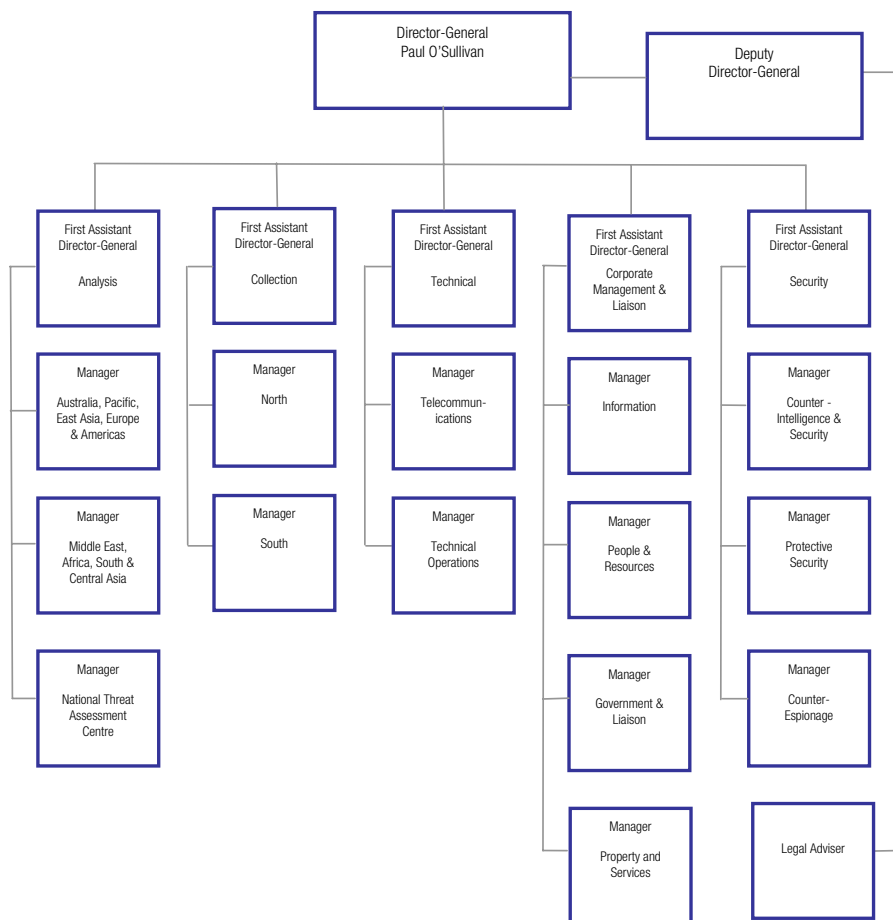


Figure 1: ASIO's organisational structure at 30 June 2005.



OUTCOME AND OUTPUT STRUCTURE

In support of the Government policy aim: ‘a secure Australia in a secure region’, ASIO contributes to the Government Outcome –

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

To achieve this ASIO delivers Output Group 1 – Security Intelligence, which includes four Outputs:

OUTPUT 1 – SECURITY INTELLIGENCE ANALYSIS AND ADVICE

- security intelligence reporting
- threat assessments
- advice on visa entry
- advice on archives issues
- advice on deterrence action
- contribution to the external policy framework

OUTPUT 2 – PROTECTIVE SECURITY ADVICE

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

OUTPUT 3 – SECURITY INTELLIGENCE INVESTIGATION AND CAPABILITY

- collection of information 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
- contribution to the external policy framework

OUTPUT 4 – FOREIGN INTELLIGENCE

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



ASIO'S FUNDING AND PERFORMANCE

Funding to ASIO in 2004–05 expressed in terms of the total price of Outputs was \$142.852m compared to \$103.023 in 2003–04.

ASIO's performance against its four Outputs is reported in detail in Part 2 of this Report.

Output	Actual	Estimated	Actual	% of total funding
	(\$m)	(\$m)	(\$m)	
	2003–04	2004–05	2004–05	
Output Group 1:				
Security Intelligence	103.022	141.802	142.852	100.0

Table 1: Price of ASIO's Outputs, 2004–05

ASIO conducts an annual survey of key Commonwealth, State and Territory clients. In 2004–05 our clients noted a general improvement in the quality and timeliness of our product with 98 percent rating it as almost always or generally useful.

Commonwealth clients commented on the high quality of our analysis and valued our unique Australian perspective, particularly in connection with threats within Australia. Some commented on the value and uniqueness of the information we obtained through our engagement with foreign liaison partners.

Police clients valued contextual information about threats to Australian interests here and abroad which informed resource deployment decisions. Several noted that local liaison arrangements generally mean police services receive the information they need before reports and threat assessments are published.

	Almost always useful (%)		Generally useful (%)		Sometimes useful (%)		Rarely useful (%)	
	03–04	04–05	03–04	04–05	03–04	04–05	03–04	04–05
Commonwealth	62.4	68	29.3	31	8.3	1	0	0
Police	66.5	57	29	40	4.5	3	0	0
Total	64.5	62.5	29.2	35.5	6.4	2	0	0

Table 2: Client Survey Results



PART 2: OUTPUT PERFORMANCE



OUTPUT 1 SECURITY INTELLIGENCE ANALYSIS AND ADVICE

ASIO contributes to the Government Outcome of 'A secure Australia in a secure region' by providing useful and timely security intelligence analysis and advice in connection with:

- threat levels in Australia and to Australian interests abroad
- foreign-influenced and local politically motivated violence
- foreign interference and espionage
- protecting critical infrastructure
- deterrence action
- border protection
- release of ASIO information

ASIO provides assessments and advice to government decision-makers and client agencies or organisations, including in the private sector, to help them manage risks and take appropriate steps to protect people, property, government business and critical infrastructure.

THREATS TO AUSTRALIAN INTERESTS

It is clear attacks on Australian interests here and abroad have been part of al-Qa'ida's strategic vision for some years. Numerous statements by Usama bin Laden, his deputy Ayman al-Zawahiri, Abu Mus'ab al-Zarqawi in Iraq and Abu Bakar Ba'asyir in Indonesia have specifically mentioned Australia. And there has been at least one aborted, disrupted or actual terrorist attack against Australian interests every year since 2000. These include:

- Jack Roche's aborted plan in 2000 to attack Israeli diplomatic interests in Australia;
- plans by Jemaah Islamiyah in Singapore in 2001 to attack Western, including Australian, interests;
- the bombing in Bali on 12 October 2002;
- activities by alleged terrorist Willy Brigitte and his associates in Australia in 2003;

- the bombing outside the Australian Embassy, Jakarta on 9 September 2004; and
- attacks on the Australian Security Detachment in Iraq in January 2005.

We must expect that Australia and its interests here and around the world will continue to be at threat from terrorist attacks, not only against diplomatic missions but also against a range of soft targets and critical infrastructure.

NATIONAL THREAT ASSESSMENT CENTRE (NTAC)

ASIO has the responsibility for assessing the likelihood and probable nature of terrorism and other acts of politically motivated violence against Australians and Australian interests here or abroad.

Since May 2004 ASIO and other agencies represented in the NTAC – the Australian Federal Police (AFP), Australian Secret Intelligence Service (ASIS), Department of Foreign Affairs and Trade (DFAT), Defence Intelligence Organisation (DIO), Department of Transport and Regional Services (DOTARS) and Office of National

We must expect that Australia and its interests here and around the world will continue to be at threat from terrorist attacks, not only against diplomatic missions but also against a range of soft targets and critical infrastructure.

NTAC product is seen as credible and as an authoritative and coordinated view of national security threats to Australian interests.

Assessments (ONA) – have adopted a whole-of-government approach to monitoring, collating and analysing all intelligence and information relating to national security threats available to the Australian government. Seconded officers have on-line access to their parent agency's communications systems and databases allowing greater connectivity and coordination between agencies and providing greater assurance that all relevant information available to the Australian government is assessed and reflected appropriately in threat assessment advice.

In 2004–05 NTAC issued 427 threat assessments in connection with the threat to Australian interests abroad.

NTAC also provides advice about the threat to foreign interests in Australia that informs risk management and resource deployment decisions of other agencies.

The Terrorist Threat Advisory Group chaired by ASIO, and consisting of representatives of Australian Intelligence Community agencies, the AFP, DFAT and the Department of the Prime Minister and Cabinet (PM&C), meets weekly or more frequently as required to ensure effective coordination between agencies in connection with threats to national security.

NTAC product is seen as credible and as an authoritative and coordinated view of national security threats to Australian interests. It is well regarded in Australia and by international partner agencies.

Subject of Assessment	2000–01	2001–02	2002–03	2003–04	2004–05
Australian interests abroad	122	176	375	559	427
Australian dignitaries	503	834	739	624	676
Diplomatic premises in Australia	77	108	55	36	24
Visiting dignitaries	79	237	674	480	228
Special events	383	147	–	–	37
Protective security	27	25	22	35	49
Demonstration notifications	100	193	149	38	56
Other threat assessments	51	66	41	245	80
TOTAL	1342	1786	2055	2017	2003

Table 3: Threat Assessments issued, 2000–01 to 2004–05

FOREIGN-INFLUENCED POLITICALLY MOTIVATED VIOLENCE

Islamic extremists in Australia generally adhere to a Salafist–Takfiri¹ interpretation of Islam which engenders a sense of hostility and isolation towards the broader Australian society and to governments in predominately Muslim countries which are considered by them to be ‘un-Islamic’. This extremist philosophy extends to support for violence against the ‘un-Islamic’ governments, against perceived Western invasion of countries and against countries they believe are attacking Islam and oppressing Muslims. This support can extend to funding and terrorist training activity as well as participation in overseas conflicts.

Most extremists are influenced by foreign events – some in Australia view the Coalition action in Iraq as an attack on all Muslims. Others believe they do not fit into Australian society or into the society of their parents. Despite a strong cultural sense of the importance of community and family, some individuals choose to lean heavily on their perceptions of conflict as a battle between Muslims and infidels. This perception engenders a sense of isolation and rejection which is difficult for moderate elements in the Australian Muslim community to counteract – and the moderates are perceived to be part of the problem by the extremists.

Extremists in Australia come from a variety of ethnic backgrounds. Some of the more extreme individuals ASIO has identified and investigated are Australian-born. Some have participated in terrorist training overseas while others have never travelled abroad.

ASIO’s terrorism investigations are aimed at identifying activity that is prejudicial to the security of Australia or to the security of other countries. There are enduring priorities for investigation that include extremist groups and individuals who are either based in Australia or have links to Australia. Developments in the international security environment can have a substantial impact on ASIO’s investigative priorities, at times with little or no notice.

JEMAAH ISLAMIAH

Jemaah Islamiyah (JI) is an extremist movement that seeks to establish a state encompassing Indonesia, Malaysia, Singapore, parts of the Philippines and Thailand. It was formed in the early 1990s by Abdullah Sungkar and, subsequently, Abu Bakar Ba’asyir. JI has become a network of individuals who share an ideology – a narrow religious interpretation, a political aim of establishing Islamic rule, a willingness to use violence – and who have trusted personal connections.

On 27 October 2002, JI was listed by the Australian government as a terrorist organisation in regulations made under the *Criminal Code Act 1995*. It was re-listed on 1 September 2004.

JI has been implicated in a series of bombings: in 2000 in Indonesia and the Philippines; the Bali bombing on 12 October 2002 that killed 202 people, including 88 Australians; the J.W. Marriott Hotel bombing on 5 August 2003 in which 12 people died; and the bomb attack outside the Australian Embassy, Jakarta on 9 September 2004. JI is also known to have undertaken planning and procurement for terrorist operations in Singapore in December 2001, including targeting of the Australian High Commission.

ASIO’s terrorism investigations are aimed at identifying activity that is prejudicial to the security of Australia or to the security of other countries.

JI has become a network of individuals who share an ideology – a narrow religious interpretation, a political aim of establishing Islamic rule, a willingness to use violence – and who have trusted personal connections.

¹ A Takfiri Muslim believes that anyone who does not share his or her strict interpretation of Islam is an infidel and can be punished. The term Salafist refers to worship in the manner of one’s ancestors (i.e. worshipping the true way as practised by the early descendents of the Prophet Mohammed).

The former leader of JI in Australia, Abdul Rahim Ayub, an Australian citizen of Indonesian origin, remains in Indonesia after leaving Australia in 2002.

Australian interests in much of South East Asia remain at threat from JI.

JI has linkages with other established extremist groups in South East Asia including the Moro Islamic Liberation Front (MILF) and the Abu Sayyaf Group (ASG) in the Philippines. JI has been involved in joint Mindanao-based training programs with these groups. It also has long-standing links to the global al-Qa'ida network.

JI in Australia

JI was first established in Australia in the early 1990s following regular visits by Abu Bakar Ba'asyir and Abdullah Sungkar. ASIO investigations into the JI presence in Australia commenced in December 2001 after authorities in Singapore discovered plans to attack Western targets, including the Australian High Commission.

The former leader of JI in Australia, Abdul Rahim Ayub, an Australian citizen of Indonesian origin, remains in Indonesia after leaving Australia in 2002.

Australian JI supporters were disrupted by the joint ASIO, AFP and State police entry and search operations in October 2002.

JI in the region

Australian interests in much of South East Asia remain at threat from JI.

ASIO continues to work with the AFP to investigate the attack on the Australian Embassy on 9 September 2004. The failure of the attack to significantly penetrate the secure area of the Embassy compound or to inflict mass Australian casualties will likely influence future JI planning for attacks against Australian interests.

In March 2005 JI leader Abu Bakar Ba'asyir was convicted of conspiracy charges in connection with the 12 October 2002 Bali bombing.

JI is also under pressure on a number of fronts as a result of:

- Indonesian and international investigations and scrutiny following the Bali, J.W. Marriott Hotel and Australian Embassy bombings;
- the introduction of counter-terrorism laws in Indonesia;
- UN listing and proscription of JI;
- the capture and sentencing of key Bali bombers; the capture and questioning of Hambali, the former JI operations commander; and the death of Fathur Rahman al-Ghozi, a key JI link to the MILF and radical Islam in the Philippines

But key terrorist planners such as Dr Azahari bin Husin and Noor Din Top remain at large. Even if they are apprehended the threat will continue because JI and its associated groups and like-minded individuals are resilient and will retain a capacity to exploit support networks to facilitate further attacks.

The December 2004 tsunami in South East Asia did not result in a fundamental re-evaluation of strategic objectives by extremists. But it is likely that in Indonesia and elsewhere in the region extremists took a tactical decision to defer operations in the short term.

OTHER EXTREMISTS IN AUSTRALIA

On 2 June 2004 Belal Khazaal was charged by the AFP with terrorism-related offences and on 10 June 2005 he was committed to stand trial.

Khazaal has twice been convicted in Lebanon for his links to planned or actual terrorist attacks and has been sentenced in absentia to a total of 15 years imprisonment. In June 2004 the Lebanese Government requested his extradition to Lebanon.

Iraq-related investigations

Two Australian citizens were detained in Iraq on terrorism charges related to anti-Coalition activities.

Brigitte investigation

Willy Brigitte was deported to France on 17 October 2003. He remains in French custody while French authorities continue to investigate his activities. Two of Brigitte's associates in Australia – Faheem Khalid Lodhi and Izhar Ul Haque – have been charged with a number of terrorism-related offences and are scheduled to stand trial in 2005–06.

AUSTRALIANS TRAINED OVERSEAS

Australians have undertaken terrorist training overseas, while other Australians are known to have attempted to travel overseas for terrorist training but were prevented from doing so by a combination of factors.

From time to time we also receive information pointing to other Australians who have received terrorist training and/or are in the service of al-Qa'ida or its affiliates overseas.

AUSTRALIANS DETAINED OVERSEAS

At the end of the reporting period a number of Australian citizens were detained overseas for terrorist or security-related reasons, including in Guantanamo Bay, Kuwait, Iraq, Lebanon, Syria and Kazakhstan. Other Australians have been released from overseas detention.

David Hicks

David Hicks was captured by the Northern Alliance in Afghanistan on or around 9 December 2001 and transferred to Guantanamo Bay in May 2002. Mr Hicks has been charged with three military commission offences. A motions hearing was held on 1–3 November 2004.

AUSTRALIANS WITH OVERSEAS TERRORIST LINKS

ASIO has pursued numerous leads about security-related activity or contacts between extremists in Australia and people abroad involved in terrorist attacks or suspected of involvement in terrorism. Two cases are set out below.

Mamdouh Habib

Mamdouh Habib was taken into custody in Pakistan by Pakistan authorities on or around 5 October 2001. He was moved to Guantanamo Bay in early May 2002 and remained there until he was released by US authorities and returned to Australia on 28 January 2005.

The Minister for Foreign Affairs cancelled Mr Habib's passport on 25 January 2005.

ASIO has pursued numerous leads about security-related activity or contacts between extremists in Australia and people abroad involved in terrorist attacks or suspected of involvement in terrorism.

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

ASIO maintains regular contact with Muslim community leaders and works closely with police services in connection with threats to the Muslim community.

Joseph Thomas

Joseph Thomas was deported to Australia from Pakistan on 4 June 2003. On 18 November 2004 Mr Thomas was arrested and charged with receiving financial support from al-Qa'ida, providing al-Qa'ida with resources or support to help it carry out a terrorist attack and having a false passport. He was granted bail on 14 February 2005 and on 1 April 2005 he was committed for trial on all charges.

EXTREMIST VISITORS TO AUSTRALIA

ASIO works closely with overseas liaison partners and with DIMIA and Customs to identify extremists attempting to travel to or enter Australia.

OTHER INVESTIGATIONS

ASIO contributed to the investigation of several kidnappings and claimed kidnappings of Australian citizens in Iraq, including the kidnapping of Douglas Wood.

Mr Wood was kidnapped on 30 April 2005 by a group calling itself the Shura Council of the Mujahideen. The hostage takers demanded the Australian Government withdraw its troops from Iraq. Mr Wood had been working in Iraq as a Baghdad-based contractor assisting in the rebuilding effort. Mr Wood was rescued on 15 June 2005 by US and Iraqi forces.

THREATS TO THE JEWISH COMMUNITY

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

THREATS TO THE MUSLIM COMMUNITY

ASIO maintains regular contact with Muslim community leaders and works closely with police services in connection with threats to the Muslim community.

COMMUNAL VIOLENCE

In the lead-up to the elections in Iraq community tensions increased in Sydney, particularly in the Auburn area. The tensions extended beyond the Australian-Iraqi community and involved individuals from a range of Middle Eastern origins. The tensions escalated some days prior to the elections with a series of verbal exchanges and fisticuffs between Sunni and Shia community members and a shooting incident on 30 January 2005 that resulted in injuries.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR TERRORISM

ASIO contributed to the international effort to assess the status of al-Qa'ida's chemical and biological weapons program and to disrupt it.

PROSCRIPTION

The process for proscription of a terrorist group in Australia under the *Criminal Code Act 1995* Subsection 102.1(2) requires that before the Governor-General makes a regulation specifying an organisation as a terrorist organisation, the Minister must be satisfied on reasonable grounds that:

- the organisation is directly or indirectly engaged in preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not the terrorist act has occurred or will occur).

ASIO identifies organisations for possible proscription and provides a 'statement of reasons' to the Attorney-General for proscribing an organisation.

ASIO considers a range of factors in assessing a group for possible proscription, including engagement in terrorism, ideology and links to other terrorist groups or networks, links to Australia, the threat to Australian interests, proscription by the United Nations or like-minded countries, and engagement in peace or mediation processes. The statement is based on publicly releasable material which is verified against all holdings, including intelligence and other classified reporting and open source information.

In 2004–05 ASIO recommended the proscription of Tanzim Qa'ida al-Jihad fi Bilad al-Rafidayn (al-Qa'ida of Jihad in the Land of the Two Rivers, also known as the al-Zarqawi network). The listing of this group on 2 March 2005 brought to 18 the total number of terrorist organisations proscribed by the Australian Government.

The Government also re-listed 13 organisations as terrorist organisations during the reporting period, including the Abu Sayyaf Group, Armed Islamic Group, Jamiat ul-Ansar, Salafist Group for Call and Combat, al-Qa'ida, Jemaah Islamiyah, Egyptian Islamic Jihad, Lashkar-e Jhangvi, Islamic Movement of Uzbekistan, Jaish-e-Mohammad, Asbat al-Ansar, Ansar al-Islam and the Islamic Army of Aden.

PROSECUTIONS AND APPEALS

Four prosecutions for terrorist-related offences were underway at the end of the reporting period – Joseph 'Jack' Thomas, Belal Khazaal, Faheem Khalid Lodhi and Izhar Ul-Haque.

