Australian Security Intelligence Organisation

REPORT TO PARLIAMENT 2005–2006

ISSN 0815-4562
ISBN 0- 9751485-3-2

Produced and printed by the Australian Security Intelligence Organisation.

Australian Government
Australian Security
Intelligence Organisation

Director-General of Security

Reference Number: eA1004090
September 2006

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 2006.

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

CONTENTS

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;

wherever those activities may occur.

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. ASIO analyses and assesses information to produce security intelligence and advice that informs and supports government decision-making. ASIO does not investigate lawful protest activity, nor does it undertake criminal investigations. ASIO officers have no power of arrest.

ASIO is the only Australian intelligence agency that is authorised to collect foreign intelligence within Australia. ASIO does this only 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. ASIO's *Corporate Plan 2007–2011* is scheduled for completion at the end of 2006.

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 version of this report in the Parliament within 20 sitting days of receipt.

ASIO produces a classified and an 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

Australia and Australians remained at threat from a range of sources in 2005–06. While the threat of terrorism from Islamic extremists posed the most immediate danger, other sources of threat – including from espionage; violent protest, nationalist and racist violence; and acts of foreign interference – also persisted.

The security environment remained complex and dangerous with no sign that the range of security threats to Australians at home or abroad is abating.

- An Australian died as a result of the London bombings on 7 July 2005.
- Terrorists struck again in Bali on 1 October 2005, killing themselves and 20 others, including four Australians. Extremists in South East Asia continue to see Australians as a target and more attacks are likely.
- Frequent terrorist attacks in Iraq resulted in the death or injury of many Iraqi citizens. An Australian security guard was killed in a bomb attack on 8 June 2006.
- Australians were also injured in the attacks in London and Bali and in an attack in Egypt.
- We saw the threat from previously unknown or unexpected sources – including the emergence of so-called home-grown extremists – come to prominence in London in July 2005 and Canada in May 2006.

Two individuals in Australia were the subject of litigation on terrorism-related charges: Joseph Thomas in connection with his links to al-Qa'ida; and Faheem Lodhi in connection with planning for a terrorist attack in Australia.

Other individuals in Australia are facing terrorism-related charges, including those arrested following the joint operational activity by ASIO and police in Sydney and Melbourne in November 2005 and March 2006.

In response to the continuing threat to Australian interests and the heavy demands placed on ASIO's resources, the Prime Minister appointed Mr Allan Taylor, AM to undertake a *Review of ASIO Resourcing*.

On 16 October 2005 the Prime Minister and the Attorney-General announced the Government's commitment of additional resources to ASIO that will see the Organisation grow to 1860 staff by 2010–11. This commitment gives ASIO the certainty it needs to plan for the future and to grow in a planned manner.

OUR ROLE

ASIO's focus in 2005–06 remained the prevention of harm to Australians and Australian interests from threats to security, particularly the threat of terrorism from Islamic extremists.

ASIO continued to grow and build its capabilities. However, even with additional resources, there can be no guarantees that intelligence always will be available that will allow us to prevent those who would do us harm from achieving their objectives.

OUR STRATEGIES

In 2005–06 ASIO continued to work with other Australian agencies and with international liaison partners to maximise our effectiveness in protecting Australians from security threats.

ASIO continued to provide advice to other Australian agencies in the form of:

- 2 216 threat assessments for Australian interests here and abroad, including for special events of national significance and for foreign interests in Australia
  - ~ compared to 2 003 in 2004–05.
- 53 147 visa security assessments
  - ~ with 12 people denied entry to Australia based on ASIO advice (one applicant applied on two occasions and was the subject of two separate assessments);
  - ~ compared to 52 417 visa assessments and 12 people denied entry in 2004–05.
- Counter-terrorism checking
  - ~ 62 285 for the aviation sector (Aviation Security Identification Cards and pilot/trainee pilot checks);
  - ~ 9 448 for Maritime Security Identification Cards;
  - ~ 7 428 for access to ammonium nitrate; and
  - ~ 56 149 for the Commonwealth Games.
- 17 908 assessments for access to national security information resulting in no adverse or qualified assessments
  - ~ up from 17 017 assessments resulting in 1 qualified assessment last year.
- Other adverse security assessments
  - ~ resulting in the refusal to issue or cancellation of eight Australian passports by the Minister for Foreign Affairs.
- Protective security advice
  - ~ valued at just over $1million, an increase of 11 percent over last year.
- Support for litigation
  - ~ ASIO was involved in 48 separate litigations (prosecutions, appeals, civil proceedings and administrative appeals proceedings) compared to 20 last year.
- Closer engagement with the business community
  - ~ the Business Liaison Unit was established in October 2005;
  - ~ the Director-General delivered four speeches to business forums.

ASIO's operating environment has become increasingly challenging.

To remain effective ASIO has needed to develop new and innovative investigative and analytical techniques as well as sophisticated technological solutions. ASIO's effectiveness was enhanced further by:

- joint operations with Australian law enforcement agencies, including in Sydney and Melbourne in November 2005 and March 2006 which resulted in 22 individuals facing terrorism-related charges;
- building links with community groups;
- the improved use of technology;
- appropriate use of special powers for the highest priority investigations, including one questioning warrant;
- continuing our lead house role in connection with telecommunications interception policy and capabilities to ensure the ongoing effectiveness of this method of intelligence collection;

- working with Australian and international partners to develop leading-edge technologies;
- expanding our covert surveillance capacity and making greater use of technology; and
- expanding and strengthening our network of international liaison offices.

In addition, ASIO has boosted its complex analysis capabilities by:

- establishing a new branch that brings together work units with a strategic analytical focus; and
- working with international liaison partners to leverage off their knowledge and expertise.

ASIO also continued to make a valuable contribution to:

- the investigation of covert activity conducted by foreign entities, including espionage and attempts to interfere in the lives of people in Australia or in political processes here or overseas;
- the collection of foreign intelligence in Australia at the request of the Minister for Foreign Affairs or the Minister for Defence;
- countering the efforts of state and non-state actors to acquire materials or technology in Australia that could be used in the production or use of weapons of mass destruction; and
- countering the efforts of foreign states that seek to intimidate people in Australia who they see as dissidents.

OUR BUDGET AND PEOPLE

ASIO's budget for 2005–06 was $181.099m compared to $142.449m in 2004–05. It is set to grow to $233.059m in 2006–07.

As at 30 June 2006 ASIO had 1110 staff. ASIO has continued to attract high calibre applicants across a range of 'job families'. In order to ensure we recruit, train and integrate the right staff at the right time ASIO developed a strategy based on:

- increased resources in our recruitment, staffing and training areas, including the use of task forces in periods of peak activity;
- innovative advertising campaigns aimed at attracting high calibre applicants from various backgrounds to fill a range of vacancies, including Intelligence Officers, Intelligence Analysts, Surveillance Officers and a range of technical, information technology, legal and administrative staff; and
- training programs to build skills in leadership and management, analysis, intelligence operations, languages and a range of corporate functions.

ASIO will continue to invest heavily in developing the range of skills and knowledge needed across all the functions of the Organisation.

ACCOUNTABILITY AND OVERSIGHT

ASIO's activities continued to attract high levels of media, community, business and Parliamentary attention.

The Inspector-General of Intelligence and Security continued his program of inspections and monitoring of ASIO's investigative work and special powers operations. He also undertook a number of inquiries into complaints made by members of the public against ASIO. Where the Inspector-General identified administrative or procedural shortcomings, ASIO initiated corrective action. Based on the various monitoring, inspection and inquiry activities undertaken by the Office of the Inspector-General of Intelligence and Security in 2005–06, Mr Carnell was satisfied that there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or the human rights of Australians.

In 2005–06 I appeared before Parliamentary committees on a range of matters, including in connection with:

- inquiries by the Parliamentary Joint Committee on Intelligence and Security into the training and recruitment activities of the intelligence agencies, reviews of the listing or re-listing of groups as terrorist organisations, the review of the questioning and detention provisions of the ASIO Act, as well as providing a number of private briefings;
- the inquiry by the Joint Public Accounts and Audit Committee into aviation security in Australia;
- the inquiry by the Senate Legal and Constitutional Legislation Review Committee into the provisions of the Anti-Terrorism Bill (Number 2) 2005; and
- the inquiry by the Security Legislation Review Committee on the anti-terrorism legislation enacted since 2002.

I also delivered 19 public and other statements addressing issues such as:

- the continuing threat of terrorism and other threats to security;
- the risk that we will not always have prior intelligence about threats to enable preventative action;
- the importance of ASIO acting ethically and strictly within the legislative framework; and
- the value of ASIO's cooperative work with Australian and international partners.

These statements are available on ASIO's website.

LOOKING AHEAD

In 2006–07 ASIO will continue to grow in a planned manner and will push ahead with the task of recruiting and training a new generation of intelligence professionals. We will strive to continue to be an employer of choice.

While growth will inevitably impose some strains on the Organisation, arrangements are in place to ensure ASIO remains effective.

Given the persistent and pervasive threat environment we face, ASIO will remain focused on its core functions of protecting Australia and Australians from threats to security.

ASIO has a key role to play in providing advice to agencies responsible for ensuring the security of the 2007 Asia Pacific Economic Cooperation forum – the most significant security event ever held in Australia.

In addition to fulfilling our responsibilities to ASIO's traditional clients we will continue to strive to enhance cooperation with the business sector and other parts of the Australian community.