ASIO is also required to respond to immigration appeals and challenges through the courts. In the case of Iranian cleric Mansour Leghaei, ASIO has been responding to successive legal challenges to a prejudicial security assessment since 2002.

In each case, the Australian Government Solicitor and/or external counsel has been briefed to represent the interests of ASIO.

The Commonwealth Director of Public Prosecutions continued to progress the prosecution of Faheem Lodhi, who was charged prior to the commencement of the reporting year with offences arising from the alleged provision of false or misleading information to ASIO under a questioning warrant, which is an offence under subsection 34G(5) of the ASIO Act. During the reporting year, one other person, Abdul Rakib Hasan, was served with a court attendance notice requiring him to appear in court in relation to similar alleged offences.

PASSPORT CANCELLATIONS

In 2004–05 the Minister for Foreign Affairs cancelled or refused to issue Australian passports following the issue by ASIO of adverse security assessments. The Minister also gave approval to seize the foreign passports of Australians with dual citizenship after ASIO issued adverse security assessments.

Since November 2001, 33 Australians have had their passports cancelled or denied after ASIO issued adverse security assessments. In one case, ASIO subsequently withdrew its assessment. At the end of the reporting period, eight persons were exercising their right of review of the assessment by the Administrative Appeals Tribunal.

ASIO's counter-proliferation effort in 2004–05 concentrated on identifying, investigating and recommending actions to prevent the exploitation of Australian products, resources or knowledge by foreign governments and non-state actors (such as terrorist groups) to assist in the development of weapons of mass destruction (WMD).

LOCAL POLITICALLY MOTIVATED VIOLENCE

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

Violent protest tactics, including against police, over several days outside the Baxter Detention Centre over Easter 2005 resulted in the arrest of 18 activists.

Several members of the Australian Nationalist Workers' Union (ANWU) in Perth, including leader Jack Van Tongeren, were arrested and charged with criminal offences under Western Australia State legislation following their racist graffiti campaign.

FOREIGN INTERFERENCE AND ESPIONAGE

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

PROLIFERATION

ASIO's counter-proliferation effort in 2004–05 concentrated on identifying, investigating and recommending actions to prevent the exploitation of Australian products, resources or knowledge by foreign governments and non-state actors (such as terrorist groups) to assist in the development of weapons of mass destruction (WMD).

PROTECTING CRITICAL INFRASTRUCTURE

Critical infrastructure encompasses physical facilities, supply chains, information technologies and communication networks. If these were destroyed, degraded or rendered unavailable for an extended period, it would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security.

Most of Australia's critical infrastructure is owned or operated by the private sector, with the remainder owned or operated by the Australian or State and Territory governments. Some infrastructure is classed as 'nationally vital', while other assets, of less national significance, are nonetheless vital to the jurisdictions in which they are located. Appendix B shows the definitions used in determining the level of criticality of each asset.

Protection of critical infrastructure is included in the National Counter-Terrorism Plan. ASIO's role is to assess and advise government and jurisdictions and (where appropriate) the private sector on security threats to critical infrastructure. The current security environment requires cooperation and coordination across government and private sector boundaries for effective critical infrastructure protection. ASIO has participated in inter-agency coordination activities and liaised with the private sector. ASIO's work has assisted governments and critical infrastructure owners and operators to understand the security environment and thereby to enhance protective security in critical infrastructure sectors.

NATIONAL CRITICAL INFRASTRUCTURE DATABASE

The database provides a consolidated listing of Australia's critical infrastructure at both national and jurisdictional levels. Work on the database continued, including liaison with jurisdictions to ensure data currency and regular review of data holdings. ASIO hosted a workshop to help jurisdictions develop a nationally consistent methodology for analysing and assessing their critical infrastructure. Other database-related activities included participation on the Australian Government Spatial Information for National Security interdepartmental committee and the Attorney-General's Department-sponsored critical infrastructure protection Modelling Analysis Project. These two projects are intended to facilitate use of geospatial information within government and to further develop understanding of critical infrastructure interdependencies.

NATIONALLY VITAL CRITICAL INFRASTRUCTURE THREAT ASSESSMENTS

These assess the terrorist threat to each of Australia's 'nationally vital' assets identified in the National Critical Infrastructure Database.

Twenty-three such assessments have been issued. They broadly canvass security and potential sources of vulnerability in the context of assessing the terrorist threat to each asset. Preparation of each assessment involves close liaison with relevant Federal, State and Territory government agencies and police services and the private sector. Information contained within them has been or will be shared with government and private sector asset owners and operators to facilitate protective security risk reviews, the development of security plans, emergency response and business continuity plans, and the adoption of measures recommended in the *National Guidelines for Protecting Critical Infrastructure from*

ASIO's work has assisted governments and critical infrastructure owners and operators to understand the security environment and thereby to enhance protective security in critical infrastructure sectors.

Terrorism, published by the Attorney-General's Department.

ASIO is also a member of the Information Infrastructure Protection Group and the Electronic Security Coordination Group.

ASIO provided security context and threat assessment briefings to Federal, State and Territory government agencies and the private sector.

SECTORAL THREAT ASSESSMENTS

ASIO produces assessments of the terrorist threat to Australia's critical infrastructure sectors (see Appendix B). These are a variation of ASIO's traditional threat assessments, addressing not only the intent and capability of threat sources but also potential weaknesses that could be exploited to cause harm. In preparing these threat assessments ASIO consults widely with government at national and jurisdictional levels, and with industry. Sectoral threat assessments are a key element in Australia's coordinated protective security arrangements. They underpin critical infrastructure protection activities undertaken by governments, and assist formulation of risk context analysis used by jurisdictions and the private sector. They address issues relevant to a wide range of assets which, while important, do not fall into the 'nationally vital' category.

NATIONAL INFORMATION INFRASTRUCTURE (NII)

NII includes telecommunications and information networks supporting banking and finance, transport, supply chains, energy and utilities, information services and critical government communications including defence and emergency services. The protection of the NII is essential given the increasing reliance and dependence by society on trusted information networks and systems. ASIO participates in the multi-agency approach to the security of the NII, the aim of which is to create a trusted and secure electronic operating environment for both government and private sectors.

ASIO continues to monitor the threat to the NII and provides advice to government on the threat to infrastructure from potential sources of computer network attack.

INFORMATION SHARING

In recognition of the need to share information with owners and operators of critical infrastructure so they can better address the terrorist threat, ASIO provided security context and threat assessment briefings to Federal, State and Territory government agencies and the private sector. ASIO is a member of the Critical Infrastructure Advisory Council, the lead committee in the Trusted Information Sharing Network coordinated by the Attorney-General's Department. ASIO attended meetings of the various critical infrastructure Industry Assurance Advisory Groups. This interaction gives ASIO officers direct access to industry experts and provides owners and operators of critical infrastructure a means to pass security concerns to ASIO.

ASIO continues to participate in international forums concerned with critical infrastructure protection and threats from computer network attack operations.

Business Liaison Unit

At the end of the reporting period recruitment was underway to establish the Business Liaison Unit. The Unit will provide a focal point for business contact with ASIO. It will assist in ensuring that owners and operators of critical infrastructure and other relevant members of the business community can access timely information on matters affecting the security of assets and staff for which they are responsible.

BORDER SECURITY

ASIO is the principal source of advice to DIMIA on the entry to Australia of people of national security significance. ASIO continued to work with DIMIA, Customs, DOTARS and DFAT to improve border control policies and arrangements to reduce the likelihood of terrorists and other individuals of security concern gaining entry to Australia. Risk-management principles are applied to the process.

The number of security assessments required for visa applicants increased markedly in 2004–05.

In 2004–05 a review of maritime security identified a gap in Australia’s capacity to conduct security checking of shipping crew. Cross-portfolio work on a range of proposals, including the introduction of a visa regime for shipping crew, was undertaken.

MOVEMENT ALERT LIST (MAL)

ASIO lists identities of security concern in the DIMIA-managed MAL. The number of ASIO entries in MAL grew again this year with a consequent increase in the number of MAL alerts referred to ASIO for

assessment. Each referral is treated as a separate security assessment. Some can be resolved quickly, while others require more comprehensive investigation.

UNAUTHORISED ARRIVALS

Unauthorised arrivals who are granted three-year Temporary Protection Visas by DIMIA are required to undergo a new security assessment prior to being granted a Further Protection Visa. In 2004–05, 5046 unauthorised arrivals were referred to ASIO and 4223 assessments were provided. This is an increase of over 200 percent on the previous year and resulted in some delays in the provision of assessments to DIMIA.

ASIO managed the caseload according to priorities set by DIMIA. Complaints about delays in the process were received by the Inspector-General of Intelligence and Security (see page 56).

PREJUDICIAL VISA SECURITY ASSESSMENTS

In 2004–05 ASIO recommended against the entry of 12 individuals assessed to be a threat to security. This included two prejudicial security assessments on unauthorised arrivals.

In 2004–05, 5046 unauthorised arrivals were referred to ASIO and 4223 assessments were provided. This is an increase of over 200 percent on the previous year and resulted in some delays in the provision of assessments to DIMIA.

	2000–01	2001–02	2002–03	2003–04	2004–05
Temporary	26 527	29 437	27 534	30 841	39 015 ¹
Permanent	7 392	9 584	12 355	13 881	13 402
Total	33 919	39 021	39 889	44 722	52 417

¹Unlike previous years the figure for 2004–05 includes visa assessments for unauthorised arrivals (4223).

Table 4: Visa security assessments, 2000–01 to 2004–05

INITIATIVES

In 2004–05 ASIO worked even more closely with DIMIA at the operational, policy and management levels to enhance effectiveness and efficiency as data volumes and workloads for both organisations continued to increase. This included:

- regular high-level management meetings;
- trialling automated MAL referrals to ASIO; and
- ASIO input to DIMIA's review of MAL.

CHALLENGES

The key challenges for ASIO remain:

- managing the growth in data volumes;
- reducing assessment times; and
- improving the data exchange between ASIO and DIMIA.

An extended hours border security capability from July 2005 and improvement in electronic connectivity with DIMIA planned for 2006 will allow ASIO to reduce assessment times in some instances where the checking is less complex.

	2000–01	2001–02	2002–03	2003–04	2004–05
Prejudicial assessments	5	5	8 ¹	3	12 ²

¹ Seven plus one diplomat expelled on advice from ASIO.

² Includes two prejudicial assessments on unauthorised arrivals.

Table 5: Prejudicial assessments

RELEASE OF ASIO'S RECORDS

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

ACCESS TO ARCHIVAL RECORDS

Members of the public can apply to the National Archives of Australia for access to ASIO records that are at least 30 years old (described as the open access period). When National Archives does not already hold records on the subject, it passes the applications to ASIO. We locate and assess relevant records and provide advice to 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. We balance the commitment to release information into the public domain with the need to protect national security.

In rare cases National Archives will inform ASIO of the identity of the applicant to facilitate our contact with them to identify relevant records or agree on priorities. ASIO does not investigate or open files on applicants or researchers.

During the reporting period, coinciding with the 50th anniversary of the Petrov defection, the sister of Mrs Petrov donated to the Australian Government via ASIO the original letters from Prime Minister Menzies to the Petrovs granting them asylum in Australia. We passed these historically significant letters to National Archives.

Performance

In 2004–05, 82 percent of applications were finalised within 90 days against a benchmark of 80 percent. This was despite the impact of several large requests made during the current and previous reporting periods and one application that covered a broad range of legislative issues and required extensive research and careful assessment.

Trends

We received applications for access to 326 separate items or subjects in 2004–05, compared to 307 in 2003–04.

With the agreement of the Inspector-General of Intelligence and Security, ASIO gives priority to requests from people seeking records on themselves or members of their family. Some 68 family requests were due for completion in 2004–05 (compared to 121 in the previous year). Eighty-three percent of these were completed within 90 days (compared to 94.75 percent last year), against a benchmark of 100 percent. This result reflects the large size of many of the requests which meant they could not be finished within the 90 days.

As in previous years, many requests related to ASIO's records on war criminals; anti-apartheid and Vietnam moratoriums/public order demonstrations; 'ASIO and the New Left'; Greek organisations, their members and related affiliations including the Communist Party of Australia; 'right-wing' activists; the 'Murphy raid' on ASIO; and the Petrovs.

Several large requests from individual/non-family researchers were also received and special arrangements were made to accommodate them. Similar requests from researchers lodged last year continued to be processed during 2004–05.

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.

The total number of folios (pages) examined was 41 181 compared to 32 708 in 2003–04.

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

Appeals

Applicants who are dissatisfied with exemptions claimed by ASIO can request an internal reconsideration of the decision. This process is undertaken in conjunction with 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. No appeals were lodged in the reporting period.

In 2004–05 there were five internal reconsiderations. Three applicants sought reviews of substantive exemptions. One case was resolved and the other two required referrals to overseas and Australian liaison partners. The fourth applicant did not accept that no records could be found but further checks of our databases confirmed our original advice. In the final case, following discussions with National Archives, it was determined there were no grounds for the applicant to appeal the decision.

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

The total number of folios (pages) examined was 41 181 compared to 32 708 in 2003–04

OUTPUT 2 PROTECTIVE SECURITY ADVICE

ASIO contributes to the Government Outcome of ‘A secure Australia in a secure region’ by providing useful and timely protective security advice in connection with:

- personnel security
- physical security, including protective security and risk management
- security equipment standards
- electronic and audio surveillance counter-measures
- the external policy framework

SECURITY IN GOVERNMENT

INTER-AGENCY SECURITY FORUM

ASIO continues to manage the Inter-Agency Security Forum (IASF) which was formed after the Government endorsed the recommendations of the *Inquiry into Security Issues* by the Inspector-General of Intelligence and Security in 2000. The IASF has representatives from all member agencies of the Secretaries Committee on National Security (SCNS) and the National Security Committee of Cabinet (NSC) – that is, Australian Intelligence Community agencies, PM&C, Defence, DFAT, Attorney-General’s Department, Treasury and DIMIA. The Protective Security Coordination Centre (PSCC) is also represented on the IASF, ensuring relevant initiatives are considered for application across the rest of government.

The IASF drives the development and implementation of best-practice security policies and procedures across the AIC and related policy departments. In 2004–05, the IASF implemented initiatives including:

- bulletins raising awareness of security issues associated with laptop computers, mobile phones and personal digital assistants;
- audit procedures for safe-hand and courier delivery services; and

- development of Australian standards and procedures for the destruction of classified computer media.

ASIO’s Deputy Director-General is the Chair of the IASF and ASIO officers chair the IASF’s four permanent working groups.

Security Status Report

Each year IASF agencies submit a security status report to PM&C for consideration by SCNS and NSC. ASIO’s (classified) Security Status Report was completed in October 2004.

POLYGRAPH TRIAL

ASIO presented its report on the polygraph trial to SCNS in August 2005.

AUSTRALIAN GOVERNMENT CONTACT REPORTING SCHEME

People working for or on behalf of the Commonwealth, both within and outside Australia, are required under the Australian Government Contact Reporting Scheme to report suspicious, unusual, persistent or on-going contact with foreign government officials, or people who have direct links to a foreign government agency. The aim of the scheme is to help identify potential threats to Australia’s

The IASF drives the development and implementation of best-practice security policies and procedures across the AIC and related policy departments.

ASIO presented its report on the polygraph trial to SCNS in August 2005.

ASIO's counter-terrorism security checking, previously limited to Aviation Security Identity Card (ASIC) holders, broadened during the reporting period, with the addition of programs of security checks for pilots, trainee pilots and people requiring access to ammonium nitrate.

ASIO completed more than 96 percent of counter-terrorism checks in five days and 99.9 percent in ten days.

national security by identifying attempts to seek information of intelligence value through unauthorised means.

During 2004–05 ASIO appointed additional staff to manage and promote the scheme.

PERSONNEL SECURITY

ASIO security assessments, whether for access to national security classified information or areas or for counter-terrorism purposes, are governed by the ASIO Act. These assessments advise whether anything in a candidate's background or activities is a cause for security concern. ASIO does not assess general suitability for the access proposed; that is the responsibility of the requesting agency. Security assessments are usually based on material provided by the submitting agency, but may also require ASIO to conduct interviews or other enquiries to resolve security issues.

ASIO either advises that it does not recommend against a security clearance or it issues 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 be relevant to decision-making. Qualified assessments also provide appropriate information to help agencies minimise the potential security risk.

The decision to grant or deny the proposed access rests with the head of the relevant agency. Candidates are informed if ASIO issues a qualified or adverse assessment.

COUNTER-TERRORISM CHECKING

ASIO's counter-terrorism security checking, previously limited to Aviation Security Identity Card (ASIC) holders, broadened during the reporting period with the addition of programs of security checks for pilots, trainee pilots and people requiring access to ammonium nitrate. The increased range of security checks is part of the government's counter-terrorism policies and programs. Assessments are passed to the AFP which advises requesting bodies of the results.

Counter-terrorism security checks are limited to inquiring whether the subject has any known links to terrorism and are completed more quickly than assessments for access to classified information. ASIO completed more than 96 percent of counter-terrorism checks in five days and 99.9 percent in ten days.

Since November 2003 ASIO has security checked individuals requiring access to security-controlled areas at Australian airports. Reissue of all existing ASICs was completed in August 2004 with on-going checking of new ASIC holders. From 1 July 2005 ASIO has also been security checking pilots and trainee pilots.

ASIO also worked with the Department of Transport and Regional Services on the introduction of Maritime Security Identity Cards (MSIC) for access to security-controlled areas in the maritime sector. MSIC checking will commence in October 2005. ASIO is improving its IT capabilities to meet this additional requirement.

The Council of Australian Government's review of hazardous materials identified a requirement for controlled access to ammonium nitrate because of its ready availability and potential use as an explosive. States and Territories are introducing licensing regimes requiring police and ASIO security checks for access to ammonium nitrate and other explosives.

The ASIO Act was amended late in 2004 to cover ammonium nitrate counter-terrorism checking and will take into account any future checking programs. In

2004–05, 1634 of these checks were completed with States and Territories aiming to have all licences issued by the end of 2005.

	2003–04	2004–05
ASICs	58 147	31 762
Flight Crew	-	6 160
Ammonium Nitrate	-	1 634
Total	58 147	39 556

Table 6: Counter-terrorism assessments

In conjunction with Victoria Police, ASIO has developed an accreditation security checking program for the March 2006 Melbourne Commonwealth Games. This program will check about 55 000 volunteers, participants and contractors. The Attorney-General has declared the Commonwealth Games a special event so that ASIO can pass the results of security

checking to Victoria Police – the ASIO Act otherwise prevents passing of security assessments to State authorities.

No qualified or adverse security assessments were issued in relation to counter-terrorism security checking during 2004–05.

ACCESS CHECKING

There was a two percent increase in access assessments in 2004–05.

Benchmarks were not met due to the continued high level of requests, the decommissioning of a work management system and its replacement with different software and staffing changes. A backlog of requests was reduced in the second half of the period.

APPEALS

Individuals have a right of appeal to the AAT in respect of an adverse or qualified ASIO security assessment. There were no appeals lodged or outstanding in 2004–05.

No qualified or adverse security assessments were issued in relation to counter-terrorism security checking during 2004–05.

Level of access	2000–01	2001–02	2002–03	2003–04	2004–05
Confidential	969	1 431	1 542	1 611	1 951
Secret	5 803	6 595	7 618	9 577	9 372
Top Secret	4 335	4 329	5 112	5 018	5 694
Total	11 107	12 355	14 272	16 206	17 017

Table 7: Access assessments – annual workloads

	2000–01	2001–02	2002–03	2003–04	2004–05
Qualified assessments	10	6	3	2	1
Adverse assessments	2	3	2	0	0
Total	12	9	5	2	1

Table 8: Adverse and qualified personnel security assessments

Our client base continued to expand during the reporting period as more government and private sector organisations sought protective security advice.

Ten Top Secret facilities were certified during 2004–05 and a further 27 facilities were inspected and provided with reports detailing physical security improvements required to meet minimum standards.

PROTECTIVE SECURITY

ASIO provides protective security advice to government departments and agencies. With the approval of the Attorney-General, we provide protective security advice to non-Commonwealth agencies, including State and Territory agencies and owners of critical infrastructure. All protective security advice is provided on a cost-recovery basis.

Our client base continued to expand during the reporting period as more government and private sector organisations sought protective security advice.