Paul O'Sullivan
Director-General

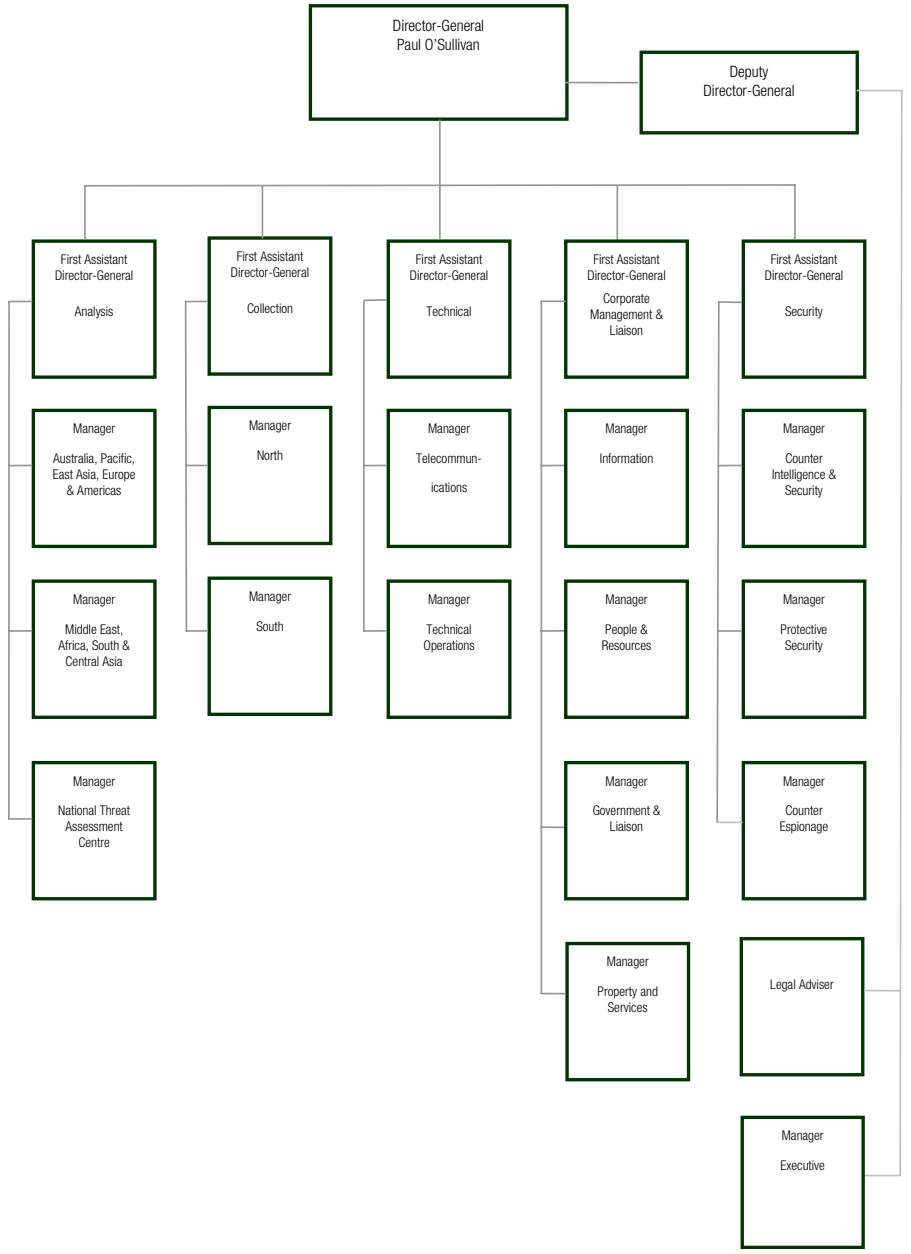


Figure 1: ASIO corporate structure as at 30 June 2006

AGENCY OVERVIEW

ORGANISATIONAL STRUCTURE

On 16 October 2005, the Prime Minister announced that the Government had accepted recommendations for the further growth of ASIO following the independent *Review of ASIO Resourcing* conducted by Mr Allan Taylor, AM.

Mr Taylor's review was extensive. He concluded that the period of growth ASIO had experienced since September 2001 should be continued for it to reach a staffing level of 1860 by 2010–11.

The forecast growth in staff and technical capability will substantially strengthen ASIO's capabilities in security intelligence collection and assessment and in all other areas relevant to its ongoing functions. Additional resources will enhance critical enabling infrastructure, such as information technology systems and accommodation.

In December 2005, ASIO established a small implementation team to support the Executive's strategic planning for continuing growth. The planning process established the need to expand ASIO's management structure early to facilitate the effective management of growth. Consequently, on 1 July 2006 ASIO moved to a nine division structure as outlined in Figure 2.

This provides an Organisational structure with clear points of focus for meeting expectations of ASIO's performance across all areas of security intelligence priority and in critical accountability or enabling areas. Some new areas were created, including:

- a division to address threats from espionage and foreign interference that complements the focus on terrorism and other extremist activity;
- new branch structures to respond to ASIO's increased involvement in legal matters. One branch with direct alignment to the intelligence business deals with the complex issue of utilising intelligence in legal proceedings; another branch forms part of an expanded team of in-house lawyers; and
- the creation of an Information Division to provide more effective knowledge management, robust delivery of critical enabling infrastructure and information systems and better IT capability to enhance security intelligence outcomes.

Other areas have retained existing structures or have been strengthened:

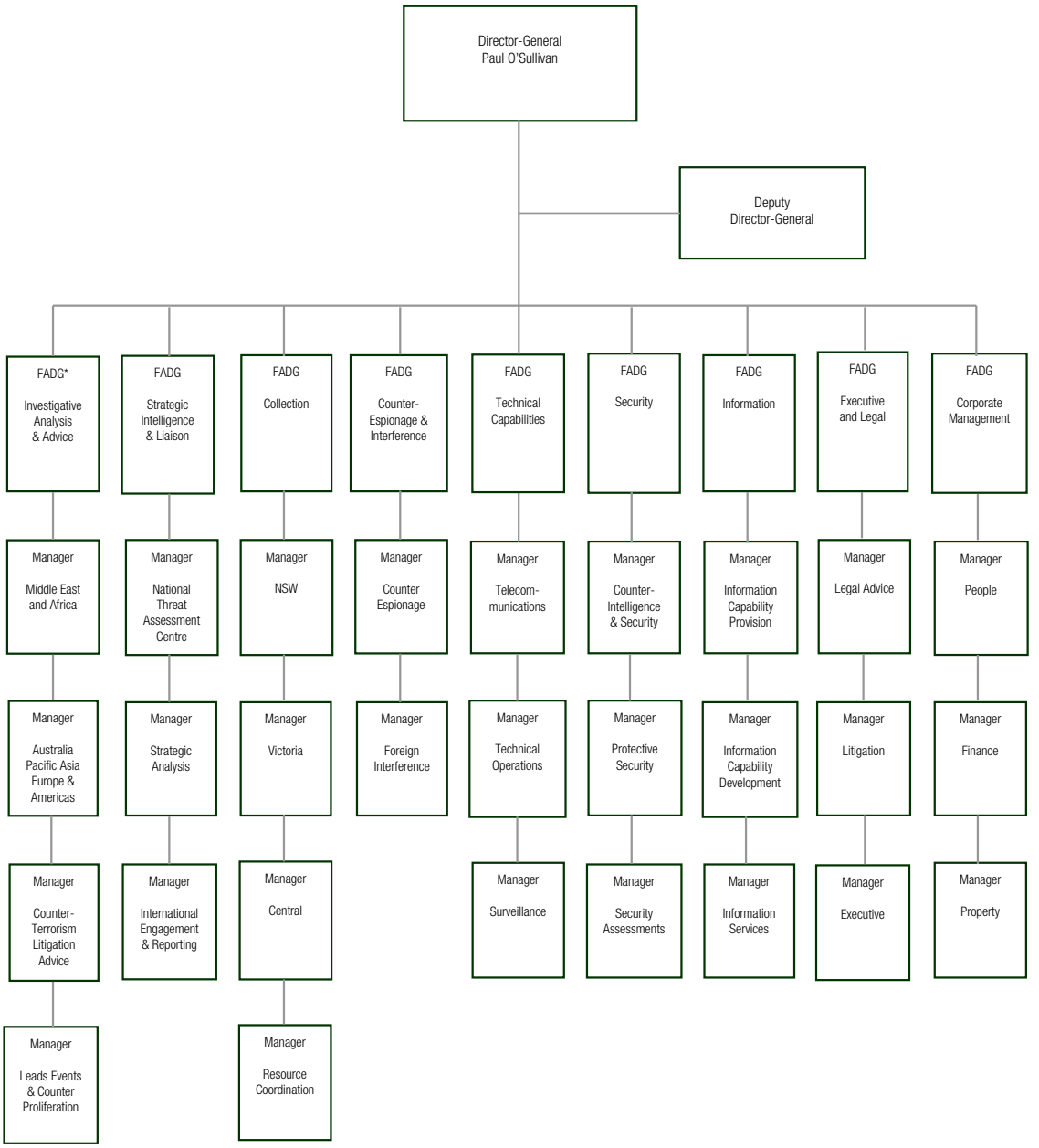
- the National Threat Assessment Centre retains its focus to provide comprehensive advice on threats to Australian interests, but remains well connected within ASIO and the rest of the Australian Intelligence Community;
- Collection Division branches have been adjusted to reflect the national coverage provided by this division; and
- Security Division retains the effective concept of a 'one-stop-shop' for security advice, continuing the connection between advice to government and advice to business.

Not all positions in this structure will be filled from 1 July 2006. ASIO plans to grow at a rate of around 170 net per year. This presents a challenge in a tight employment market. In response, ASIO has enhanced staff recruitment and improved processes to meet the challenge while maintaining high standards.

ASIO has recognised the challenge of recruiting the right people at the right time – to grow while continuing to meet critical business priorities.

- the structure ASIO will grow into by 2010–11 has been finalised; and
- progress against targets is regularly reviewed by ASIO's Executive.