During 2004–05 ASIO continued to provide protective security advice on the Defence Headquarters Joint Operations Command at Bungendore. ASIO has taken the lead in providing and coordinating advice to this project on all aspects of security, including the finalisation of the project output specification used by the tenderers to design and cost the facility over its proposed 30 year life. ASIO will continue its coordination and advising role through to project completion in 2007.

In 2004–05, \$901 053 was recovered from clients, including the AFP, Department of Finance and Administration and the Defence Imagery and Geospatial Organisation. This figure remained largely unchanged from last year while significant growth in ASIO-commissioned protective security advice occurred.

Notional charges for work conducted for ASIO totalled \$540 421. This figure, significantly higher than 2003–04 (\$313 179), reflects the increased time spent on ASIO projects this year.

TOP SECRET CERTIFICATIONS

ASIO is responsible for inspecting and certifying sites to hold Top Secret information to ensure they meet required standards. Re-certification of facilities is required every five years or following significant structural changes.

Ten Top Secret facilities were certified during 2004–05 and a further 27 facilities were inspected and provided with reports detailing physical security improvements required to meet minimum standards.

ACCREDITATION AND TRAINING

We continued to accredit security practitioners on behalf of the Interdepartmental Security Construction and Equipment Committee (SCEC) and provided protective security and risk management training.

- Fifty-two locksmiths were accredited to install and maintain combination and secure area door locks.
- Two consultants received accreditation as 'SCEC approved' security consultants.
- We delivered presentations on eleven protective security and five physical security training courses facilitated by the Protective Security Coordination Centre.
- A further four waste destruction facilities were endorsed, taking the total number of endorsed facilities to ten.
- One classified information storage facility was inspected and accredited during the period with another facility's accreditation likely to be finalised in 2005. This will take the total number of accredited facilities to five.

SECURITY EQUIPMENT

On behalf of the SCEC, ASIO evaluates security products for use by government and inclusion in the Security Equipment Catalogue. Forty-nine security products were evaluated in 2004–05.

A revised *Security Equipment Catalogue* was published in July 2004. An updated version will be published in early 2006. It is available for purchase by government organisations and contractors conducting work on their behalf. An order form is available at www.asio.gov.au.

TECHNICAL SURVEILLANCE COUNTER-MEASURES (TSCM)

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

We also conducted sweeps for the Department of Defence. The majority of this activity was in relation to certification of Top Secret Defence Sites.

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

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



OUTPUT 3 SECURITY INTELLIGENCE INVESTIGATION AND CAPABILITY

To meet its responsibilities under legislation, ASIO must develop and maintain specialised capabilities within a challenging security environment.

Output 3 is delivered through a range of integrated activities, conducted within a strict legislative and accountability framework, that collectively make up ASIO's security intelligence collection and counter-terrorism capability. These include:

- human source intelligence collection
- covert surveillance
- special powers operations
- technical research and development
- monitoring and alert functions
- cooperation with Australian agencies
- cooperation with international liaison partners

Output 3 contributed to the Government Outcome of 'A secure Australia in a secure region' 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.

OPERATING ENVIRONMENT

The business of a security intelligence agency is fundamentally one of collecting and analysing information.

ASIO's task is to make the best possible assessment of a threat to security based on the information available at the time. In assessing the threat, judgements need to be made about the credibility and reliability of that information. ASIO needs to be in the best position to judge credibility and reliability, to resolve ambiguities and to provide well-founded advice that is as specific as possible.

ASIO can call on technical capabilities, surveillance resources, special powers under warrant, human sources and its analytical resources to identify, investigate and assess a threat and provide advice to government.

Notwithstanding these capabilities, the security environment remains challenging.

*... the security
environment remains
challenging.*

LEGISLATIVE FRAMEWORK

The ASIO Act was twice amended during 2004–05, first by the passing of the *Anti-terrorism Act (No.3) 2004* and second by the passing of the *Australian Security Intelligence Organisation Amendment Act 2004*.

ANTI-TERRORISM ACT (NO.3) 2004

The Anti-terrorism Act (No.3) 2004 received royal assent on 16 August 2004. The part of the Act affecting the ASIO Act (Schedule 2) commenced on 13 September 2004. It amended the ASIO Act by creating a power for ASIO to require a person to surrender their passports (both Australian and foreign) where the Director-General has requested the Attorney-General to consent to the issue of a questioning warrant but the warrant has not yet been issued by an issuing authority (new section 34JBA).

Therefore, the power is directed at an emergency situation where the Director-General has requested the Attorney-General to consent to the issuing of a questioning warrant and receives information that the subject of the warrant may attempt to leave the country before the Attorney-General decides whether to consent to issuing the warrant or the warrant can be issued by an issuing authority.

The Act also created new offences under the ASIO Act for failure to comply with a demand for the surrender of a person's passport and for leaving Australia when a person is subject to a request for consent to apply for a questioning warrant.

Once a warrant is issued, other provisions of the ASIO Act require a person to surrender any passport in the person's possession.

ASIO is yet to have an operational need to exercise the powers. However, the amendments improve Australia's counter-terrorism legal framework.

The Anti-terrorism Act (No.3) 2004 also amended the *Passports Act 1938*, to provide a power for the responsible Minister to order the surrender of a person's foreign travel documents (new section 16). The Minister may make such an order where, among other grounds, a competent authority suspects on reasonable grounds that unless the person's foreign travel documents are surrendered, the person would be likely to engage in conduct that might prejudice the security of Australia or a foreign country.

Prior to the amendment the Minister for Foreign Affairs could cancel a person's Australian passport under section 8 of the *Passports Act 1938* on the basis of an adverse security assessment furnished to the Minister by ASIO under section 37 of the ASIO Act. An effect of this amendment is to enable the Minister also to order the surrender of a person's foreign travel documents on the basis of an adverse security assessment. A security assessment furnished in this circumstance would contain a request that the Minister order the surrender of the person's foreign travel documents ('adverse security assessment' and 'prescribed administrative action' are defined in section 35 of the ASIO Act).

AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION AMENDMENT ACT 2004

The Australian Security Intelligence Organisation Amendment Act 2004 commenced on 14 December 2004. It amended the ASIO Act to expand and clarify ASIO's ability to furnish security assessments by expanding the definition of 'prescribed administrative action' in section 35 of the ASIO Act.

ASIO can provide security assessments to Commonwealth agencies in relation to 'prescribed administrative action' that might be taken by those agencies. Previously, 'prescribed administrative action' was defined as action that relates to access by a person to 'any information

The amendment enables ASIO to provide security assessments to enable the Commonwealth, States and Territories to prevent persons who are a security risk from being able to access ammonium nitrate.

or place' which is controlled or limited on security grounds.

The definition was amended to include action that relates to or affects a person's ability to perform an activity in relation to, or involving, a thing (other than information or place) if that access is controlled or limited on security grounds.

The need for the amendment arose in the context of the regulation of access to ammonium nitrate, under regimes being put in place by the Commonwealth and the States and Territories, as agreed by the Council of Australian Governments. The amendment enables ASIO to provide security assessments to enable the Commonwealth, States and Territories to prevent persons who are a security risk from being able to access ammonium nitrate.

While the amendment was made for the specific purpose of enabling regulation of access to ammonium nitrate on security grounds, it will enable ASIO to provide security assessments in the event that access to other substances is regulated on security grounds.

OTHER LEGISLATIVE CHANGES

Other legislative changes to impact or potentially impact upon ASIO in 2004–05 were the *National Security Information (Criminal Proceedings) Act 2004*, the *National Security Information (Criminal Proceedings) Amendment (Application) Act 2005* and the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004*.

The *National Security Information (Criminal Proceedings) Act 2004* received royal assent on 14 December 2004. The main provisions of the Act commenced on 11 January 2005. The Act strengthens the laws for protecting information that, if disclosed during the course of Federal criminal proceedings, would be likely to prejudice Australia's national security.

The Act initially applied only to Federal criminal proceedings instituted after the

date of assent. However, the *National Security Information (Criminal Proceedings) Amendment (Application) Act 2005* (which commenced on 21 March 2005) amended the Act to ensure that it can be applied to proceedings, even if the proceedings began before 11 January 2005, the day on which the main provisions of the Act commenced.

The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* amended the *Telecommunications (Interception) Act 1979* to change the way in which it deals with access to stored communications. Under the *Telecommunications (Interception) Act 1979*, it is generally prohibited to intercept without a warrant a communication passing over a telecommunications system, such as a telephone call or an e-mail message, without the knowledge of the person making the communication.

The amendment made by the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004*, which commenced on 15 December 2004, excludes the interception of stored communications from that general prohibition. 'Stored communication' means a communication that is stored on equipment or any other thing but not a Voice Over Internet Protocol (VOIP) communication or any other communication that is stored on a highly transitory basis and as an integral function of the technology used in its transmission.

The practical effect of the amendment is that it is no longer necessary to obtain a warrant under the *Telecommunications (Interception) Act 1979*, or to rely on another exception to the general prohibition against interception, in order to intercept a stored communication. A stored communication may be intercepted by a person having lawful access to the communication or to the equipment on which it is stored. A telecommunications interception warrant is still required in order to intercept communications that are in transit over a telecommunications system when intercepted.

The amendment will cease to have effect on 15 December 2005, 12 months after it commenced, during which time there is to be a review of access to electronic communications under the *Telecommunications (Interception) Act 1979*.

COUNTER-TERRORISM RESPONSE CAPABILITIES

ASIO contributes to Australia's counter-terrorism response capability. As outlined in the *Report of the Inquiry into Australian Intelligence Agencies*, the ASIO Act makes it clear ASIO's responsibility is to protect Australia and its people and property against threats to their security from within or outside Australia.

In 2004–05 ASIO continued to contribute to whole-of-government counter-terrorism policy coordination and national counter-terrorism arrangements.

ASIO has strengthened its links with the Australian Intelligence Community (AIC) and other policy and operational agencies at all levels to ensure that comprehensive intelligence assessments and advice inform the government's consideration of security policy.

During the reporting period ASIO was a member of numerous working groups. These working groups, covering a broad range of areas including critical infrastructure, border security, transport security and science and technology, were responsible for progressing work on behalf of the National Counter-Terrorism Committee and the Australian Government Counter-Terrorism Policy Committee.

SUPPORT TO NATIONAL COUNTER-TERRORISM COMMITTEE (NCTC)

As a member of the NCTC, ASIO participated in the coordination of Australia's national counter-terrorism arrangements by contributing to strategic

policy advice, building an effective nationwide counter-terrorism capability and ensuring effective arrangements are in place for sharing relevant intelligence and information between agencies and jurisdictions.

While the Australian government relies on high-quality intelligence to prevent and disrupt attacks against Australians or Australian interests at home or abroad, it is important to ensure ASIO's counter-terrorism response capabilities are ready to deploy in response to any terrorist incident.

ASIO has well-practised capabilities ready to coordinate quickly and efficiently security intelligence requirements in response to an act of terrorism. Under the National Counter-Terrorism Plan, ASIO has responsibility for the National Intelligence Group (NIG), which includes members of other relevant agencies. The NIG, an operations centre located in ASIO Central Office, coordinates and disseminates intelligence to support policymakers and operational commanders. ASIO also supports police operational commanders by providing staff to the Joint Intelligence Group (JIG) and Police Forward Command Posts (PFCP), both located at or near the scene of an incident.

To ensure ASIO remains prepared to respond to a terrorist incident it participates in the NCTC exercise and training program. This program brings together Federal, State and Territory security, law enforcement, intelligence and emergency management agencies in exercises designed to test, strengthen and maintain effective working relationships.

During the reporting period ASIO was one of several agencies that helped plan and conduct three NCTC training exercises. Two exercises were conducted in Victoria as part of preparations for the 2006 Commonwealth Games and the other was in the Northern Territory.

ASIO was one of several agencies that helped plan and conduct three NCTC training exercises.

OTHER COMMITTEES

ASIO is a member of the Australian Government Counter-Terrorism Policy Committee (AGCTPC).

ASIO is a member of the Australian Government Counter-Terrorism Committee (AGCTC), chaired by the Protective Security Coordination Centre.

ASIO is also a member of the DFAT-led Interdepartmental Emergency Task Force (IDETF) arrangements for responding to a terrorist incident overseas involving Australia or Australian interests. ASIO maintains a capability to support these by hosting the NIG and the ability to deploy intelligence support overseas.

EXERCISE WYVERN SUN

In July 2004 ASIO helped plan and conduct and participated in Exercise WYVERN SUN, a combined Australian and Thai counter-terrorism exercise held in Thailand. It involved a special recovery operation in response to a terrorist incident with Australian hostages. It provided an opportunity for ASIO to test its capabilities as part of an Australian emergency task force response.

TECHNICAL SUPPORT UNIT

ASIO's Technical Support Unit (TSU) can be deployed in the event of a terrorist or siege incident to assist the AFP and State and Territory police.

The TSU provides technical support to the police commander managing an incident and to police technical units gathering intelligence at the scene. The TSU is maintained in a high state of readiness and is regularly exercised.

In 2004–05 the TSU acquired new vehicles which will provide greater flexibility in deploying a technical collection capability.

The TSU was deployed to assist State police technical units in tactical response exercises (TACREX) in:

- Western Australia in August 2004;
- Victoria in April 2005; and
- South Australia in May 2005.

INTELLIGENCE COLLECTION

ASIO's collection activities are directed on a strategic level by the Intelligence Co-ordination Committee (ICC, see page 53).

While ASIO has access to a range of intrusive powers to assist in investigations, protocols exist which require that the level of any intrusion into the privacy of individuals must be commensurate with the assessed level of threat. Accordingly, the majority of investigations will begin using less intrusive methods, including community interviews. Investigations will only progress to more intrusive methods if the initial investigation is inconclusive and the assessed level of threat warrants further investigation.

Within a tightly focused risk-management framework we investigate known threats to security while at the same time seek to identify unknown and emerging threats/issues.

HUMAN SOURCE INTELLIGENCE COLLECTION

We continue to devote significant resources towards developing the cultivation and recruitment skills of our intelligence officers. Training includes in-house ASIO courses and a range of other courses; language training in Australia and abroad; and conferences.

The TSU provides technical support to the police commander managing an incident and to police technical units gathering intelligence at the scene.



TSU vehicle being driven onto a RAAF aircraft.

ASIO's surveillance capability can be deployed anywhere in Australia to collect intelligence on persons of security interest.

Only the Director-General can request a warrant and must provide the Attorney-General with a written statement specifying the grounds on which it is considered necessary to use special powers to progress an investigation.

SURVEILLANCE

ASIO's surveillance capability can be deployed anywhere in Australia to collect intelligence on persons of security interest. Surveillance is used to support investigations, including covert operational activity.

In 2004–05 surveillance resources were heavily utilised, primarily to progress high-priority counter-terrorism investigations.

ASIO's surveillance capacity expanded in 2004–05 with the recruitment and training of additional officers.

ASIO also works closely with police services on surveillance matters.

SPECIAL POWERS OPERATIONS

The Attorney-General's guidelines for the collection of intelligence require investigations to be conducted with as little intrusion into privacy as possible, consistent with the national interest. The use by ASIO of intrusive investigative methods is determined by the gravity and immediacy of the threat to security posed by the subject. Where the threat is assessed to be serious, or could emerge quickly, a greater degree of intrusion, such as the use of the special powers under Division 2 or Division 3 of Part III of the ASIO Act and Part III of the *Telecommunications (Interception) Act 1979*, may be necessary. Use of these powers – which are governed by strict warrant procedures – requires that a subject's activities are, or are reasonably suspected to be, or are likely to be, prejudicial to security.

WARRANT APPROVALS

Only the Director-General can request a warrant and must provide the Attorney-General with a written statement specifying the grounds on which it is considered necessary to use special powers to progress an investigation.

Prior to submission to the Attorney-General, the warrant request is thoroughly assessed within ASIO, including by the ASIO Legal Adviser. A senior official of the Attorney-General's Department independently advises the Attorney-General on whether the relevant statutory requirements have been met.

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

In 2004–05 the Attorney-General approved all warrant requests submitted to him.

Emergency Warrants

Under legislation, the Director-General may issue a warrant for up to 48 hours in emergency situations. The Attorney-General is to be advised of any such warrants.

QUESTIONING AND DETENTION

The ASIO Act permits the Director-General, with the Attorney-General's consent, to seek a warrant from an issuing authority to allow ASIO to question a person if there are reasonable grounds for believing that questioning a person will substantially assist the collection of intelligence in relation to a terrorism offence and if reliance on other intelligence collection methods would be ineffective. In limited circumstances, a warrant may also authorise the detention of a person.

Any questioning pursuant to a warrant must be undertaken in the presence of a prescribed authority. The Inspector-General of Intelligence and Security may attend during any questioning or detention under the warrant.

ASIO executed 11 questioning warrants issued in 2004–05 involving 10 people. None of these warrants authorised the detention of a person.

Under the legislation a person who provides false or misleading information under a questioning warrant can be guilty of an offence. Faheem Lodhi, who was questioned in October and November 2003 under a questioning warrant, was charged with terrorism offences under section 101 of the *Criminal Code Act 1995*, and with five counts of false and misleading statements under section 34G(5) of the ASIO Act. On 11 June 2005 Lodhi was committed to stand trial on all charges.

In July 2005 another of Willy Brigitte's associates, Abdul Rakib Hasan, was charged with providing false and misleading information under section 34G of the ASIO Act.

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

- the number of requests made under section 34C to issuing authorities during

the year for the issue of warrants under section 34D: 11

- the number of warrants issued during the year under section 34D: 11
- the number of warrants issued during the year that met the requirement in paragraph 34D(92)(a) (about requiring a person to appear before a prescribed authority): 11
- the number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year that met the requirement in paragraph 34D(2)(a) and the total of all those hours for all those persons:

Person 1	15 hours, 50 minutes
Person 2	5 hours, 17 minutes
Person 3	7 hours, 37 minutes
Person 4	12 hours, 49 minutes
Person 5	2 hours, 38 minutes
Person 6	5 hours, 24 minutes
Person 7	4 hours, 05 minutes
Person 8	4 hours, 05 minutes
Person 9	5 hours, 17 minutes
Person 10	6 hours, 02 minutes
Total	69 hours, 04 minutes

Table 9: Questioning under warrant

- the number of warrants issued during the year that met the requirement in paragraph 34(D)(b) (about authorising a person to be taken into custody, brought before a prescribed authority and detained): 0
- the number of times each prescribed authority had people appear for questioning before him or her under warrants issued during the year – four people (one of whom appeared twice) appeared before one prescribed authority; three people appeared before

ASIO executed 11 questioning warrants issued in 2004–05 involving 10 people. None of these warrants authorised the detention of a person.

The Telecommunications Act 1997 requires all carriers and carriage service providers (C/CSPs), including Internet service providers (ISPs) to give ASIO and law enforcement agencies such help as is reasonably necessary for the purposes of safeguarding national security, enforcing criminal law and protecting public revenue.

another prescribed authority; two people appeared before a third prescribed authority; and one person appeared before a fourth prescribed authority.

The information reported above reflects all periods of questioning which occurred under warrants issued in 2004–05.

A review by the Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD) into the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act, which contains the questioning and detention powers, commenced. The Committee is required to complete its review by 22 January 2006.

The Inspector-General of Intelligence and Security or a member of his staff was present during each of ASIO's questioning under warrant for significant portions of the duration. In his submission to the PJCAAD, the Inspector-General came to the following conclusions in respect of each of the section 34D warrants he had witnessed, namely:

- the questioning of the subjects of the warrants had been conducted in a professional and appropriate manner;
- the individuals who had been the subject of questioning had been accorded dignity and respect;
- the facilities used for each questioning warrant had been appropriate;
- due consideration had been given in each case to the subject's physical comfort and religious needs; and
- the existing commitments of subjects had been taken into account in determining the timing of questioning.

The Inspector-General has raised a number of issues with the Director-General (of a largely procedural nature). These are outlined in his submission to the inquiry and are available on the website: www.aph.gov.au/house/committee/pjcaad, submission number 74.

TELECOMMUNICATIONS INTERCEPTION (TI)

Regulatory Framework

The *Telecommunications Act 1997* requires all carriers and carriage service providers (C/CSPs), including Internet service providers (ISPs) to give ASIO and law enforcement agencies such help as is reasonably necessary for the purposes of safeguarding national security, enforcing criminal law and protecting public revenue. That help extends to the provision of interception services, including services in executing an interception warrant under the *Telecommunications (Interception) Act 1979*. C/CSPs are required to develop, install and maintain interception capabilities unless specifically exempted. C/CSPs bear the costs of these capabilities. The Act also requires C/CSPs to develop, install and maintain delivery capabilities to enable the intercepted communications to be transmitted to the monitoring facilities of ASIO and law enforcement agencies. C/CSPs are able to recover these costs from ASIO and law enforcement agencies. Agencies must develop and maintain their own processing and monitoring capabilities.