The Cabinet Implementation Unit in the Department of the Prime Minister and Cabinet will report on progress.



* First Assistant Director-General (FADG)

Figure 2: ASIO corporate structure at 1 July 2006

OUTCOME AND OUTPUT STRUCTURE

In support of the Government policy aim of '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, published 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 2005–06 expressed in terms of total price of Outputs was $181.099m compared to $142.449m in 2004–05.

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

Output	Actual 2004–05 $m	Estimated 2005–06 $m	Actual 2005–06 $m	% of total funding
Output Group 1: Security Intelligence	142.449	180.761	181.099	100.0

Table 1: Price of ASIO's Outputs

CLIENT SATISFACTION

ASIO conducts an annual survey of key Commonwealth, State and Territory clients. In 2005–06 our clients noted the contribution ASIO's reporting made to widening knowledge and understanding of the threats we face, and informing agencies' decisions on resource deployment and risk management.

Commonwealth clients commented on the uniqueness of ASIO's reporting, which brings together information from diverse sources. Information obtained from ASIO's international partners offers a particularly valuable perspective.

Police clients commented that ASIO is the most authoritative and relevant commentator on security issues impacting on Australia. ASIO product remains distinctive in terms of its depth and breadth and makes a significant contribution to the understanding by police of all aspects of the security environment. Police clients commented favourably on the timeliness of ASIO reporting.

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:

- **threats in Australia and to Australian interests abroad**
- **foreign-influenced and local politically motivated violence**
- **foreign interference and espionage**
- **protecting critical infrastructure**
- **deterrence action**
- **border security**
- **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.

THE GLOBAL TERRORIST THREAT

Terrorism predates the attacks on New York's twin towers on 11 September 2001. Over the past century, the world has seen a succession of terrorist campaigns in support of various ideological or nationalist causes.

The main terrorist threat globally over the past decade has been driven by an Islamist ideology that espouses 'global jihad'. This doctrine, which pre-dates the rise of al-Qa'ida, calls for its adherents to attack its enemies wherever possible.

These extremists are convinced that the United States and its allies are waging a war against Islam, they have contempt for 'apostate' Muslim regimes, and they reject liberal democracy as atheistic and decadent. Their cause is absolutist – one with which there can be no negotiation.

Al-Qa'ida – defined as a core group of terrorists who have sworn allegiance to Usama bin Laden – has been the vanguard of the international jihadist movement, first in an operational and now in more of an ideological capacity. It has planned and undertaken attacks itself, funded and facilitated attacks by others, run a sophisticated global propaganda campaign and become an inspiration to other jihadists.

Al-Qa'ida's current ability to undertake operations itself, outside certain restricted areas, is reduced. Its primary role now consists of inspiring or encouraging others to engage in terrorist acts, or to view their local insurgencies based on nationalistic or ethnic issues in global, strategic terms.

The linkages between the diverse array of terrorists and terrorist groups in the world does not form any definable organisation, nor is one needed. Formal alliances, as between al-Qa'ida and the now deceased Abu Mus'ab al-Zarqawi's al-Qa'ida in Iraq, are rare. Most linkages are based on personal connections and shared experiences – the organisational model of modern Islamic terrorism is a loose network of loose networks.

the organisational model of modern Islamic terrorism is a loose network of loose networks

Jihadi doctrine asserts the individual duty of Muslims to undertake jihad – in any country in which it is possible to do so. Adherence to the doctrine underpins the development of autonomous, largely self-sufficient 'home-grown' terrorist groups. While such autonomy imposes certain operational constraints on groups, it also makes detection by security agencies more difficult. For example, both the Madrid bombings of March 2004 and the London bombings of July 2005 were conducted by largely self-sufficient groups with a low security profile.

THREATS TO AUSTRALIAN INTERESTS

Until 2000, terrorist attacks in Australia were directed primarily against the interests of other countries, for example:

- the 1980 assassination of the Turkish Consul-General in Sydney;
- the 1982 bombings of the Israeli Consulate and Hakoah Club in Sydney; and
- the 1986 bombing of the Turkish Consulate in Melbourne.

Planning by Jack Roche in 2000, on behalf of al-Qa'ida, was directed at attacks against the Israeli Embassy in Canberra and the Consulate in Sydney.

But it is now clear Islamic extremists see Australian interests around the world and Australia itself as targets for terrorist attacks.

In 2005–06, Australians were killed or injured in terrorist attacks

In 2005–06, Australians were killed or injured in terrorist attacks:

- on 8 June 2006 in Iraq when a roadside bomb blast resulted in the death of an Australian security guard and several others;
- on 24 April 2006 two Australians were among more than 60 people injured in a triple bomb attack in the Egyptian resort town of Dahab that killed 21 people;
- on 1 October 2005, three suicide bombers in Bali detonated explosive devices killing themselves and 20 others, including four Australians; and
- on 7 July 2005 one Australian was among 56 people killed in London when four suicide bombers detonated explosive devices on three underground trains and a bus; eight Australians were among the several hundred injured.