'Lead House' Role

Consistent with its functions, ASIO has a 'lead house' role in managing the development of interception and delivery capabilities for use by Commonwealth, State and Territory law enforcement agencies, as well as for its own purposes.

Commercial Environment

There are now 169 licensed carriers (of which approximately 129 are active) and some 1569 CSPs registered with the Telecommunications Industry Ombudsman. Of these some 1069 are listed as ISPs.

Telecommunications Interception Policy

As part of its 'lead house' role, ASIO continued to work with the Attorney-General's Department in developing telecommunications interception-related policy. ASIO has also actively engaged with the Department of Communications, Information Technology and the Arts, the Attorney-General's Department, the Australian Communications Authority, the telecommunications industry and a number of other organisations on a range of policy issues expected to impact on telecommunications interception in the longer term.

ASIO provided technical and operational input to the work of the Agency Coordinator's Office in the Attorney-General's Department. This included comment on carriers' interception capability plans, applications for carrier licences and applications for exemption from interception obligations.

ASIO contributed to the development of legislation, including the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004, which was enacted in December 2004. ASIO was consulted on, and provided a submission to, the Review of the Regulation of Access to Communications.

TECHNICAL CAPABILITIES

ASIO's technical operations group supports our intelligence collection capabilities by providing technical expertise in a range of areas.

ASIO also maintains an engineering development and production group to undertake complex engineering projects in-house and to manage out-sourced projects to develop uniquely engineered technical capabilities.

Cooperation with Australian agencies

ASIO works closely with the AFP, ASIS, DSD and the Defence Science and Technology Organisation (DSTO) to ensure that research and development work remains focused on high-priority requirements and that effort is not duplicated across agencies. ASIO contributes to PM&C's Scientific, Engineering and Technology Unit, including through a seconded officer. Cooperation with State and Territory police services on technical matters also continued to increase.

ASIO works closely with the AFP, ASIS, DSD and DSTO to ensure that research and development work remains focused on high-priority requirements and that effort is not duplicated across agencies.

The role of the AAU is to support investigations by applying mathematical and statistical analysis techniques to complex intelligence problems.

ASIO has a long history of working closely with police services but our relationships have strengthened and deepened in recent years.

MONITORING AND ALERTING

Since becoming operational in September 2002, the Research and Monitoring Unit (RMU) has been an important part of ASIO's business process. It is now relied on for its two principal functions:

- 'around-the-clock' monitoring of the global and domestic security environment, drawing from both open source and classified information, to ensure real-time responsiveness for all ASIO investigative, assessment and reporting functions; and
- providing a specialised open source research capacity to meet the requirements of all areas of ASIO.

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

In addition, RMU issues alerts in response to significant security developments in Australia or overseas.

Open-source research

The demand for open source information from all parts of ASIO continues to grow.

The RMU provides a specialised open source research capacity for 15 hours each weekday with urgent requests outside that period dealt with by monitoring staff who are on duty 24 x 7. This change was made in response to demand for support from ASIO staff operating in other time zones and staff of the National Threat Assessment Centre, itself a 24 x 7 operation.

ADVANCED ANALYTICAL UNIT (AAU)

The role of the AAU is to support investigations by applying mathematical and statistical analysis techniques to complex intelligence problems.

COOPERATION WITH AUSTRALIAN AGENCIES

POLICE

ASIO has a long history of working closely with police services. Our relationships have strengthened and deepened in recent years – particularly as changes to legislation and increased ASIO and police resources have been directed towards prosecuting individuals with links to terrorism. This is most notable in the Federal sphere and in New South Wales and Victoria.

In all States and Territories ASIO officers have regular contact with senior and working-level police to identify and work through issues, coordinate resources and conduct operations and investigations in the most effective manner.

Joint training

Throughout Australia our engagement with the police also includes a significant two-way training commitment. Police services provide ASIO with training and awareness programs particularly around issues such as evidence handling and on the collection of intelligence in ways to maximise its evidentiary value. ASIO provides training and briefings to police about our role, intelligence collection and the background and history of extremist and terrorist organisations.

THE JOINT COUNTER-TERRORISM INTELLIGENCE CO-ORDINATION UNIT (JCTICU)

The JCTICU was established in September 2002 to enhance collaboration on counter-terrorism investigations. It has representatives from the AFP, ASIO, ASIS, DSD and DIGO and is managed by an ASIO Senior Officer. The strategic direction of the JCTICU is set by a steering committee comprising senior representatives of each agency and chaired by the Deputy Director-General of ASIO.

National Security Hotline

Since it was established in December 2002, the Protective Security Coordination Centre's National Security Hotline (NSH) has referred over 24 000 calls to ASIO. While not all NSH calls provide useful intelligence, those that do can be significant.

We work closely with police in respect of new leads, including those generated by the NSH. ASIO and the relevant police service cooperate and coordinate the response to lead information generated by NSH calls, with each agency taking responsibility for particular issues or investigations and sharing the outcomes of their enquiries.

OTHER DEPARTMENTS AND AGENCIES

ASIO works closely with other government departments, particularly:

- Australian Customs Service; and
- Department of Immigration and Multicultural and Indigenous Affairs.

SPECIAL EVENTS

ASIO worked closely with relevant Federal and State agencies and with the M2006 Corporation to ensure security for the Melbourne Commonwealth Games. ASIO's contribution is focused on the provision of high-quality and timely threat and other security intelligence advice, security checking for accreditation purposes and the provision to DIMIA of security-related visa checking advice.

At the time of the Games ASIO will closely coordinate its activities with other Federal and State government agencies and police, particularly Victoria Police, which has overall responsibility for security and the maintenance of law and order within Victoria for M2006 and related activities. A number of ASIO officers will be co-located with Victoria Police in the lead-up to and during the Games. Additional resources, including ASIO's counter-terrorism response capability, will be deployed to Melbourne during the Games period.

The JCTICU was established in September 2002 to enhance collaboration on counter-terrorism investigations.

By 30 June 2005 ASIO had liaison relationships with 266 authorities in 112 countries.

LIAISON WITH INTERNATIONAL PARTNERS

ASIO's international liaison network is a keystone in our ability to fulfil our responsibilities under the ASIO Act.

By 30 June 2005 ASIO had liaison relationships with 266 authorities in 112 countries.

In addition to establishing new liaison relationships – with the approval of the Attorney-General – the breadth and depth of our engagement with both traditional and non-traditional partners has undergone significant transformation.

- Having ASIO liaison officers abroad has expanded ASIO's access to security intelligence.

All liaison officers sent to posts where English is not the primary language are given intensive language training. ASIO officers have received language training ranging from 1 to 18 months, including training in Australia and in-country before the commencement and throughout their posting.

ASIO liaison officers travel widely within their respective regions to engage as frequently as is necessary with liaison partners.

Upgrading ASIO's IT connectivity with its liaison posts continued in 2004–05.

INTERNATIONAL TRAINING AND DEVELOPMENT

In addition to the exchange of intelligence, our developing relationships have provided a number of training opportunities with traditional and non-traditional partners.

COUNTER-TERRORISM INTELLIGENCE TRAINING PROGRAM

In the 2005–06 Budget the Government allocated \$19.9m over four years to establish a Centre for Counter-Terrorism Intelligence Cooperation and Joint Training within ASIO to coordinate intelligence training and enhance cooperation in the region.

The activity will bring together resources, people and expertise and be known as the Counter-Terrorism Intelligence Training Program (CTITP). It will provide counter-terrorism intelligence training that best meets the needs of our regional partners where this is mutually agreed and advantageous.

Although the program did not formally commence until 2005–06, ASIO – working with others in the Australian Intelligence Community – undertook preparatory work in the reporting period.

VISITS AND CONFERENCES

In 2004–05 ASIO participated in a broad range of bilateral and multilateral conferences and visits with international liaison partners.

It will provide counter-terrorism intelligence training that best meets the needs of our regional partners where this is mutually agreed and advantageous.

INTERNATIONAL EVENTS

Athens Olympics 2004

ASIO was a member of the Greek Olympics Advisory Security Group and had a team of officers in Athens in the lead-up to and during the Olympics and the Paralympics.

ANZAC Day 2005, Gallipoli

Intelligence provided by liaison partners informed the NTAC's assessments of the threat to Prime Minister Howard and other Australian VIPs at the 90th anniversary commemoration.

Beijing Olympics 2008

ASIO will remain engaged with Chinese authorities in the lead-up to the Beijing Olympics.

ASIO will remain engaged with Chinese authorities in the lead-up to the Beijing Olympics.

A large part of this performance report is 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 in a secure region' by:

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

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



PART 3: MANAGEMENT AND ACCOUNTABILITY



PART 3

MANAGEMENT AND ACCOUNTABILITY

ASIO conducts its work with respect for freedom of opinion and civil liberties and avoidance of bias. ASIO operates within a framework designed to ensure its accountability, including:

- the Attorney-General, to whom ASIO is responsible
- the National Security Committee of Cabinet, which sets policy, decides budgets and reviews the performance of intelligence agencies
- the Parliamentary Joint Committee on ASIO, ASIS and DSD
- the Inspector-General of Intelligence and Security, who monitors the legality and propriety of ASIO's activities
- a classified *Annual Report to Government*, a copy of which is provided to the Leader of the Opposition, and an unclassified *Report to Parliament*, which is publicly available on ASIO's website.

CORPORATE GOVERNANCE

ASIO has corporate governance arrangements and a culture that supports accountability, risk management, flexible allocation of resources to meet business needs, regular critical review and performance management. Business priorities are regularly reviewed by senior management. ASIO also has an active audit, evaluation and fraud control program.

The Corporate Executive, chaired by the Director-General and consisting of the five division heads, two managers on rotation and the President of the Staff Association as an observer, sets the strategic direction and corporate priorities; oversees resource management; and regularly reviews corporate performance within a risk-management framework. Analysis of trends and identification of pressure points provides an objective basis for managing risk and making informed resource deployment decisions.

The Corporate Executive is supported by six committees.

The Intelligence Coordination Committee (ICC) consists of the five division heads

and is chaired by the Deputy Director-General. It uses a risk-management approach to set investigative priorities and review performance against objectives. It also reviews the security environment, recommends resource adjustments and considers operational policy issues.

The Audit and Evaluation Committee includes a senior executive from the Australian National Audit Office. Chaired by the Deputy Director-General, it sets the audit and evaluation program for the Organisation, reviews the outcomes of audits and evaluations and oversees the implementation of recommendations.

The Information Management Committee is chaired by the Deputy Director-General, and sets priorities for information management projects, provides guidance to the information management area and monitors and evaluates the implementation of projects.

ASIO has corporate governance arrangements and a culture which support accountability, risk management, flexible allocation of resources to meet business needs, regular critical review and performance management.

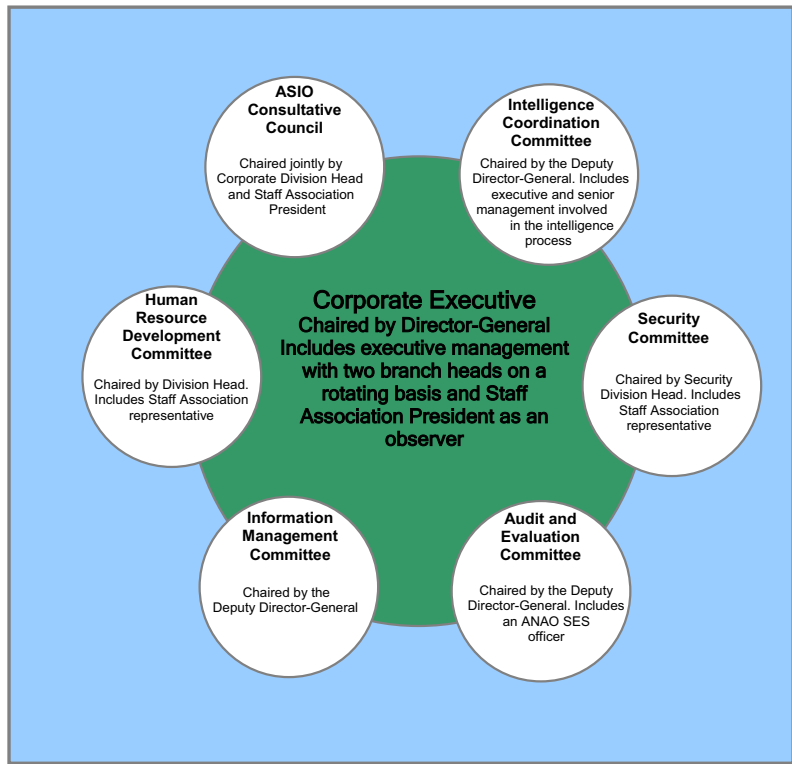


Figure 2: ASIO's corporate governance structure

The ASIO Consultative Council is chaired jointly by the head of the Corporate Management and Liaison Division and the President of the Staff Association. It allows managers and staff to meet in a structured way to discuss and resolve corporate issues. It is a deliberative and advisory forum, not a determining body.

The Human Resource Development Committee is chaired by a Division head and includes representatives of the Staff Association. It provides guidance on the implementation of training programs and other staff development issues, ensures that relevant training is delivered to the right people and that the Organisation continues to build its human resource capabilities.

The Security Committee is chaired by the head of the Security Division and includes representatives of the Staff Association. It ensures security is appropriately considered in all major developments or initiatives and promotes sound security practice.

CORPORATE PLANNING

ASIO's *Corporate Plan 2002–06* articulates the Organisation's values, business focus, outputs and performance indicators within a security environment characterised by heightened levels of threat and a diverse and volatile international and regional environment. Our business focus remained:

- competing for the best people;
- staying ahead of technology;
- maintaining best security practice;
- leveraging partnerships; and
- satisfying customers.

The *Corporate Plan 2002–06* is available publicly at www.asio.gov.au.

ACCOUNTABILITY AND EXTERNAL SCRUTINY

THE GOVERNMENT

National Security Committee of Cabinet (NSC)

The NSC sets policy and decides intelligence agencies' budgets. The Director-General is a member of NSC and it receives ASIO's classified *Annual Report* that contains detailed information about ASIO's performance and governance. The NSC considers the performance of the intelligence agencies, including ASIO, based on advice from the Department of the Prime Minister and Cabinet.

Attorney-General

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

The number of briefings and submissions to the Attorney-General remained high at 237 – compared to 268 in 2003–04 and 214 in 2002–03.

ASIO operational activity uses methods commensurate with the assessed risk

under the Attorney-General's guidelines for the collection of intelligence.

The Attorney-General receives reports from the Inspector-General of Intelligence and Security on inquiries relating to ASIO, including complaints.

THE PARLIAMENT

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

The 2004 *Report of the Inquiry into Australian Intelligence Agencies* by Mr Philip Flood AO noted that the PJCAAD, established in 2001 to replace the Parliamentary Joint Committee on ASIO, has provided a significant parliamentary insight into the intelligence community, as well as opportunities for agencies to benefit from the perspectives of experienced parliamentarians.

The PJCAAD has a mandate under s29(1)(a) of the *Intelligence Services Act 2001* to review the administration and expenditure of ASIO, ASIS and DSD and can also enquire into matters referred to it by the Government or by the Parliament. On 7 March 2005 the PJCAAD reported on its third review of administration and expenditure. ASIO appeared before the Committee on 6 May 2004 in connection with this review.

In addition, under s102.1A of the *Criminal Code Amendment (Terrorist Organisations) Act 2004* the PJCAAD can review the listing of an organisation as a terrorist organisation. ASIO appeared before the PJCAAD on:

- 1 February in connection with the re-listing of al-Qa'ida, Jemaah Islamiyah, the Abu Sayyaf Group, the Armed Islamic Group, Jamiat ul-Ansar, and the Salafist Group for Call and Combat as terrorist organisations; and
- 2 May in connection with the listing of Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn (the al-Zarqawi network).

The number of briefings and submissions to the Attorney-General remained high at 237 – compared to 268 in 2003–04 and 214 in 2002–03.

ASIO presented classified and unclassified submissions to the PJCAAD in connection with its review of the questioning and detention powers under Division 3 of Part III of the ASIO Act.

- The former Director-General appeared before the Committee in connection with this review on 2 May 2005.

The former Director-General also provided a private background briefing on 31 January to new Committee member, the Hon Duncan Kerr, SC, MP and a private briefing to the PJCAAD on the security environment on 1 February.

Other parliamentary oversight

In 2004–05 the former Director-General appeared before the Senate Legal and Constitutional Committee on 15 February and 24 May. On 23 June the Acting Director-General provided a private briefing to the Public Works Committee regarding the proposed extension to the ASIO Central Office building. ASIO also responded to 84 Questions on Notice from Members and Senators.

INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The role of the Inspector-General of Intelligence and Security (IGIS) is to ensure ASIO and other intelligence agencies act legally and with propriety, comply with ministerial guidelines and show due regard for human rights. The IGIS may, in respect of ASIO, initiate inquiries, respond to requests by the Prime Minister or the Attorney-General, or investigate complaints from members of the public.

Monitoring and review

The IGIS conducts regular reviews of various aspects of ASIO's work, including:

- use of special powers under warrant;
- access to and use of AUSTRAC and Australian Taxation Office information;
- compliance with the *Archives Act 1983*;

- liaison with, and provision of information to, law enforcement agencies;
- official use of alternate identification documentation in support of assumed identities; and
- operational activity and investigations.

These inspections by the IGIS identified a number of administrative or procedural matters requiring attention – remedial action was taken in all instances. Further details of these inspection activities can be found in the IGIS *Annual Report* at www.igis.gov.au.

Details of the IGIS's monitoring of the use of questioning and detention powers are recorded under Output 3, page 63.

Complaints

In 2004–05 the IGIS commenced 27 new full or preliminary inquiries into complaints made by members of the public or their legal representatives:

- 14 concerned the progress of visa applications
- 13 concerned a range of issues related to ASIO's operational activities.

AUDIT, EVALUATION AND FRAUD CONTROL

Fraud Control Plan

ASIO's *Fraud Control Plan* was updated in 2004 and will be reviewed in 2005–06. All ASIO staff are required to attend a program on ethics and accountability at least once every three years. The program includes a substantial component on fraud control, ASIO's values and code of conduct, and ASIO's expectations of its staff in relation to legal and ethical behaviour and propriety.

No fraud investigations were undertaken in 2004–05.



Inspector-General of Intelligence and Security, Ian Carnell, addressing an Ethics and Accountability course, June 2005

Internal audits and evaluations

In 2004–05 eleven internal audits and one evaluation were completed.

Recommendations resulting from these audits to address administrative or procedural shortcomings were implemented or addressed. No loss of monies was reported.

Assumed identities

All use of assumed identities by ASIO is authorised under Part 1AC of the *Crimes Act 1914 (Cth)*, commonly referred to as the 'Commonwealth Assumed Identity Scheme'. This scheme provides a mechanism whereby the Director-General or a delegate may authorise the use of assumed identities and the acquisition of supporting documents from Commonwealth agencies and non-government agencies.

An audit was conducted in January 2005 of records of authorisations under the Commonwealth scheme, with no discrepancies detected.

During the year, assumed identity approvals were granted in accordance with the *NSW Law Enforcement and National Security (Assumed Identities) Act 1998*. The NSW scheme is used by ASIO in addition to the Commonwealth scheme where evidence of assumed identity is sought in NSW.

The most recent audit required in accordance with Section 11 of the Act was completed in July 2005 for the preceding financial year. The audit did not disclose any fraudulent or other criminal behaviour.

ACCESSIBILITY TO THE PUBLIC

ASIO WEBSITE

Interest in ASIO's website (www.asio.gov.au) continued to increase, but at a lower rate than in 2003–04. In 2004–05 the site recorded an average of 1110 visitor sessions per day (up slightly from 931 sessions per day in 2003–04) and 50 565 hits (up from 37 915 last year). ASIO's annual *Report to Parliament* and employment pages remained the most popular, particularly coinciding with the timing of advertising and recruitment campaigns.

MEDIA POLICY

Consistent with long-standing practice ASIO will not normally comment on specific cases or sensitive national security matters. Where appropriate, the Attorney-General (or the Director-General with the Attorney's agreement) will provide public comment concerning ASIO where this may assist in promoting public confidence in the legality, propriety and effectiveness of the Organisation.

PUBLIC SPEECHES

The former Director-General gave three public speeches in 2004–05 concerning the terrorist threat to Australian interests and our response to it, including to the Sydney Institute on 26 October, the Australian Chamber of Commerce and Industry in Canberra on 3 November, and to the LawAsia Conference on the Gold Coast on 23 March. The Deputy Director-General addressed the Security in Government Conference in Canberra on 10 May. These speeches are available on ASIO's website.



Consistent with long-standing practice ASIO will not normally comment on specific cases or sensitive national security matters.

INTERVIEWS OF MEMBERS OF THE PUBLIC

In the course of progressing investigations ASIO officers frequently seek assistance from members of the public. ASIO officers operate under a code of conduct based on the Australian Public Service code of conduct. ASIO officers engaged in operational or investigative activity carry official identification and are required to conduct themselves in a professional manner. Any concerns about an ASIO officer's bona fides or conduct should be reported to ASIO or to the Inspector-General of Intelligence and Security.

With its workforce projected to increase to 1150 by 2005–06, the Organisation has continued to focus its efforts on attracting, developing and retaining quality people to ensure organisational performance and capabilities are sustained and enhanced.

OUR PEOPLE

As at 30 June 2005 ASIO employed 955 staff. With its workforce projected to increase to 1150 by 2005–06, the Organisation has continued to focus its efforts on attracting, developing and retaining quality people to ensure organisational performance and capabilities are sustained and enhanced.

		2000–01	2001–02	2002–03	2003–04	2004–05
Band 1	Female	1	2	2	2	4
	Male	9	8	9	9	10
Band 2	Female	1	1	1	1	1
	Male	2	2	4	4	4
Band 3	Male	1	1	1	1	1
Total		14	14	17	17	20

Table 10: SES equivalent staff classification and gender at 30 June, 2000–01 to 2004–05. (does not include the Director-General)

	2000–01	2001–02	2002–03	2003–04	2004–05
Full-time staff equivalent (FSE) at 30 June	551	597	637	770	894
Number of staff at 30 June	584	618	668	805	955

Table 11: Staffing levels and number at 30 June, 2000–01 to 2004–05

	2000–01	2001–02	2002–03	2003–04	2004–05
Permanent full-time	453	497	536	603	693
Temporary full-time ¹	63	58	51	103	155
Permanent part-time	26	25	28	38	43
Temporary part-time	14	18	23	28	22
Casual	25	19	30	33	42
Non-operational (including unattached and on compensation)	3	1	-	-	-
Total	584	618	668	805	955

¹ Includes 15 secondees and 5 locally engaged staff.

Table 12: Composition of workforce, number at 30 June, 2000–01 to 2004–05

WORKPLACE RELATIONS AND REFORMS

A principal element of the employment relations framework is the ASIO Consultative Council (see page 54) whose membership is comprised of Management and Staff Association representatives. The Council met at least monthly throughout the year to address workplace issues and endorse enhancements to people management policies and practices.

ASIO's current Workplace Agreement is due to expire in March 2006 and staff received the final four percent salary increase in April 2005. Planning for the Organisation's Seventh Workplace Agreement commenced, with staff to vote in early 2006.

Owing to changes in corporate priorities and the subsequent reallocation of resources, major reforms such as consolidating terms and conditions of employment into a single 'plain English' document were progressed but not completed during the reporting period. These are expected to be completed in 2005–06.

A staff survey was conducted in June 2005 to measure employee perceptions,

attitudes, concerns and areas of satisfaction across a range of key cultural and performance dimensions. Analysis of the results is expected to be provided to staff in early 2005–06.

PERFORMANCE PAY

SES officers are eligible to receive performance pay, with the amount based on a percentage of gross salary. In 2004–05, 14 officers received performance pay for 2003–04 with amounts ranging from \$2767 to \$21 566. The average payment was \$9330 and the total amount paid was \$130 630.

RECRUITMENT AND STAFFING

During 2004–05 we recruited 224 staff, compared to 195 in 2003–04. Once again this was an exceptional effort, being the most staff ever recruited into the Organisation over a financial year.

Recruitment remains one of ASIO's key challenges as we continue to seek quality staff to fill a broad range of roles. Linguistic, intelligence analysis and surveillance capabilities remain a particular priority. The level of recruitment will remain high into 2005–06.

ASIO staff recruitment remains a resource-intensive task because of the need for security clearances and other general suitability (including psychological) requirements. The lead time in recruitment represents an ongoing challenge for meeting government requirements. We have had to pay close attention to recruitment targets and times, and this will need to continue into 2005–06.

STAFFING PROFILE

We continued to engage temporary employees on a contract basis to meet short-term needs and provide flexibility to our staffing arrangements. At 30 June 2005, 23 percent of staff were temporary employees compared to 20 percent in 2003–04.

STAFF RETENTION

ASIO's attrition rate has dropped over the last 12 months to 5.8 percent of the workforce, the lowest since June 1999.

In separation interviews with our personnel and security areas, staff cited similar reasons as last year for their leaving – better promotional opportunities, increased remuneration, greater job satisfaction and greater rewards and recognition.

Action taken by ASIO to address these issues may have contributed to the

reduced numbers of staff leaving over the past year.

ADVERTISING

ASIO continued a broad 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. We did further work on our graduate recruitment campaign to update the look of advertisements and our website.

Advertising costs, mainly in the print media, were \$835 347 compared to \$753 836 in 2003–04.

During 2004–05 we recruited 224 staff, compared to 195 in 2003–04. Once again this was an exceptional effort, being the most staff ever recruited into the Organisation over a financial year.

DEVELOPING OUR PEOPLE

We invested \$3 613 963 (about 2.8 percent of our budget) in training and development in 2004–05, including corporately funded training and job-specific courses funded by individual work groups. The corporate training program focused on developing intelligence capability as well as management and administrative competencies across the organisation.

Management and leadership skills

Leadership development continued to be a priority for staff with management responsibilities, including all Senior Executive Service (SES) and Senior Officers (SO). A comprehensive Leadership Development Strategy was put in place, ensuring that leadership capability across the organisation is aligned to national public sector best practices. The broad range of training activities included time-outs, formal in-house and external courses, including the introduction of a new 'From Management to Leadership' program and support for tertiary education.

Three SES time-outs focused on performance improvement, managing organisational growth, ethics and accountability, budget and new policy proposals, corporate governance and effectively addressing the emerging security environment.

A total of 152 SOs attended focus groups generating ideas for quality improvement in a wide range of areas, including linguistic capability, organisational growth, ethics and accountability, training and performance management.

All Senior Officers and SES staff attended two SES–SO time-outs focusing on organisational priorities, counter-terrorism, information management, security, ethics and accountability and managing growth. These included presenters from outside the Organisation to provide an external context.

Analytical and operational skills

A comprehensive intelligence training program throughout the year delivered over 3860 days of training in areas such as intelligence gathering, analysis, investigation management and reporting skills for ASIO's intelligence officers. Some of this training is conducted in cooperation with foreign intelligence partners.

Graduate Traineeship

The first delivery of the redesigned Graduate Traineeship program was completed with 24 officers graduating from the 12-month program in January 2005. A review of the program concluded it was highly successful in developing the fundamental intelligence officer skills required of newly graduated Generalist Intelligence Officers (GIOs), but suggested some minor changes which are being implemented.

ASIO recruited a further 43 GIO trainees in 2004–05. They commenced in January 2005. The minimum academic qualification to enter the GIO Traineeship is a four-year degree or equivalent.

At the end of the reporting period, recruitment of a further 30–35 graduates to commence in 2005–06 was well underway.

An external review of GIO trainee recruitment was conducted during the year to identify opportunities for improvement of the various processes and to ensure we did not disadvantage candidates from non-English-speaking backgrounds. The core GIO competencies were reviewed and validated, and improvements were made to the assessment centre selection process.

The corporate training program focused on developing intelligence capability as well as management and administrative competencies across the organisation.

Secondments and personnel exchanges with other agencies in Australia and overseas both into and out of ASIO continued, reflecting the partnership approach to counter-terrorism.

Linguistic capability

The Flood Report noted the need for a stronger language capability in Australian intelligence agencies. ASIO has developed a program to commence in 2005–06 to train several officers each year in languages. Training will be full-time for up to two years and will involve in-country components. Officers who receive this training will be placed in positions where they will be able to apply their language skills to enhance their effectiveness.

Administrative skills

A full program of administrative training was delivered including contract management, selection panel skills, presentation skills, trainer training, critical thinking, interviewing, effective reading and writing, ethics and accountability, finance and budgeting, and introduction to ASIO:

- 236 staff received training in the use of our administrative and intelligence computer systems and applications;
- the Ethics and Accountability in ASIO program continued to be delivered for ASIO staff with 133 staff attending the program in 2004–05; and
- 59 people were provided with support for tertiary studies.

Joint Australian Intelligence Community (AIC) training

The Flood Report identified a need for greater cooperation and sharing of resources in relation to training across the AIC. ASIO is a member of the Joint AIC Induction Steering Committee and the Joint AIC Induction Curriculum Development Committee. ASIO officers participated in the monthly Joint AIC Induction Program, which commenced in May 2005, both as students and presenters.

SECONDMENTS

Secondments and personnel exchanges with other agencies in Australia and overseas both into and out of ASIO continued, reflecting the partnership approach to counter-terrorism.

ASIO has officers seconded to the AFP, ASIS, DFAT, DOTARS, ONA and PM&C. Prior to 11 September 2001 ASIO only had one external secondment – to PM&C. Within ASIO, officers are seconded from the AFP, ASIS, AUSTRAC, Defence, DFAT, DIGO, DIO, DOTARS, DSD, DSTO and ONA. Before 11 September 2001 there was only one external secondment into ASIO – from Defence.

WORKPLACE DIVERSITY

The Organisation launched its *Workforce Diversity Program 2005 to 2009* which encourages the recognition and appreciation of each individual and their contribution to the corporate mission and objectives. It incorporates both ongoing initiatives and introduces some new ones, including enhanced collection of recruitment and employment statistics, and raising awareness of diversity issues among managers and staff.

Diversity and Harassment Contact Officers

The established Diversity and Harassment Contact Officer (DHCO) networking group continued to address and raise the profile of diversity, harassment and bullying issues within the workplace by informing and supporting staff and managers. Eleven new DHCOs were elected during the reporting period and the Organisation took the opportunity to bring all the DHCOs together for refresher training.

Diversity Statistics

The percentage of female staff has increased to 43 percent and the percentage of senior officers who are female has risen slightly to 26 percent.

Following an evaluation of our recruitment strategies in early 2004–05, the overall representation of ethnically diverse staff has increased to about 15 percent, an increase of about 4 percentage points from 2003–04. Statistical data on workforce profile and representation of designated work groups are contained in Appendix C.

DISABILITY STRATEGY

ASIO's Disability Action Plan focuses on addressing the needs of people with disabilities through the provision of services and dissemination of information about disability issues. ASIO is committed to addressing the Commonwealth Disability Strategy principles by:

- ensuring a working environment in which staff, clients or members of the public with disabilities are not discriminated against, in that they are accepted, promoted and retained on the basis of their abilities and have access to services and facilities;
- identifying and removing barriers in access to policy and program development and delivery; and
- developing plans and strategies to ensure the needs of people with a disability are taken into account in planning and service delivery.

OCCUPATIONAL HEALTH AND SAFETY

The Occupational Health and Safety Sub-Committee continued to meet during the reporting period and, while operational pressures prevented some activities normally undertaken each year from occurring, the Organisation:

- offered free influenza vaccinations and medical examinations to promote health and well-being in the workplace and reduce absenteeism;
- provided free and subsidised skin examinations; and

- selected and trained first aid and health and safety representatives.

In accordance with its legislative obligations, ASIO notified Comcare of one incident causing serious personal injury. This incident, plus another, resulted in two staff members being incapacitated for a period of 30 days or more.

WORKERS' COMPENSATION CLAIMS

There were 13 claims for workers' compensation submitted in 2004–05 and liability was accepted for all. This was the same number of claims as reported in 2003–04.

Following an evaluation of our recruitment strategies in early 2004–05, the overall representation of ethnically diverse staff has increased to about 15 percent, an increase of about 4 percent from 2003–04.

Border security initiatives also have been a major component of our IT work this year.

Central to ASIO's information management program has been the need to balance widespread development of new capability and the maintenance of a reliable and robust information processing environment.

INFORMATION MANAGEMENT

ENABLING ORGANISATIONAL GROWTH

The growth during 2004–05 and the need for increased information technology (IT) to service that growth, together with increased demand associated with 24 x 7 operations, resulted in a heightened pace of IT work during 2004–05. Central to ASIO's information management program has been the need to balance widespread development of new capability and the maintenance of a reliable and robust information processing environment.

Key enhancements to our technical infrastructure have been significantly increased network bandwidth to our State offices and overseas liaison offices, upgrading our processor and storage capacity and progressing our electronic records management system.

RECORDS MANAGEMENT

The improvements to ASIO's records management during the year will provide a stable and supportable facility for the management of electronic documents and records within a need-to-know security framework. This is a complex and demanding change that requires detailed analysis and planning in any agency. The complexity of this task is further complicated by the rigorous need-to-know security model that is necessary in this environment.

IT SUPPORT FOR BORDER SECURITY

Border security initiatives also have been a major component of our IT work this year.

Identity matching

The increasing demand for name checking for visa and security clearances has meant we have had to implement new systems to automate the receipt and matching of names. The Aviation Security Identity Card started this automation process and we have been able to adapt it to use for any bulk name-matching inputs that conform to a certain standard.

PROCESSING BACKLOGS

Since the 11 September 2001 attacks there has been a rapid and substantial increase in the rate and volume of information flowing to ASIO, including new streams of intelligence. This has contributed to the development of large processing backlogs.

IT BUSINESS CONTINUITY

Business continuity has also been an important focus for the year.

We also have identified critical business processes and are putting business resumption plans together to ensure response to a disaster is seamlessly integrated with the technology deployments.

ASSURING VALUE FOR MONEY IN IT PURCHASING

ASIO continues to identify suppliers of hardware and services in line with the principle of market testing.

SECURITY OF ASIO

ASIO seeks to improve security performance and lead best security practice. We do this by protecting ASIO's information, product and advice consistent with its classification; protecting knowledge of ASIO's staff, targets, sources, methods, operations and systems; and contributing to the external policy framework.

SECURITY MANAGEMENT PLAN

ASIO's (classified) *Security Plan 2005–09* was developed and endorsed. (It replaced the classified *Security Management Plan 2001–04*.) The plan provides a strategic overview for the management of security within ASIO and sets out strategies for achieving and maintaining security best practice. It addresses changes in the security environment and includes updated requirements for information concerning counter-intelligence and physical security threats to ASIO.

The objectives of the *Security Management Plan* are to:

- identify areas of risk to ASIO's operations, information, people, resources and assets through security risk assessment;
- identify policies and outline strategies that will control these risks at a level acceptable to all significant stakeholders;
- allocate responsibility and resources to these strategies; and
- ensure personnel, physical, information, information technology and telecommunications security standards are commensurate with risk levels and meet or exceed government minimum standards as determined by the *Commonwealth Protective Security Manual* (PSM), the IASF and Australian government IT security policies.

SECURITY AUDITS

During the reporting period ASIO conducted security audits in line with the scope and framework set by the IASF.

SECURITY POLICIES

ASIO's security policies are consistent with IASF best-practice guidelines and conform to the minimum standards contained in the Protective Security Manual and Australian Government IT Security Policies. In early 2005 ASIO's security policies and procedures were reviewed and updated. This led into a security awareness and education campaign that commenced in June 2005 aimed at enhancing the Organisation's security culture and decreasing the number of security breaches.

The (classified) *ASIO-ONA Workplace Emergency Response Plan* was endorsed in May 2005. The plan outlines responses to various emergency situations to ensure the safety of all staff.

PERSONNEL SECURITY

Security clearance re-evaluations

As a result of a review conducted under the auspices of the IASF in 2004, ASIO (along with other AIC agencies) is trialling the (classified) *Guidelines for Assessing Suitability to Hold a TOP SECRET (Positive Vetting) Security Clearance*, which was endorsed by the IASF. The trial will extend from February 2005 to June 2006.

ASIO maintained its regime of revalidating security clearances every 30 months and fully re-evaluating them at intervals not exceeding five years in accordance with the PSM.

File reviews and interviews with new officers, consultants and contractors were conducted during the reporting period. Such interviews, which are a non-mandatory component of our process of reviewing staff security clearances, are conducted within 5–6 months of commencement of employment and

ASIO seeks to improve security performance and lead best security practice.

ASIO's security policies are consistent with IASF best-practice guidelines and conform to the minimum standards contained in the Protective Security Manual and Australian Government IT Security Policies.

provide the opportunity for new staff to discuss any security concerns, for security procedures to be reinforced, and for the Employee Assistance Program to be explained.

In addition to the above, each officer, consultant and contractor and his/her line manager completes an Annual Security Certification which forms part of the revalidation/re-evaluation package. This is in accordance with a recommendation from the 2000 *Inquiry into Security Issues* conducted by a former Inspector-General of Intelligence and Security, Mr Bill Blick.

The growth in staff numbers over the last two years has necessitated an increase in appropriately trained revalidation and re-evaluation staff. Further growth in the Organisation will require more revalidation and re-evaluation staff.

Supporting our staff

ASIO provides active support to staff through its Employee Assistance Program. The program helps staff deal with professional and personal issues so they remain productive and viable in the workplace and to reduce the possibility of their problems becoming security issues at a later date. Much of the assistance is provided through ASIO's internal Psychological Services Unit (PSU) but external consultants with specialist skills are used when required. With the growth in staff over recent years, the program and the PSU have experienced increased demand.

IT SECURITY

ASIO continues to monitor its computer networks for insecure, unauthorised and inappropriate usage.

Current trends in IT security have focused effort on audit and investigative capability, and on the business requirement to share and transmit data securely with other government agencies.

In 2005–06 we will upgrade our IT audit capability to address the growth of the Organisation in both IT capability and staff numbers.

PHYSICAL SECURITY

The Russell Passive Defence project was completed, providing enhanced protective security measures in and around the Russell precinct including ASIO Central Office. Vehicle barrier systems comprising a combination of reinforced plinth walls, additional bollards, and security landscaping provide added protection to each facade of the building.

All incoming public mail to ASIO's Central Office is inspected using an X-ray unit and a biological containment vessel. All interstate offices have the capability to X-ray suspect items and open mail in a biological containment vessel.

BUILDING MANAGEMENT

To allow for the growth of ASIO and ONA, and our continued co-location as recommended in the Flood Report, the Government has committed \$132.6 million over four years for an extension to ASIO's Central Office building in Canberra.

Of this, \$63.2 million will be provided to the Department of Finance and Administration for the construction of the extension, \$56.5 million will be provided to ASIO and \$12.9 million to ONA for fit-out work. Construction is scheduled to commence in October 2006 and be completed in 2008–09.

Planning has commenced for a refurbishment of our State offices to accommodate growth.

In August 2004 laboratory results from a routine monthly inspection of the cooling towers at Central Office identified excess levels of Legionella bacteria. Immediate remedial action was taken to the satisfaction of ACT Health and Comcare. Both ASIO and ONA continued operating as normal as the building was safe for occupation. The dosing equipment was subsequently upgraded and a new contractor engaged for monthly maintenance and testing. Readings taken since the excess levels were recorded have all been negative for the presence of Legionella.

ECOLOGICALLY SUSTAINABLE DEVELOPMENT AND ENVIRONMENTAL PERFORMANCE

ASIO continues to pursue measures to reduce energy consumption and minimise our impact on the environment.

An upgrade of the wet areas in Central Office included energy saver shower-heads and auto-flush urinals and reusable walling systems. The recycling of paper and cardboard waste continued. However, energy demand in Central Office remained high as a result of the increased operational tempo, higher staffing levels, and 24 x 7 operations.

Pressure testing of our underground bulk fuel facilities found the system to be environmentally sound, and resulted in recommendations to further enhance environmental performance over the longer term.

Chemical usage was reduced via the introduction of a new system of cooling tower water treatment which meters chemical doses more accurately.

In May 2005 ASIO responded to the Australian National Audit Office cross-portfolio performance audit of green procurement examining agency procurement practices in relation to environmental sustainability.

To allow for the growth of ASIO and ONA, and our continued co-location as recommended in the Flood Report, the Government has committed \$132.6 million over four years for an extension to ASIO's Central Office building in Canberra.

ASIO continues to pursue measures to reduce energy consumption and minimise our impact on the environment.

In 2004–05, ASIO implemented each of the ANAO's recommendations and we continue to improve our contracting practices in line with Australian Government policy.