These incidents illustrate the continuing threat to Australians globally, either directly or indirectly from terrorist attacks against a range of 'soft targets'.

Various reasons have been given by jihadists as to why Australia is a target for terrorism, including our alliance with the United States, our contribution to the War on Terror and our involvement in Afghanistan, Iraq and East Timor. But fundamentally we are identified by them as a part of the West – a 'Crusader' nation – which makes us their enemy and a legitimate target for attacks.

Public statements by al-Qa'ida's leaders and others have singled out Australia for criticism and encouraged attacks against us since 2001. In 2005–06, statements issued by senior al-Qa'ida members, including Usama bin Laden, Ayman al-Zawahiri and the now deceased Abu Mus'ab al-Zarqawi, did not specifically mention Australia but they continued to threaten attacks on allies of the United States.

However, Australian interests continued to be directly threatened in statements by other Islamic extremists associated with al-Qa'ida:

- in September 2005, a United States network aired a video statement featuring an American al-Qa'ida member, Adam Gadahn, who warned of possible future attacks on Los Angeles and Melbourne;
- al-Qa'ida in Iraq issued a statement claiming responsibility for a triple suicide bombing outside hotels in Baghdad, claiming the attack had been directed at 'American, British and Australian security companies'; and
- in November 2005, a statement posted on a jihadist website in the name of a senior al-Qa'ida operative included a call for Islamic extremists to attack a number of countries, including Australia.

While individual statements by al-Qa'ida leaders and others do not generally contain specific pointers to an attack, they do continue to resonate with extremists and provide ongoing motivation for them.

Public statements by al-Qa'ida's leaders and others have singled out Australia for criticism and encouraged attacks against us since 2001

THE NATIONAL THREAT ASSESSMENT CENTRE (NTAC)

Since May 2004 the NTAC has brought together Australian government agencies with a role in monitoring, collating and analysing all threat intelligence available to the Australian government, including:

- Australian Federal Police;
- Australian Secret Intelligence Service;
- Department of Foreign Affairs and Trade;
- Defence Intelligence Organisation;
- Department of Transport and Regional Services; and
- Office of National Assessments.

Seconded officers have on-line access to their parent agency's communications systems and databases. This allows for connectivity and coordination between agencies and provides greater assurance that all relevant information available to the Australian government is assessed and reflected in threat assessment advice.

The NTAC's 24/7 threat assessment capability also enhances ASIO's capability to disseminate advice rapidly to clients in response to security incidents in Australia and internationally.

Since May 2004 the NTAC has brought together Australian government agencies with a role in monitoring, collating and analysing all threat intelligence available to the Australian government

Subject of Assessment	2003–04	2004–05	2005–06
Australian interests abroad and within	559	427	503
Australian dignitaries	624	676	755
Diplomatic premises in Australia	36	24	22
Visiting dignitaries	480	228	162
Special events	–	37	58
Protective security	35	49	48
Vital Infrastructure		29	20
Demonstration notifications	38	56	32
Liaison threat advice		347	492
Threat analysis papers			6
Other threat assessments	245	130	118
TOTAL	2017	2003	2216

Table 2: Threat reporting issued from 2003–04 to 2005–06

The NTAC's core responsibilities involve the provision of threat assessments for:

- Australian high office holders, both in Australia and when travelling overseas;
- foreign dignitaries visiting Australia;
- in collaboration with ASIO's Critical Infrastructure Protection Directorate, threat assessments on national critical infrastructure, sites of national significance, government buildings and defence establishments;
- Australian interests abroad;
- foreign interests in Australia, such as diplomatic and consular missions;
- significant events in Australia such as the Melbourne Commonwealth Games, the G20 Finance Ministers' Meeting in November 2006 and APEC 2007; and
- significant events overseas such as the Winter Olympics in Turin in February 2006, the Soccer World Cup in Germany in June 2006 and the annual ANZAC Day commemoration at Gallipoli.

Melbourne Commonwealth Games

ASIO coordinated the collection, analysis and dissemination of security-related advice and assessments for the Commonwealth Games. NTAC threat assessments informed the security architecture that protected the infrastructure, facilities, athletes, officials and domestic and international dignitaries associated with the Games.

ASIO also assisted in developing the threat assessment capability of other Australian agencies at the tactical level. This program was seen by international observers as a model to be replicated for future events (see also page 49).

ANZAC Day 2006

The commemorations for the 91st ANZAC Day at Gallipoli passed without security incident. NTAC threat assessments assisted planning for the event by the Department of Foreign Affairs and Trade, the Department of Veterans' Affairs, the Protective Security Coordination Centre and other Commonwealth agencies.

G20 Finance Ministers' Meeting

ASIO will coordinate the collection, analysis and dissemination of security intelligence advice for the G20 Finance Ministers' Meeting, scheduled for November 2006.