PURCHASING

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

The Director-General issued revised Chief Executive's Instructions in October 2004 that are available to all staff on the Organisation's Intranet. The Instructions give direction on purchasing goods and services, and entering into and managing contracts, agreements and arrangements. Detailed guidance on tendering and contract management was also made available to staff on the Intranet.

In 2004–05 ASIO's annual investment program continued. Purchasing objectives focused on investment in key business areas including technical capabilities, information technology infrastructure and protective security measures.

COMMONWEALTH PROCUREMENT GUIDELINES

In June 2005 the Director-General issued a Chief Executive's Instruction regarding the Organisation's compliance with certain aspects of the Commonwealth Procurement Guidelines released in January 2005 to reflect the Australian Government's obligations under the Australia–United States Free Trade Agreement. The Instruction directs ASIO officials to refrain from the mandatory procurement requirements and other publication requirements where the protection of national security is in the public interest.

EXEMPT CONTRACTS

In August 2004 the Director-General directed that details of ASIO agreements, contracts and standing orders must not be notified in the Purchasing and Disposals Gazette on the basis that these are exempt documents under the *Freedom of Information Act 1982* for the reason that disclosure of such documents would, or could reasonably be expected to, cause damage to the security of the Commonwealth.

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

CONTRACTS AUDIT

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

In 2004–05, ASIO implemented each of the ANAO's recommendations and we continued to improve our contracting practices in line with Australian government policy.

CONSULTANTS

During 2004–05, ASIO let 11 consultancy contracts, which was down from 19 in 2003–04. Total expenditure on consultancy contracts during the year (including contracts let during the previous year) came to \$0.158m, down from \$0.412m in 2004–05.

The decrease resulted from a greater use of in-house expertise to inform agency decision making. The main areas for consultancies were in the corporate management, information technology, protective security, accommodation and technical services areas.

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

In April 2005, ASIO responded to the Australian National Audit Office cross-portfolio performance audit of the management and reporting of expenditure on consultants.

COMPETITIVE TENDERING AND CONTRACTING



ASIO did not undertake any competitive tendering and contracting (CTC) activities in 2004–05. The scope for CTC activity by ASIO continues to be limited by national security considerations.

Parts of this report have been 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



INDEPENDENT AUDIT REPORT

To the Attorney-General

Scope

The financial statements and Director-General's responsibility

The financial statements comprise:

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

of the Australian Security Intelligence Organisation for the year ended 30 June 2005.

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

Audit approach

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

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

I have performed procedures to assess whether, in all material respects, the financial statements present fairly, in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, accounting standards and other mandatory financial reporting requirements in Australia, a view which is consistent with my understanding of the Australian Security Intelligence

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

Organisation's financial position, and of its performance as represented by the statements of financial performance and cash flows.

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

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

Independence

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

Audit Opinion

In my opinion, the financial statements of the Australian Security Intelligence Organisation:

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

Additional Statutory Disclosure

As detailed in Note 19 of the financial statements, the Australian Security Intelligence Organisation has contravened section 83 of the Constitution and has therefore breached section 48 of the *Financial Management and Accountability Act 1997*.

Australian National Audit Office



Brandon Jarrett
Executive Director

Delegate of the Auditor-General

Canberra
7 September 2005

Statement by the Director-General of Security

In my opinion, the attached financial statements for the year ended 30 June 2005 have been prepared based on properly maintained financial records (except for those matters detailed in Note 19) and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.

A handwritten signature in black ink, appearing to read 'Paul O'Sullivan', with a horizontal line underneath it.

Paul O'Sullivan
Director-General of Security

7 September 2005

STATEMENT OF FINANCIAL PERFORMANCE FOR THE YEAR ENDED 30 JUNE 2005

	Notes	2005 \$'000	2004 \$'000
Revenues from ordinary activities			
Revenues from Government	4A	137,456	98,210
Goods and services	4B	2,624	1,993
Interest	4C	—	—
Revenue from sale of assets	4D	403	976
Other revenues	4E	2,369	1845
Revenues from ordinary activities		142,852	103,023
Expenses from ordinary activities (excluding borrowing costs expense)			
Employees	5A	74,089	61,068
Suppliers	5B	56,119	33,211
Depreciation and amortisation	5C	10,624	7,739
Write-down of assets	5D	1,058	700
Value of assets sold	4D	431	959
Expenses from ordinary activities (excluding borrowing costs expense)		142,321	103,678
Borrowing costs expense	6	5	24
Net surplus / (deficit) from ordinary activities before income tax		526	(679)
Net credit to asset revaluation reserve	12	(762)	3,217
Total revenues, expenses and valuation adjustments attributable to members of the parent entity and recognised directly in equity		(762)	3,217
Total changes in equity other than those resulting from transactions with owners as owners		(236)	2,539

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

STATEMENT OF FINANCIAL POSITION AS AT 30 JUNE 2005

	Notes	2005 \$'000	2004 \$'000
ASSETS			
Financial assets			
Cash	7A	18,299	7,216
Receivables	7B	3,717	1,846
Total financial assets		22,016	9,062
Non-financial assets			
Land and buildings	8A, 8C	23,431	16,550
Infrastructure, plant and equipment	8B, 8C	37,809	28,344
Intangibles	8D	3,245	3,071
Other non-financial assets	8E	1,299	2,398
Total non-financial assets		65,784	50,362
Total Assets		87,800	59,424
LIABILITIES			
Interest bearing liabilities			
Leases	9	–	115
Total interest bearing liabilities		–	115
Provisions			
Employees	10A	17,274	17,019
Accommodation leases	10B	3,374	1,487
Total provisions		20,648	18,506
Payables			
Suppliers	11	6,505	3,854
Total payables		6,505	3,854
Total Liabilities		27,153	22,475
NET ASSETS		60,647	36,949
EQUITY			
Contributed equity	12	56,714	32,781
Reserves	12	8,734	9,496
Retained surpluses or (accumulated deficits)	12	(4,801)	(5,328)
TOTAL EQUITY		60,647	36,949
Current assets		23,315	11,460
Non-current assets		64,485	47,964
Current liabilities		14,593	12,754
Non-current liabilities		12,560	9,721

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

STATEMENT OF CASH FLOWS FOR THE YEAR ENDED 30 JUNE 2005

	Notes	2005 \$'000	2004 \$'000
OPERATING ACTIVITIES			
Cash received			
Goods and services		2,348	3,847
Appropriations		137,456	98,210
Net GST received from ATO		6,155	4,521
Total cash received		145,959	106,578
Cash used			
Employees		73,833	57,830
Suppliers		55,885	39,567
Borrowing costs		5	24
Total cash used		129,723	97,421
Net cash from / (used by) operating activities	13	16,236	9,157
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		403	976
Total cash received		403	976
Cash used			
Purchase of intangibles		1,356	1,300
Purchase of property, plant and equipment		28,018	17,386
Total cash used		29,374	18,687
Net cash from / (used by) investing activities		(28,971)	(17,711)
FINANCING ACTIVITIES			
Cash received			
Appropriations - contributed equity		23,933	10,637
Total cash received		23,933	10,637
Cash used			
Repayment of debt		115	216
Total cash used		115	216
Net cash from / (used by) financing activities		23,818	10,420
Net increase / (decrease) in cash held		11,083	1,867
Cash at the beginning of the reporting period		7,216	5,350
Cash at the end of the reporting period	7A	18,299	7,216

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

SCHEDULE OF COMMITMENTS AS AT 30 JUNE 2005

	Notes	2005 \$'000	2004 \$'000
BY TYPE			
Capital commitments			
Infrastructure, plant and equipment	A	5,180	847
Total capital commitments		5,180	847
Other commitments			
Operating leases	B	77,212	48,984
Other commitments		7,028	2,176
Total other commitments		84,240	51,160
Commitments receivable		2,194	6,508
Net commitments		87,226	45,499
BY MATURITY			
Capital commitments			
One year or less		5,180	847
From one to five years		–	–
Over five years		–	–
Total capital commitments by maturity		5,180	847
Operating lease commitments			
One year or less		11,378	6,046
From one to five years		45,516	24,112
Over five years		20,318	18,826
Total operating lease commitments by maturity		77,212	48,984
Other commitments			
One year or less		7,028	2,176
From one to five years		–	–
Over five years		–	–
Total other commitments by maturity		7,028	2,176
Commitments Receivable		2,194	6,508
Net commitments by maturity		87,226	45,499

Commitments are GST inclusive where relevant

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

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

Nature of lease	General description of leasing arrangement
Leases for office accommodation	Various arrangements apply to the review of lease payments: – 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 2005

	Notes	2005 \$'000	2004 \$'000
Contingent liabilities		200	40
Contingent assets		—	—
Net contingencies		<u>200</u>	<u>40</u>

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS FOR THE YEAR ENDED 30 JUNE 2005

Note 1: Summary of significant accounting policies

1.1 Objective of ASIO

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.

1.2 Basis of accounting

The financial statements are required by *section 49* of the *Financial Management and Accountability Act 1997* and are a general purpose financial report. The financial statements have been prepared in accordance with the agreement between the Finance Minister and the Attorney-General. This agreement states that ASIO's financial statements must be prepared in accordance with the *Financial Management and Accountability Orders (Financial Statements for reporting periods on or after 30 June 2005)* except where the disclosure of information in the notes to the financial statements would, or could reasonably be expected to be operationally sensitive. Subject to the requirements of the agreement, the financial statements are prepared in accordance with:

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

The Statements of Financial Performance and Financial Position have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets which, as noted, are at valuation. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position.

Assets and liabilities are recognised in the Statement of Financial Position when and only when it is probable that future economic benefits will flow and the amounts of the assets or liabilities can be reliably measured. However, assets and liabilities arising under agreements equally proportionately unperformed are not recognised unless required by an Accounting Standard. Liabilities and assets that are unrecognised are reported in the Schedule of Commitments and the Schedule of Contingencies.

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

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

1.3 Revenue

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

Revenues from Government

Amounts appropriated for Departmental outputs appropriations for the year (adjusted for any formal additions and reductions) are recognised as revenue, except for certain amounts that relate to activities that are reciprocal in nature, in which case revenue is only recognised when it is earned. Additions are amounts offered up in Portfolio Additional Estimates Statements. Reductions are amounts by which appropriations have been legally reduced by the Finance Minister under Appropriation Act No.3 of 2004-05.

Appropriations receivable are recognised at their nominal amounts.

Resources Received Free of Charge

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

Other revenue

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

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

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

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

ASIO Report to Parliament 2004–2005

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

1.4 Transactions with the Government as Owner

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

1.5 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 and sick leave are measured at their nominal amounts. Other employee benefits expected to be settled within 12 months of the reporting date are also measured at their nominal amounts.

The nominal amount is calculated with regard to the rates expected to be paid on settlement of the liability.

All other employee benefit liabilities are measured as the present value of the estimated future cash outflows to be made in respect of services provided by employees up to the reporting date.

Leave

The liability for employee entitlements includes provision for annual leave and long service leave. No provision has been made for sick leave as all sick leave is non-vesting and the average sick leave taken in future years by employees is estimated to be less than the annual entitlement for sick leave.

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

The liability for annual leave reflects the value of total annual leave entitlements of all employees at 30 June 2005 and is recognised at the nominal amount.

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

Superannuation

Staff of ASIO contribute to the Commonwealth Superannuation Scheme and the Public Sector Superannuation Scheme. The liability for their superannuation benefits is recognised in the financial statements of the Australian Government and is settled by the Australian Government in due course.

ASIO makes employer contributions to the Australian Government at rates determined by an actuary to be sufficient

to meet the cost to the Government of the superannuation entitlements of ASIO's employees.

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

1.6 Leases

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

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

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

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

Accommodation leases – make good

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

1.7 Borrowing Costs

All borrowing costs are expensed as incurred except to the extent that they are directly attributable to qualifying assets, in which case they are capitalised. The amount capitalised in a reporting period does not exceed the amounts of costs incurred in that period.

1.8 Cash

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

1.9 Other Financial Instruments

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

Trade Creditors

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

Contingent Liabilities and Contingent Assets

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

1.10 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.

1.11 Property, Plant and Equipment (PP&E)

Asset recognition threshold

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

Revaluations

Land, buildings, infrastructure, plant and equipment are carried at valuation. Valuations undertaken in any year are as at 30 June.

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

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

Assets which are surplus to requirements are measured at their net realisable value. At 30 June 2005 ASIO had no assets in this situation.

Frequency

The Finance Minister's Orders require that all property, plant and equipment assets be measured at up-to-date fair values from 30 June 2005 onwards. All ASIO's assets have been revalued at 30 June 2005 to fair value. Revaluations will be performed when the fair value of an asset class differs materially from its carrying amount.

Conduct

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

Depreciation

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

Depreciation/amortisation rates (useful lives) and methods are reviewed at each balance date and necessary adjustments are recognised in the current, or current and future reporting periods, as appropriate. Residual values are re-estimated for a change in prices only when assets are revalued.

Depreciation and amortisation rates applying to each class of depreciable asset are based on the following useful lives:

	2005	2004
Buildings on freehold land	25-40 years	25-40 years
Leasehold improvements	Lease term	Lease term
Plant and equipment	3-15 years	3-15 years

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

1.12 Impairment of Non-Current Assets

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

1.13 Intangibles

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

All software assets were assessed for indications of impairment as at 30 June 2005. No impairment write-down was booked.

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

ASIO Report to Parliament 2004–2005

The useful life of ASIO's software is 3 to 4 years (2003-04: 3 to 4 years).

1.14 Inventories

ASIO does not hold inventory for re-sale.

1.15 Taxation

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

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

1.16 Administered items

ASIO has no administered items.

1.17 Foreign currency

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

Associated currency gains and losses are not material.

1.18 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.

1.19 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.

1.20 Comparative figures

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

1.21 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.

1.22 Changes in accounting policy

The accounting policies used in the preparation of these financial statements are consistent with those used in 2003-04.

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

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

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

For-profit entities complying fully with AEIFRS will be able to make an explicit and unreserved statement of compliance with International Financial Reporting Standards (IFRS) as well as a statement that the financial report has been prepared in accordance with Australian Accounting Standards.

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

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

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

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

Where an entity is not able to make a reliable estimate, or where quantitative information is not known, the entity should update the narrative disclosures of the key differences in

accounting policies that are expected to arise from the adoption of AEIFRS.

The purpose of this Note is to make these disclosures.

Management of the transition to AEIFRS

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

- The ASIO Audit and Evaluation Committee oversees the transition to and implementation of AEIFRS. The Chief Finance Officer is formally responsible for the project and reports regularly to the Committee on progress against the formal plan approved by the Committee.
- The plan requires the following steps to be undertaken and sets deadlines for their achievement:
 - All major accounting policy differences between current AASB standards and AEIFRS as at 30 June 2004 were identified by 31 October 2004.
 - Identification of processes to be able to report under AEIFRS, including those necessary to enable capture of data under both sets of rules for 2004-05 was completed by 28 February 2005. This included the testing and implementation of those changes.
 - A transitional balance sheet as at 1 July 2004, under AEIFRS was completed and presented to the Audit & Evaluation Committee on 28 April 2005.
 - An AEIFRS compliant balance sheet as at 30 June 2005 was also prepared during the preparation of the 2004-05 statutory financial reports.
 - The 2004-05 balance sheet under AEIFRS will be reported to the Department of Finance and Administration in line with their reporting deadlines.
- The plan will also address the risks to successful achievement of the above objectives and include strategies to keep implementation on track to meet all deadlines.
- A consultant was engaged where necessary to assist with each of the above steps.

Major changes in accounting policy

ASIO believes the first financial report prepared under AEIFRS, i.e. at 30 June 2006, will be prepared on the basis that ASIO will be a first time adopter under AASB 1 *First time Adoption of Australian Equivalents to International Financial Reporting Standards*. Changes in accounting policies under AEIFRS are applied retrospectively, i.e. as if the new policy had always applied, except in relation to the exemptions available and prohibitions under AASB 1. This means an AEIFRS compliant balance sheet has to be prepared as at 1 July 2004. This will enable the 2005-06 financial statements to report comparatives under AEIFRS.

A first time adopter of AEIFRS may elect to use exemptions under paragraphs 13 to 25E. When developing the accounting policies applicable to the preparation of the 1 July opening balance sheet, no exemptions were applied by ASIO.

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

Property, plant and equipment

It is expected the 2005-06 *Finance Minister's Orders* will continue to require property, plant and equipment to be valued at fair value in 2005-06.

Under AEIFRS the cost of an item of property, plant and equipment includes the initial estimate of the costs of dismantling and removing the item and restoring the site on which it is located. A corresponding provision for these costs is also recognised as a liability.

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

Sales of non-current assets

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

Employee benefits

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

AEIFRS require that annual leave that is not expected to be taken within 12 months of balance date is to be discounted.

Financial Instruments

AEIFRS include an option for entities not to restate comparative information in respect of financial instruments in the first AEIFRS report. It is expected that *Finance Minister's Orders* will require entities to use this option. Therefore, the amounts for financial instruments presented in ASIO's 2004-05 primary financial statements are not expected to change as a result of the adoption of AEIFRS.

ASIO will be required by AEIFRS to review the carrying amounts of financial instruments at 1 July 2005 to ensure they align with the accounting policies required by AEIFRS. It is expected that the carrying amounts of financial instruments held by ASIO will not materially change as a result of this process.

ASIO Report to Parliament 2004–2005

Reconciliation of Impacts - AGAAP* to AEIFRS

	30 June 2005** \$ '000	30 June 2004 \$ '000
Reconciliation of Departmental Equity		
Total Departmental Equity under AGAAP	60,647	36,949
Adjustments to accumulated results	745	969
Adjustments to other reserves	702	–
Total Equity under AEIFRS	62,094	37,918
Reconciliation of Departmental Accumulated Results		
Total Departmental Accumulated Results under AGAAP	(4,801)	(5,328)
Adjustments:		
Assets - carrying value	1,487	1,487
Depreciation	(742)	(519)
Total Accumulated Results under AEIFRS	(4,056)	(4,360)
Reconciliation of Departmental Reserves		
Total Departmental Reserves under AGAAP	8,734	9,496
Adjustment:		
Asset Revaluation Reserve	702	–
Total Departmental Reserves under AEIFRS	9,436	9,496
Reconciliation of Departmental Contributed Equity		
Total Departmental Contributed Equity under AGAAP	56,714	32,781
Adjustments:	–	–
Total Contributed Equity under AEIFRS	56,714	32,781
Reconciliation of Net surplus / (deficit) from ordinary activities for year ending 30 June 2005		
Net surplus / (deficit) from ordinary activities under AGAAP	526	
Adjustments:		
Depreciation and amortisation	(223)	
Net surplus / (deficit) from ordinary activities under AEIFRS	303	

* Australian General Accepted Accounting Principles

** 30 June 2005 total represents the accumulated impacts of AEIFRS from the date of transition

Note 3: Events occurring after reporting date

There were no events occurring after reporting date which had an effect on the 2005 financial statements.