APEC 2007

Between December 2006 and September 2007, Australia will host the Asia Pacific Economic Cooperation (APEC) forum. The APEC Economic Leaders' Meeting, to be held in Sydney on 8–9 September 2007, will bring together the leaders of all major Asia Pacific economies and thousands of delegates. It will be the most significant international meeting ever hosted by Australia. ASIO has provided security intelligence advice to inform APEC preparations since June 2005 and has well-established processes to satisfy the increasing demand for security intelligence as the event draws closer.

Performance

Feedback on the NTAC during its second year of operation confirms that it continues to provide an authoritative and coordinated view on threat intelligence. NTAC's product is seen as valuable and credible within the Australian official community.

ASIO also assisted in developing the threat assessment capability of other Australian agencies at the tactical level

FOREIGN INFLUENCED POLITICALLY MOTIVATED VIOLENCE

The threat of terrorism is complex and multi-faceted. Determining responsibility for a terrorist attack requires more than monitoring public statements made by terrorist leaders.

Some groups and individuals may be influenced by events overseas but appear to be largely autonomous and able to plan and conduct devastating terrorist attacks – as we saw in London in July 2005.

In some cases, terrorist training and extremist religious indoctrination has contributed to a radicalisation process over an extended period of time. In other cases, it appears the process of radicalisation has been very short – and there may be no indication that terrorist planning or attacks have been directed by extremists outside the country in question.

Determining responsibility for a terrorist attack requires more than monitoring public statements made by terrorist leaders

Responding to this dynamic threat necessitates close cooperation with other Australian government and law enforcement agencies. This cooperation has brought better coordination to major investigations and enhanced Australia's capability to respond to particular threats.

Improved coordination between agencies and the National Security Hotline has increased the volume of threat-related information passed to ASIO and other agencies.

JEMAAH ISLAMIYAH

Australia continues to be a target for Jemaah Islamiyah activities.

2005 Bali Bombings

On 1 October 2005, three suicide bombers detonated explosive devices in Bali, killing themselves and 20 others, including four Australians. More than 100 people were wounded. The bombings were directed by Noordin Mohamed Top and Azahari bin Husin and reinforced the continuing high level of threat to Australian interests in South East Asia.

Further, the backpack bombs used in the attack, along with the smaller improvised explosive devices seized during the raid on Azahari's safe house, suggests a diversification in tactics by Jemaah Islamiyah.

Jemaah Islamiyah in the region

Jemaah Islamiyah remains a serious threat and has adapted to changing circumstances.

Jemaah Islamiyah has demonstrated resilience through its exploitation of religious, social and familial networks for operational purposes.

Senior members have a history of recruiting individuals from within established networks to undertake attacks, including the bombings in Jakarta of the Marriott Hotel in August 2003, the Australian Embassy in September 2004 and the October 2002 and 2005 bombings in Bali.

These 'operational networks' have included kindred extremist groups in Indonesia such as Darul Islam and Jemaah Islamiyah-linked pesantren.

- The arrest in Indonesia of three members of the Islamic Defenders Front for providing assistance to the Noordin Top network underlines Jemaah Islamiyah's ability to draw upon individuals from kindred groups.

Jemaah Islamiyah also has formed strong alliances with elements of the Moro Islamic Liberation Front and the Abu Sayyaf Group in the Philippines and has been involved in Mindanao-based joint training programs.

Jemaah Islamiyah continues to foment and participate in violent jihad in areas of Indonesia prone to communal conflict, notably Maluku and Sulawesi.

A number of key leaders remain at large or are due to be released from custody. These include Abu Bakar Ba'asyir (who was released from Indonesian custody on 14 June 2006), Abu Rusdan, Abu Dujana, Zulkarnaen, Noordin Top, Umar Patek and Dulmatin.

Death of Azahari

The death of key bomb-maker Dr Azahari bin Husin, in an Indonesian National Police raid on 9 November 2005, did not change the threat to Australian interests in Indonesia.

SUNNI EXTREMISM IN AUSTRALIA

Other groups and individuals in Australia also adhere to the extreme interpretation of Islam that advocates violence.

Some of these are Australian-born and others have lived here for most of their lives. Some are associated with extremist groups and terrorist identities overseas and some have trained with terrorist groups in other countries. Yet other so called 'home-grown' extremists have no identifiable links overseas but use the Internet and other resources to obtain terrorism knowledge and to radicalise and reinforce their own extremist views about violence.

ASIO continued to investigate leads relating to individuals in Australia with links to overseas extremists and terrorist activity, including al-Qa'ida and like-minded groups.

Other groups and individuals in Australia also adhere to the extreme interpretation of Islam that advocates violence

OTHER INVESTIGATIONS

Iraq

The ongoing violence in Iraq continues to have an impact on the Middle East community in Australia. During 2005, in the lead-up to the elections in Iraq, tensions increased between members of the Sunni and Shia communities in Sydney, particularly in the Auburn area.