	2005 \$'000	2004 \$'000
Note 4: Operating revenues		
<i>Note 4A: Revenues from Government</i>		
Appropriations for outputs	137,456	98,210
Total revenues from Government	137,456	98,210
<i>Note 4B: Goods and services</i>		
Goods	57	13
Services	2,567	1,980
Total sales of goods and services	2,624	1,993
Provision of goods to:		
Related entities	29	6
External entities	28	7
Total sales of goods	57	13
Provision of services to:		
Related entities	2,387	1,757
External entities	180	223
Total rendering of services	2,567	1,980
Cost of sales of goods	57	13
<i>Note 4C: Interest revenue</i>		
Interest on deposits	–	–
<i>Note 4D: Net gains from sale of assets</i>		
Infrastructure, plant and equipment:		
Proceeds from disposal	403	976
Net book value of assets disposed	(431)	(959)
Net gain/(loss) from disposal of infrastructure, plant and equipment	(28)	17
TOTAL proceeds from disposals	403	976
TOTAL value of assets disposed	(431)	(959)
TOTAL net gain from disposal of assets	(28)	17
<i>Note 4E: Other revenues</i>		
Resources received free of charge	1,154	836
Rent	807	604
Miscellaneous	408	404
Total other revenue	2,369	1,845

	2005 \$'000	2004 \$'000
Note 5: Operating expenses		
Note 5A: Employee expenses		
Wages and salary	54,123	44,615
Superannuation	10,066	7,086
Leave and other entitlements	1,848	2,308
Separation and redundancies	167	498
Other employee expenses	7,379	6,129
Total employee benefits expense	73,583	60,636
Workers compensation premiums	506	432
Total employee expenses	74,089	61,068
Note 5B: Suppliers' expenses		
Goods	4,978	3,639
Services	44,187	23,925
Operating lease rentals *	6,954	5,647
Total supplier expenses	56,119	33,211
* These comprise minimum lease payments only.		
Goods from related entities	585	127
Goods from external entities	4,393	3,512
Services from related entities	15,815	7,950
Services from external entities	28,372	15,975
Note 5C: Depreciation and amortisation		
<i>Depreciation</i>		
Other infrastructure, plant and equipment	9,337	6,788
Buildings	105	93
Total Depreciation	9,442	6,881
<i>Amortisation</i>		
Intangibles	1,182	859
Total Depreciation and amortisation	10,624	7,739
The aggregate amount of depreciation or amortisation expensed during the reporting period for each class of depreciable assets are as follows:		
Buildings	105	93
Leasehold improvements	1,654	1,480
Plant and equipment	7,683	5,308
Intangibles	1,182	859
Total	10,624	7,739

	2005 \$'000	2004 \$'000
Note 5D: Write down of assets		
<i>Financial assets</i>		
- Bad and doubtful debts expense	17	13
- Foreign exchange variations	5	12
<i>Non-financial assets</i>		
- Plant and equipment written off at stocktake	176	526
- Plant and equipment - other	28	150
- Plant and equipment - revaluation decrement	697	-
- Intangibles written off at stocktake	135	-
Total	1,058	700
Note 6: Borrowing costs expense		
Note 6: Borrowing costs expense		
Leases	5	24
Note 7: Financial assets		
Note 7A: Cash		
Cash at bank and on hand	18,299	7,216
All cash is recognised as a current asset		
Note 7B: Receivables		
Goods and services	2,502	1,165
Less provision for doubtful debts	(17)	-
	2,485	1,165
GST receivable from the Australian Taxation Office	1,232	681
Total receivables (net)	3,717	1,846
All receivables are current assets		
Receivables (gross) are aged as follows:		
Not overdue	3,381	1,489
Overdue:		
- less than 30 days	94	275
- 30 to 60 days	20	36
- 60 to 90 days	3	3
- more than 90 days	219	43
	3,717	1,846

	2005 \$'000	2004 \$'000
Note 8: Non-financial assets		
<u>Note 8A: Land and buildings</u>		
Freehold land - at 2004-05 valuation (fair value)	1,500	1,340
Buildings on freehold land - at cost	–	121
Accumulated depreciation	–	–
	–	121
Buildings on freehold land - at 2004-05 valuation (fair value)	2,019	2,009
Accumulated depreciation	–	–
	2,019	2,009
Leasehold improvements - at cost	58	3,578
Accumulated amortisation	–	(340)
	58	3,239
Leasehold improvements - at 2004-05 valuation (fair value)	19,854	9,841
Accumulated amortisation	–	–
	19,854	9,841
Total	23,431	16,550
<u>Note 8B: Infrastructure, plant and equipment</u>		
Plant and equipment - at cost	11,119	8,930
Accumulated depreciation	(511)	(317)
	10,608	8,613
Plant and equipment - at 2004-05 valuation (fair value)	27,202	19,731
Accumulated depreciation	(1)	–
	27,201	19,731
Total	37,809	28,344

Note 8C: Analysis of property, plant and equipment

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

Item	Land \$'000	Buildings \$'000	Buildings- Leasehold Improvements \$'000	Total Buildings \$'000	Total Land & Buildings \$'000	Plant & Equipment \$'000	Total \$'000
As at 1 July 2004							
Gross book value	1,340	2,130	13,419	15,549	16,889	28,661	45,550
Accumulated depreciation / amortisation	–	–	(340)	(340)	(340)	(317)	(657)
Opening net book value	1,340	2,130	13,079	15,210	16,549	28,344	44,893
Additions							
by purchase	–	1	8,908	8,909	8,909	18,973	27,882
from acquisition of operations	–	–	–	–	–	–	–
Net revaluation increment/(decrement)	160	(7)	(406)	(413)	(253)	(1,205)	(1,458)
Depreciation/ amortisation expense	–	(105)	(1,654)	(1,759)	(1,759)	(7,683)	(9,442)
Recoverable amount write-downs	–	–	–	–	–	–	–
Disposals							
from disposal of operations	–	–	–	–	–	–	–
other disposals	–	–	(15)	(15)	(15)	(620)	(635)
As at 30 June 2005							
Gross book value	1,500	2,019	19,912	21,932	23,431	38,321	61,752
Accumulated depreciation / amortisation	–	–	–	–	–	(512)	(512)
Closing Net book value	1,500	2,019	19,912	21,932	23,431	37,809	61,240

ASIO Report to Parliament 2004–2005

Table B - Assets at valuation

Item	Land \$'000	Buildings \$'000	Buildings- Leasehold Improvements \$'000	Total Buildings \$'000	Total Land & Buildings \$'000	Plant & Equipment \$'000	Total \$'000
As at 30 June 2005							
Gross value	1,500	2,019	19,854	21,873	23,373	27,202	50,576
Accumulated depreciation / amortisation	–	–	–	–	–	(1)	(1)
Net book value	1,500	2,019	19,854	21,873	23,373	27,201	50,575
As at 30 June 2004							
Gross value	1,340	2,009	9,841	11,850	13,190	19,762	32,952
Accumulated depreciation / amortisation	–	–	–	–	–	–	–
Net book value	1,340	2,009	9,841	11,850	13,190	19,762	32,952

Table C - Assets held under finance lease

Item	Land \$'000	Buildings \$'000	Buildings- Leasehold Improvements \$'000	Total Buildings \$'000	Total Land & Buildings \$'000	Plant & Equipment \$'000	Total \$'000
As at 30 June 2005							
Gross value	–	–	–	–	–	–	–
Accumulated depreciation/ amortisation	–	–	–	–	–	–	–
Net book value	–	–	–	–	–	–	–
As at 30 June 2004							
Gross value	–	–	–	–	–	326	326
Accumulated depreciation/ amortisation	–	–	–	–	–	–	–
Net book value	–	–	–	–	–	326	326

Table D - Assets under construction

Item	Buildings \$'000	Buildings- Leasehold Improvements \$'000	Total Buildings \$'000	Total Land & Buildings \$'000	Plant & Equipment \$'000	Total \$'000
Gross value at 30 June 2005	–	–	–	–	1,660	1,660
Gross value at 30 June 2004	–	–	–	–	1,446	1,446

	2005 \$'000	2004 \$'000
Note 8D: Intangible assets		
Purchased computer software - at cost	8,934	9,012
Accumulated amortisation	(5,689)	(5,941)
Total	3,245	3,071

Table A - Reconciliation of the opening and closing balances of intangibles

Item	Computer Software \$'000
As at 1 July 2004	
Gross book value	9,012
Accumulated depreciation / amortisation	(5,941)
Opening Net book value	3,071
Additions by purchase	1,491
Depreciation/ amortisation expense	(1,182)
Write-downs	(135)
As at 30 June 2005	
Gross book value	8,934
Accumulated depreciation / amortisation	(5,689)
Closing Net book value	3,245

Note 8E: Other non-financial assets

Prepayments	1,299	2,398
All other non-financial assets are current assets		

Note 9: Interest bearing liabilities

Finance lease commitments		
Payable:		
within one year	-	121
in one to five years	-	-
Minimum lease payments	-	121
Deduct: future finance charges	-	(6)
Net Lease liability	-	115
Lease liability is represented by:		
Current	-	115
Non-current	-	-
Net lease liability	-	115

	2005 \$'000	2004 \$'000
Note 10: Provisions		
Note 10A: Employee provisions		
Salaries and wages	221	1,792
Leave	16,607	14,789
Superannuation	47	278
Other	399	160
Aggregate employee benefit liability and related on-costs	17,274	17,019
Current	7,898	8,733
Non-current	9,376	8,286
Note 10B: Accommodation Leases		
Provision for make good	2,520	1,487
Lease incentives	854	–
Total accommodation leases	3,374	1,487
Note 11: Payables		
Trade creditors	6,497	3,853
Operating lease rentals	8	1
Total supplier payables	6,505	3,854
Supplier payables are represented by:		
Current	6,505	3,853
Non-Current	–	–
Total supplier payables	6,505	3,853
Settlement is usually made net 30 days.		

Note 12: Equity

Analysis of equity

Item	Accumulated Results		Asset Revaluation Reserves		Contributed Equity		TOTAL EQUITY	
	2005 \$'000	2004 \$'000	2005 \$'000	2004 \$'000	2005 \$'000	2004 \$'000	2005 \$'000	2004 \$'000
Opening balance as at 1 July	(5,328)	(4,649)	9,496	6,279	32,781	22,144	36,949	23,774
Net surplus/(deficit)	526	(679)	n/a	n/a	n/a	n/a	526	(679)
Net revaluation increments/ (decrements)	n/a	n/a	(762)	3,217	n/a	n/a	(762)	3,217
Transactions with owner:								
Contributions by owner:								
Appropriations (equity injection)	–	–	–	–	23,933	10,637	23,933	10,637
Closing balance as at 30 June	(4,801)	(5,328)	8,734	9,496	56,714	32,781	60,646	36,949

	2005 \$'000	2004 \$'000
Note 13: Cash flow reconciliation		
Reconciliation of Cash per Statement of Financial Position to Statement of Cash Flows:		
Cash at year end per Statement of Cash Flows	18,299	7,216
Statement of Financial Position items comprising above cash: 'Financial Asset - Cash'	18,299	7,216
Reconciliation of net surplus (deficit) to net cash from operating activities:		
Net surplus (deficit)	526	(679)
Depreciation/amortisation	10,624	7,739
Net write down of non-financial assets	1,036	676
Net loss on disposal of assets	28	(17)
(Increase)/Decrease in receivables	(1,872)	185
(Increase)/Decrease in prepayments	1,099	(1,770)
Increase/(Decrease) in provisions	1,887	455
Increase/(Decrease) in employee provisions	256	3,237
Increase/(Decrease) in supplier payables	2,652	(670)
Net cash from/(used by) by operating activities	16,236	9,157

Note 14: Contingent liabilities and assets

Quantifiable contingencies

The Schedule of Contingencies reports contingent liabilities in respect of claims for damages/costs of \$200,000 (2004: \$40,000). The amount represents an estimate of ASIO's liability based on precedent cases. ASIO is defending the claims.

Unquantifiable contingencies

At 30 June 2005, ASIO had a number of legal claims against it. ASIO has denied liability and is defending the claims. It is not possible to estimate amounts of any eventual payments that may be required in relation to these claims.

Note 15: Executive remuneration

The number of executive officers who received or were due to receive a total remuneration of \$100,000 or more:

	2005	2004
\$100 000 to \$109 999	–	1
\$120 000 to \$129 999	1	–
\$130 000 to \$139 999	1	–
\$140 000 to \$149 999	1	–
\$150 000 to \$159 999	–	1
\$160 000 to \$169 999	1	2
\$170 000 to \$179 999	1	1
\$180 000 to \$189 999	4	2
\$190 000 to \$199 999	4	3
\$200 000 to \$209 999	1	–
\$210 000 to \$219 999	1	2
\$220 000 to \$229 999	2	3
\$230 000 to \$239 999	2	1
\$250 000 to \$259 999	2	–
\$270 000 to \$279 999	1	–
\$280 000 to \$289 999	–	1
\$320 000 to \$329 999	1	–
\$360 000 to \$369 999	–	1
\$370 000 to \$379 999	–	–
\$390 000 to \$399 999	–	1
\$400 000 to \$409 999	1	–

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

\$5,245,105 \$4,328,270

The aggregate amount of separation and redundancy/termination benefit payments during the year to executive officers shown above.

\$95,893 \$415,878

Note 16: Remuneration of auditors

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

The fair value of audit services provided was:

\$60,000 \$54,500

Included in the amount above, is an amount of auditor remuneration relating to the 2005-06 financial statements audit, arising from work done on the opening balance sheet to be prepared under Australian equivalents to International Financial Reporting Standards.

No other services were provided by the Auditor-General.

Note 17: Average staffing levels

Full time staff equivalent (FSE) at the end of the year

2005 2004

894 770

Note 18: Financial instruments

Note 18A: Interest rate risk

Financial Instrument	Notes	Floating Interest Rate		Fixed Interest Rate Maturing In			Non-Interest Bearing		Total		Weighted Average Effective Interest Rate	
		2005 \$'000	2004 \$'000	1 year or less	1 to 5 years	> 5 years	2005 \$'000	2004 \$'000	2005 \$'000	2004 \$'000	2005 %	2004 %
Financial Assets												
Cash at bank	7A	-	-	-	-	-	18,299	7,216	18,299	7,216	-	-
Receivables for goods and services (gross)	7B	-	-	-	-	-	2,502	1,165	2,502	1,165	n/a	n/a
Total		-	-	-	-	-	20,801	8,381	20,801	8,381		
Total Assets							87,800	59,424				

Financial Liabilities												
Finance lease liabilities	9	-	-	115	-	-	-	-	-	-	115	7.08
Trade creditors	11A	-	-	-	-	-	6,497	3,853	6,497	3,853	n/a	n/a
Total		-	-	115	-	-	6,497	3,853	6,497	3,968		
Total Liabilities							27,153	22,475				

Note 18B: Net fair values of financial assets and liabilities

		2005	2005	2004	2004
		Total carrying amount	Aggregate net fair value	Total carrying amount	Aggregate net fair value
	Note	\$'000	\$'000	\$'000	\$'000
Departmental Financial Assets					
Cash at bank	7A	18,299	18,299	7,216	7,216
Receivables for goods and services (net)	7B	2,502	2,502	15	15
Total Financial Assets		20,801	20,801	7,230	7,230
Financial Liabilities (Recognised)					
Finance lease liabilities	9	–	–	115	115
Trade creditors	11	6,497	6,497	3,702	3,702
Total Financial Liabilities (Recognised)		6,497	6,497	3,817	3,817

Financial assets

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

Previously, AAS 33 was interpreted as excluding financial assets due from related parties such as other Commonwealth agencies. This was because the agreement between the two parties was considered not strictly "contractual". The Department of Finance and Administration now considers these items as "contractual" and, hence, financial instruments. Comparative figures have been adjusted to reflect this.

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.

Previously, AAS 33 was interpreted as excluding financial liabilities due to related parties such as other Commonwealth agencies. This was because the agreement between the two parties was considered not strictly "contractual". The Department of Finance and Administration now considers these items as "contractual" and, hence, financial instruments. Comparative figures have been adjusted to reflect this.

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

Note 18C: 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 19: Appropriations

Note 19A: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund (CRF) for Ordinary Annual Services Appropriation

Particulars	Total
Year Ended 30 June 2005	\$
Balance carried forward from previous year	7,215,726
Correction of prior year error in disclosure	(1,739,000)
Unspent prior year appropriation - ineffective s31 (A)	(5,476,479)
Adjusted balance carried forward	247
Appropriation Act (No.1) 2004-2005	134,729,000
Appropriation Act (No.3) 2004-2005	2,727,000
Sub-total 2004-05 Annual Appropriation	137,456,247
Appropriations to take account of recoverable GST (FMAA s304)	4,104,750
Annotations to 'net appropriations' (FMAA s31)	–
30 June 2005 - variation - s31 (B)	8,254,149
Total appropriations available for payments	149,815,146
Cash payments made during the year (GST inclusive)	136,686,529
Balance of Authority to draw cash from the CRF for Ordinary Annual Services Appropriations	13,128,617

<i>Represented by:</i>	
Cash at bank and on hand	13,128,370
Add: Receivables - GST receivable from customers	223,000
Add: Receivables - GST receivable from the ATO	1,231,248
Less: Payables - GST payable to suppliers	(1,454,248)
Total	13,128,370

Particulars	Total
Year ended 30 June 2004 (comparative period)	\$
Balance carried from previous year	5,350,305
Appropriation Act (No.1) 2003-2004	95,236,000
Appropriation Act (No.3) 2003-2004	2,974,000
Appropriations to take account of recoverable GST (FMAA s304)	4,521,011
Annotations to 'net appropriations' (FMAA s31)	4,823,000
Total appropriations available for payments	112,904,316
Payments made during the year (GST inclusive)	105,688,590
Balance carried to the next period	7,215,726

- (A) Under Section 31 of the *Financial Management and Accountability Act 1997* (the FMA Act), the Minister for Finance may enter into a net appropriation agreement with an agency Minister. Appropriation Acts No.s 1 and 3 (for the ordinary annual services of government) authorise the supplementation of an agency's annual net appropriation by amounts received in accordance with its Section 31 Agreement, eg. receipts from charging for goods and services.

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

An officer for and on behalf of the Minister for Finance and Administration and an officer for and on behalf of the Director-General of Security executed our Section 31 Agreement covering the period 1 July 1999 to 30 June 2004. Whilst we have operated and recorded Section 31 monies as though an effective agreement existed, we did not have an express delegation or authority for signing the agreement, with the result that our agreement was ineffective and we did not have control over Section 31 monies.

Our current Section 31 Agreement was made on 27 June 2005 between our acting Director-General of Security as the delegate of the Attorney-General and an officer of the Department of Finance and Administration as the delegate of the Minister for Finance. Acknowledging the ineffectiveness of the prior agreement, this agreement was varied on 27 June 2005, with effect from 1 July 2004 to capture retrospectively all monies that were subject to an ineffective prior agreement. This variation does not validate past breaches of section 83 of the Constitution.

Accordingly:

- Amounts disclosed in previous financial years as available for spending under our departmental outputs appropriations up to 30 June 2004 were overstated by \$21,840,000; - of this amount, \$5,476,479 was unspent as at 30 June 2004 and was incorrectly reflected in the balance brought forward to 1 July 2004;
- the 30 June 2005 variation to our agreement increased our appropriation by the amount of affected receipts (\$24,617,670); - of this amount, \$16,364,000 is not available to be spent, being from 1999 to 2005 which has already been spent;
- in addition, spending up to and including 30 June 2004 totalling \$16,364,000 was made without the authority of the Parliament, in contravention of section 83 of the Constitution; and
- therefore, also resulting in a breach of section 48 of the FMA Act.

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

Particulars	99-00 \$'000	00-01 \$'000	01-02 \$'000	02-03 \$'000	03-04 \$'000	Sub-total \$'000	04-05 \$'000	Total \$'000
Receipts affected	2,320	2,973	9,645	2,079	4,823	21,840	2,778	24,618
Unspent	2,320	624	1,339	(1,900)	3,093	5,476	2,778	8,254
Amount spent without appropriation	–	2,349	8,306	3,979	1,730	16,364	–	16,364

- (B) This amount represents receipts of \$24,618,000 appropriated by the variation of 30 June 2005, less the amount spent prior to 2004-05 of \$16,364,000.

ASIO Report to Parliament 2004–2005

Note 19B: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund (CRF) for Other than Ordinary Annual Services Appropriation

Particulars	Total
Year Ended 30 June 2005	\$
Balance carried from previous year	–
Correction of prior year error in disclosure	1,739,000
Appropriation Act (No.2) 2004-2005	18,011,000
Appropriation Act (No.4) 2004-2005	5,922,000
Appropriations to take account of recoverable GST (FMAA s30A)	2,050,091
Total appropriations available for payments	27,722,091
Cash payments made during the year (GST inclusive)	22,551,000
Balance of Authority to draw cash from the CRF for Other than Ordinary Annual Services Appropriations	5,171,091

<i>Represented by:</i>	
Cash at bank and on hand	5,171,091
Total	5,171,091

Particulars	Total
Year ended 30 June 2004 (comparative period)	\$
Balance carried from previous year	–
Appropriation Act (No.2) 2003-2004	9,129,000
Appropriation Act (No.4) 2003-2004	1,508,000
Total appropriations available for payments	10,637,000
Payments made during the year (GST inclusive)	10,637,000
Balance carried to the next period	–

Note 19C: Special Accounts

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 2005 and 30 June 2004, both special accounts had nil balances and there were no transactions debited or credited to them. For the periods 2003-04 and 2004-05 ASIO has not used section 39 of the FMA Act regarding investments in respect of this Special Account.

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. For the periods 2003-04 and 2004-05 ASIO has not used section 39 of the FMA Act regarding investments in respect of this Special Account.

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. For the periods 2003-04 and 2004-05 ASIO has not used section 39 of the FMA Act regarding investments in respect of this Special Account.

Note 20: Specific Payment Disclosures

	2005	2004
	\$	\$
No payments were made during the reporting period under the 'Defective Administration Scheme'. (2004: Two payments made).	<u>Nil</u>	<u>182,600</u>
No payments were made under s73 of the <i>Public Service Act 1999</i> during the reporting period. (2004: No payments made)	<u>Nil</u>	<u>Nil</u>
No waivers of amounts owing to the Commonwealth were made pursuant to subsection 34(1) of the <i>Financial Management and Accountability Act 1997</i> . (2004: No payments made)	<u>Nil</u>	<u>Nil</u>

Note 21: Reporting of Outcomes**Note 21A: Total Cost/Contribution of Outcomes (Whole of Government)**

	Total	
	2005 \$'000	2004 \$'000
Total expenses	142,326	103,702
Costs recovered from provision of goods and services to the non-government sector	208	230
Other external revenues		
Revenue from disposal of assets	403	976
Other	2,369	1,845
Goods and services revenue from related entities	2,416	1,764
Net cost / (contribution) of outcome	136,930	98,888

Note 21B: Major Revenues and Expenses by Output Group

	Total	
	2005 \$'000	2004 \$'000
Operating Revenues		
Revenues from government	137,456	99,046
Sale of goods and services	2,624	1,992
Other non-taxation revenues	2,772	1,984
Total operating revenues	142,852	103,023
Operating expenses		
Employees	74,089	61,068
Suppliers	56,119	33,211
Depreciation and amortisation	10,624	7,739
Other	1,489	1,659
Total operating expenses	142,321	103,678

PART 5: APPENDICES



APPENDIX A

MEMBERSHIP OF THE PARLIAMENTARY JOINT COMMITTEE ON ASIO, ASIS AND DSD

The Parliamentary Joint Committee on ASIO, ASIS and DSD comprises seven members, three from the Senate and four from the House of Representatives. Four members are from the Government and three from the Opposition. Membership of the PJCAAD during the reporting year was:

Hon. David Jull, MP (Chair)	Liberal Party, QLD
Mr Stewart McArthur, MP	Liberal Party, VIC
Senator Sandy Macdonald	National Party, NSW
Senator Alan Ferguson	Liberal Party, SA
Hon. Kim Beazley, MP (until 28/01/05)	Australian Labor Party, WA
Mr Leo Macleay, MP (until 31/08/04)	Australian Labor Party, NSW
Mr Anthony Byrne, MP (from 7/03/05)	Australian Labor Party, VIC
Hon. Duncan Kerr, SC, MP (from 9/12/04)	Australian Labor Party, TAS
Senator the Hon. Robert Ray	Australian Labor Party, VIC

APPENDIX B CRITICAL INFRASTRUCTURE AND NATIONALLY VITAL ASSETS

Criticality	Definition
Vital	Alternative services and/or facilities cannot be provided by States or Territories or nationally. Loss or compromise will result in abandonment or long-term cessation of the asset.
Major	If services and/or facilities are severely disrupted, major restrictions will apply and the service/facility will require national assistance.
Significant	Services and/or facilities will be available but with some restrictions and/or responsiveness and/or capacity compared to normal operation. The service may be provided within the State or Territory but reliance may also be placed on other States or Territories.
Low	Services and/or facilities can be provided within State, Territory or nationally with no loss of functionality.

Table 13: National criticality categories

Sectors
Food
Health
Energy
Utilities
Transport
Manufacturing
Communications
Banking & Finance
Government Services
Icons and Public Gatherings

Table 14: Critical infrastructure sectors

APPENDIX C WORKPLACE DIVERSITY STATISTICS

Group	Total staff ¹	Women	Race/ Ethnicity ²	ATSI ³	PWD ⁴	Available EEO data ⁵
SES (excluding DG)	20	5	0	0	0	20
Senior Officers ⁶	187	50	19	0	2	176
A05 ⁷	329	157	56	1	4	292
A01–4 ⁸	368	192	46	3	8	348
IT01–2 ⁹	50	8	8	0	0	44
ENG1–2 ¹⁰	1	0	0	0	0	1
Total	955	412	129	4	14	881

¹Based on staff salary classifications recorded in ASIO's human resource management information system.

²Previously non-English speaking background.

³Aboriginal and Torres Strait Islander.

⁴People with a disability.

⁵Provision of EEO data is voluntary.

⁶Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications.

⁷ASIO Officer Grade 5 translates to APS Level 6 and includes Generalist Intelligence Officers (GIO).

⁸Translates to span the APS 1 to 5 classification levels. GIO trainees are included in this group (equivalent to APS Level 3).

⁹Information Technology Officers Grades 1 and 2.

¹⁰Engineers Grades 1 and 2

Table 15: Representation of designated groups within ASIO at 30 June 2005

Group	June 2001	June 2002	June 2003	June 2004	June 2005
Women ¹	40	40	42	41	43.14
Race/Ethnicity ²	6	11	12	11	14.64
ATSI ³	0.3	0.75	0.74	0.41	0.45
PWD ⁴	3	4	4	2	1.59

¹Percentages of women based on total staff; percentages for other groups based on staff for whom EEO data was available.

²Previously NESB: non-English speaking background.

³Aboriginal and Torres Strait Islander.

⁴People with a disability.

Table 16: Percentage representation of designated groups in ASIO 2001–05.

APPENDIX D

ASIO SALARY CLASSIFICATION STRUCTURE AT 30 JUNE 2005

ASIO MANAGERS			
SES Band 3	\$159 798		minimum point
SES Band 2	\$126 305		minimum point
SES Band 1	\$105 935		minimum point
AEO 3	\$93 888		
AEO 2	\$85 174	to	\$93 888
AEO 1	\$75 104	to	\$81 069
GENERALIST INTELLIGENCE OFFICERS			
GIO	\$51 630	to	\$65 413
ASIO OFFICERS			
ASIO Officer 5	\$57 348	to	\$65 413
ASIO Officer 4	\$47 298	to	\$51 630
ASIO Officer 3	\$41 246	to	\$44 443
ASIO Officer 2	\$36 322	to	\$40 178
ASIO Officer 1	\$32 194	to	\$35 489
ASIO ITOs			
SITOA	\$93 888		
SITOB	\$85 174	to	\$93 888
SITOC	\$75 104	to	\$81 069
ITO2	\$57 348	to	\$65 413
ITO1	\$44 443	to	\$51 630
ASIO ENGINEERS			
SIO(E)5	\$95 379		
SIO(E)4	\$85 174	to	\$93 888
SIO(E)3	\$75 104	to	\$81 069
SIO(E)2	\$57 348	to	\$65 413
SIO(E)1	\$44 443	to	\$51 630

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

AAU	Advanced Analytical Unit	ICC	Intelligence Coordination Committee
ACS	Australian Customs Service	IDETF	Inter-Departmental Emergency Task Force
AFP	Australian Federal Police	ISP	Internet Service Provider
AGCTC	Australian Government Counter-Terrorism Committee	JCLEC	Joint Centre for Law Enforcement Cooperation
AGCTPC	Australian Government Counter-Terrorism Policy Committee	JCTICU	Joint Counter-Terrorism Intelligence Coordination Unit
AIC	Australian Intelligence Community	JI	Jemaah Islamiyah
ASEAN	Association of South East Asian Nations	MAL	Movement Alert List
ASIC	Aviation Security Identity Card	NCTC	National Counter-Terrorism Committee
ASIS	Australian Secret Intelligence Service	NII	National Information Infrastructure
AUSTRAC	Australian Transaction Reports and Analysis Centre	NSC	National Security Committee
CBRN	Chemical Biological Radiological and Nuclear	NSH	National Security Hotline
C/CSP	Carrier/Carriage Service Provider	NTAC	National Threat Assessment Centre
CIP	Critical Infrastructure Protection	ONA	Office of National Assessments
CTITP	Counter-Terrorism Intelligence Training Program	PM&C	Department of the Prime Minister and Cabinet
DFAT	Department of Foreign Affairs and Trade	RMU	Research and Monitoring Unit
DIGO	Defence Imagery and Geospatial Organisation	SCH	Security Checking Handbook
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs	SCNS	Secretaries Committee on National Security
DIO	Defence Intelligence Organisation	TSU	Technical Support Unit
DOTARS	Department of Transport and Regional Services	WMD	Weapons of Mass Destruction
DSD	Defence Signals Directorate		
DSTO	Defence Science and Technology Organisation		
FBI	Federal Bureau of Investigation		

COMPLIANCE INDEX

Annual Report requirement	Page
Advertising and market research	60
Assumed identities	57
Certified agreements and AWAs	59
Consultants and contractors	68–9
Contact details	Back cover
Corporate governance	53–4
Disability strategy	63
Environmental performance	67
External scrutiny	55–7
Financial performance	11
Financial statements	71–104
Fraud control measures	56–7
Freedom of Information	27
Glossary	111
Index	113
Internet home page and Internet address for report	Back cover
Letter of transmittal	iii
Management of human resources	58–63
Occupational health and safety	63
Organisational structure	7
Outcome and Output structure	9
Overview of agency	vii
Performance pay	59
Purchasing	67
Report on performance	13–49
Resource tables by outcomes	11
Review by Director-General	3–5
Roles and functions	vii
Staffing statistics	58–9, 109–10
Summary resource table	11
Table of contents	v
Warrants issued under section 34D of the <i>ASIO Act 1979</i>	41–2

GENERAL INDEX

A

Abu Sayyaf Group, 18, 21, 55
 Administrative Appeals Tribunal (AAT), 28
 accountability, 55–7
 Advanced Analytical Unit (AAU), 44
 advertising costs, 60
 al-Qa'ida, 15, 18, 19, 20, 21, 55
 al-Zarqawi, Abu Mus'ab, 3, 4, 15, 55
 al-Zawahiri, Ayman, 3, 15
 ammonium nitrate, 4, 30–1
 Ansar al-Islam, 21
 ANZAC ceremony, Gallipoli, 47
 appeal mechanisms, 21, 28, 31
 archival records, access to, 27–8
Archives Act 1983, 27
 Armed Islamic Group (GIA), 21, 55
 Asbat al-Ansar, 21
 ASIO staff. *See* staff
 assumed identities, 56
 Attorney-General, accountability to, 53, 55
 audio counter-measures. *See* technical surveillance counter-measures
 audit and evaluation, 56–7
 Australian agencies, liaison with. *See* liaison: with Australian agencies
 Australian Federal Police, liaison with. *See* liaison with police
 Australian Government Counter-Terrorism Committee (AGCTC), 39
 Australian Government Counter-Terrorism Policy Committee (AGCTPC), 39
 Australian Nationalist Workers' Union, 22
 Aviation Security Identity Cards, 3, 5, 30, 31, 64
 Ayub, Abdul Rahim, 18

B

Ba'aysir, Abu Bakar, 3, 15, 18
 Bali bombing, 15
 Baxter Detention Centre, 22
 Bin Laden, *See* al-Qa'ida
 biological warfare. *See* WMD
 border security. *See* visa checking
 Brigitte, Willy, 15, 19, 41
 building management, 67
 business continuity, 64
 business focus, 55
 Business Liaison Unit, 5, 24

C

chemical, biological, radiological or nuclear (CBRN) threats. *See* WMD
 client survey, 11
 communal violence, 20
 communications. *See* information management
 compensation claims, 63
 complaints about ASIO, 55
 compliance index, 112
 computer attack. *See* critical infrastructure protection
 computer exploitation. *See* warrant operations – computer access
 consultants and contractors, 65, 66, 69
 Contact Reporting Scheme, 29–30
 controversial visitors. *See* visa checking – recommendations against entry
 corporate governance, 53–4
Corporate Plan 2002–2006, vii, 54
 corporate planning, 54
 cost recovery, 32
 counter-espionage, 4, 22
 counter-intelligence. *See* security of ASIO
 counter-proliferation. *See* WMD

Counter-Terrorism Intelligence Training Program, 46

Critical Infrastructure Advisory Council, 24

critical infrastructure protection, 23–4, 108

cyber security, 24

D

disability strategy, 63

E

ecologically sustainable development, 67

Egyptian Islamic Jihad, 21

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

engineering development. *See* technical capabilities and development

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

environmental performance, 67

equal employment opportunity (EEO). *See* workplace diversity

equipment testing. *See* security equipment testing and standards

e-security. *See* critical infrastructure protection

espionage. *See* counter-espionage

evaluation. *See* audit and evaluation

external scrutiny. *See* accountability

F

Flood Report. *See* *Report of the Inquiry into Australian Intelligence Agencies*

foreign intelligence collection (Output 4), 49

foreign interference, 22

foreign liaison. *See* liaison with overseas services

fraud control, 56–7

G

glossary, 111

H

Habib, Mamdouh, 19

Hasan, Abdul Rakib, 21, 41

Hicks, David, 19

human resource management. *See* staff

human source intelligence, 39

Husin, Azahari bin, 18

I

illegal arrivals. *See* unauthorised arrivals

Indonesia, 15, 17, 18

industrial democracy. *See* staff – workplace relations

Industry Assurance Advisory Groups, 24

industry, engagement with, 24

information management, 53, 61, 64

information security. *See* security of ASIO

infrastructure. *See* critical infrastructure protection

Inquiry into Security Issues, 29, 66

Inspector-General of Intelligence and Security (IGIS), 4, 25, 27, 29, 42, 53, 55, 56, 58, 66

Inter-Agency Security Forum, 29, 65

Interdepartmental Emergency Task Force (IDETF), 39

international training and development, 46

investigative priorities, 17, 22, 25, 40

Iraq, 3, 15, 17, 19, 20, 22

Islamic Army of Aden, 21

Islamic Movement of Uzbekistan, 21

issue-motivated groups, 22

J

Jaish-e-Mohammed, 21
Jakarta bombing, 3, 15, 17
Jamiat ul-Ansar, 21, 55
Jemaah Islamiyah, 15, 17–18, 21, 55
Jewish community, threats to, 20
Joint Counter-Terrorism Intelligence
Coordination Unit (JCTICU), 45
Joint Intelligence Group, 38

K

Khazaal, Belal, 19, 21

L

Lashkar-e Jhangvi, 21
Leghaei, Mansour, 21
legislation (Commonwealth):
– *Anti-terrorism Act (No. 3) 2004*, 36
– *Archives Act 1983*, 27
– *Australian Security Intelligence
Organisation Act 1979*, vii, 21, 36,
38, 40, 41, 42, 46
– *Australian Security Intelligence
Organisation Amendment Act 2004*,
36–7
– *Crimes Act 1914*, 57
– *Criminal Code Act 1995*, 17, 21, 41
– *Criminal Code Amendment
(Terrorist Organisations) Act 2004*,
55
– *Freedom of Information Act 1982*,
27
– *National Security Information
(Criminal Proceedings) Act 2004*, 37
– *National Security Information
(Criminal Proceedings) Amendment
(Application) Act 2005*, 37
– *Passports Act 1938*, 36
– *Telecommunications Act 1997*, 42
– *Telecommunications (Interception)
Act 1979*, 37, 38, 40, 42
– *Telecommunications (Interception)
Amendment (Stored
Communications) Act 2004*, 37, 43
legislation (NSW):

– *Law Enforcement and National
Security (Assumed Identities) Act
1998*, 57

liaison with Australian agencies:

- Australian Federal Police: 15, 16,
18, 19, 39, 43, 45
- Australian intelligence agencies, 15,
16, 29, 38, 45, 46, 62
- Other Commonwealth agencies, 11,
15–16, 21, 23–7, 29–33, 38–9, 43–
5, 62
- State/territory police, 11, 18, 20, 22,
23, 38–40, 43–5

liaison with overseas agencies, 46–7

- approved agencies, 46
- ASIO liaison posts, 46
- conferences, 46

locksmith accreditation, 32

Lodhi, Faheem Khalid, 19, 21, 41

M

management and accountability. *See*
corporate governance

media policy, 57

Moro Islamic Liberation Front (MILF),
18

Movement Alert List (MAL). *See* visa
checking

Muslim community, threats to, 20

N

National Anti-Terrorism Exercise
(NATEX). *See* counter-terrorism
exercises

National Archives of Australia, 27, 28

National Counter-Terrorism Committee
(NCTC), 38

National Counter-Terrorism Plan
(NCTP), 23, 38

National Critical Infrastructure
Database, 23

National Information Infrastructure
Protection. *See* critical infrastructure
protection

National Intelligence Group (NIG), 38

National Security Committee of
Cabinet (NSC), 29, 53, 55

National Security Hotline, 3, 45
National Threat Assessment Centre (NTAC), 15–16,
nuclear proliferation. *See* WMD

O

occupational health and safety, 63
– compensation claims, 63
Olympic Games:
– Athens 2004 Games, 47
– Beijing 2008 Games, 47
open source information, 44
organisational structure chart, 7
Outcome structure, 9
output performance, 13–49
outputs:
– enabling, 51–69
– executive, 53–5
– foreign intelligence, 49
– price of, 11
– protective security advice, 29–34
– security intelligence analysis & advice, 15–28
– security intelligence investigation & capability, 35–48
overseas posts. *See* liaison with overseas agencies – ASIO liaison posts

P

Parliamentary committees, 55–6
Parliamentary Joint Committee on ASIO, ASIS and DSD, 4, 42, 53, 55, 56, 68, 69, 107
passport cancellations, 3, 19, 21
people management. *See* staff
performance pay, 59
performance reporting, 13–48
personnel security assessments, 30–1
– adverse and qualified assessments, 31
– ammonium nitrate, 4, 30–1
– appeals, 31
– Aviation Security Identity Cards, 3, 30, 31
– Commonwealth Games, 31

– flight crew, 3, 30, 31
– physical security, 32
– shipping crew, 30
police, liaison with. *See* liaison with Australian agencies
politically motivated violence (PMV):
– foreign influenced, 17–20
– local, 22
polygraph trial, 29
proliferation. *See* WMD
proscribed organisations, 4, 21
protective security advice (Output 2), 29–34
Protective Security Coordination Centre (PSCC), 29, 32, 39, 45
protective security risk reviews. *See* protective security advice
protest activity. *See* politically motivated violence – local
public, ASIO contact with, 57
public speeches, 57
purchasing, 64, 68

R

recruitment. *See* staff – recruitment
Report of the Inquiry into Australian Intelligence Agencies, 38, 55, 62, 67
Research and Monitoring Unit, 44
Richardson, Dennis, 4
risk-management advice. *See* protective security advice
Roche, Jack, 15

S

Salafist Group for Call and Combat, 21, 55
salary classification structure, 110
secondments, 62
Secretaries Committee on National Security (SCNS), 29
sectoral threat assessments, 24
security assessments:
– illegal arrivals. *See* visa checking
– personnel. *See* personnel security assessments

Security Checking Handbook. *See* visa checking – *Security Checking Handbook*

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

Security Construction and Equipment Committee (SCEC), 32–3

security environment, 3, 17, 23, 35

Security Equipment Catalogue, 33

security equipment testing and standards, 33

Security Management Plan 2005–09, 65

security of ASIO, 65–6

Security Status Report, 29

Senate Legal and Constitutional Legislation Committee, 5, 56

special events, 45

Staff:

- attrition rate, 60
- performance pay, 59
- profile, 60
- recruitment, 58, 60
- salary classification structure, 110
- security clearances, 60, 65–6
- Staff Association, 53, 54
- statistics, 59
- training and development, 5, 39, 46, 61–2
- workplace diversity, 62–3
- workplace relations, 59

surveillance, 35, 40

sweeps. *See* technical surveillance counter-measures

T

technical capabilities and development, 35, 39, 43

Technical Support Unit, 39

technical surveillance counter-measures, 33

telecommunications interception, 42–3

terrorism. *See* politically motivated violence

terrorist groups, proscription of. *See* proscribed organisations

Terrorist Threat Advisory Group, 16

terrorist training, 17, 18, 19

Thomas, Joseph, 20, 21

threat assessments, 3, 11, 16

Tongeren, Jack Van, 22

Top, Noor Din, 18

Top Secret certification, 32

training and development. *See* staff – training and development

Trusted Information Sharing Network (TISN), 24

U

Ul-Haque, Izhar, 19, 21

unauthorised arrivals. *See* visa checking

V

vetting. *See* personnel security assessments

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

visa checking, 3, 25–6

- Movement Alert List (MAL), 25–6
- recommendations against entry, 3, 25
- unauthorised arrivals, 3, 25

W

warrant operations:

- approvals, 40
- emergency, 40
- questioning and detention powers, 3, 41–2

weapons of mass destruction (WMD), 20, 22

website, 57

Wood, Douglas, 20

women in ASIO, 62

Workplace Agreement, 59

workplace diversity, 62, 109

Z

Zarqawi. *See* al-Zarqawi, Abu Mus'ab

Zawahiri. *See* al-Zawahiri, Ayman