LOCAL INFLUENCED POLITICALLY MOTIVATED VIOLENCE

PROTEST VIOLENCE

ASIO worked with Federal, State and Territory police services in connection with violent protest in Australia.

ASIO also worked with overseas liaison partners in connection with transnational trends in violent protest activity.

Protests spanning three days in connection with the Forbes Global CEO Conference in Sydney saw protestors push down security fences, force the closure of several ANZ Bank branches and engage in several confrontations with police.

Australian Defence Force recruitment stalls at universities in Queensland and Victoria were subject to disruptive and damaging protests in early 2006.

NATIONALIST EXTREMISTS/RACIST EXTREMISTS

Australian Nationalist Workers' Union

The Australian Nationalist Workers' Union regained prominence when its leader Jack Van Tongeren and fellow group member Matthew Billing breached bail and absconded.

Both had been charged with offences relating to their involvement in a series of racist and graffiti attacks across Perth suburbs and planning to firebomb four Chinese restaurants in 2004.

FOREIGN INTERFERENCE AND ESPIONAGE

ASIO investigates covert activity conducted by foreign entities, 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 or others 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.

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

FOREIGN INTERFERENCE

Chinese deserters – Chen Yong Lin and Hao Fengjun

ASIO interviewed Chen and Hao and looked closely at their claims of monitoring and harassment of members of Chinese dissident groups in Australia. ASIO subsequently provided advice to the Attorney-General's Office consistent with its responsibility for matters of security.

A review by the Senate Foreign Affairs, Defence and Trade References Committee noted that ASIO cooperated to the full extent possible in regard to these matters and the Committee was satisfied with ASIO's evidence in regard to the claims made by Chen and Hao.

COUNTER-PROLIFERATION

Concerns about state acquisition of weapons of mass destruction (WMD) were fuelled by Iran's apparent intention to acquire nuclear weapons and continued claims by the Democratic People's Republic of North Korea that it has nuclear weapons. Indications that non-state entities, chiefly al-Qa'ida and other terrorist groups, as well as state actors, retain an interest in developing or acquiring chemical, biological, radiological or nuclear weapons further underlined the diversity and complexity of this threat.

ASIO's counter-proliferation work in 2005–06 was concentrated on identifying, investigating and recommending actions to prevent the exploitation of Australian products, resources or knowledge by foreign governments and non-state actors to assist in the development of WMD.

STATE-SPONSORED PROGRAMS

A major focus of ASIO's counter-proliferation investigations continued to be attempts by states to exploit Australia's industrial, technological and educational resources to gain advantage in their WMD development programs.

Australian and International Cooperation

Consistent with the whole-of-government effort on counter-proliferation, ASIO continued to participate in a number of counter-proliferation groups and to engage with a range of government departments and agencies.

ASIO also continued to work closely with liaison partners on counter-proliferation initiatives.

Our counter-proliferation effort has been enhanced by the recruitment of additional resources with further resource injections planned for 2006–07.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR AND EXPLOSIVES TERRORISM

Improvised explosive devices using home-made explosives and commercial grade explosives are currently the most common terrorist weapon. Planned, aborted or disrupted terrorist attacks against Australian interests since 2000 have all involved the use of explosives.

Although explosives are the most common terrorist weapon, there are indications of terrorist interest in chemical, biological and radiological (CBR) agents. There have been ongoing attempts by al-Qa'ida and others to acquire CBR weapons through the purchase or development of CBR-related materials, recruitment of scientists or others with technical expertise, and the acquisition of relevant information.

Recent examples of this interest have appeared in Western countries, such as the activity relating to ricin and radioactive agents in Britain in 2004.

ASIO has strengthened its capability to address extremist interest and activity relating to chemical biological, radiological, nuclear and explosives terrorism (CBRNE).

ASIO continues to provide advice to government on the CBRNE threat which guides policy development and national preparedness. ASIO is a member of the Australian Government CBRN Strategy Group that has recently drafted the National CBRN Security Strategy.

It is also a member of the Emergency Management Australia co-ordinated National CBR Working Group that provides threat briefs to first responders.

ASIO provides advice to counter-terrorism agencies to use in identifying and addressing capability gaps that require research and development to build national preparedness.

In collaboration with the Defence Intelligence Organisation and the Australian Federal Police CBRN and

A major focus of ASIO's counter-proliferation investigations continued to be attempts by states to exploit Australia's industrial, technological and educational resources

Explosives Data Centre, ASIO maintains national classified databases on CBRNE terrorism.

ASIO provided advice to government for the Council of Australian Government's review of hazardous CBR materials.

ASIO worked with the Australian Intelligence Community and police to establish the Special Weaponry Analysis Group (SWAG) where ASIO, the Defence Intelligence Organisation, Defence Science and Technology Organisation, and the Australian Federal Police CBRN and Explosives Data Centre meet regularly to discuss intelligence relating to global terrorist activity with explosives and CBRN agents.

The SWAG member agencies provide 24/7 mutual support during times of an emerging threat and following an incident.

ASIO provided advice to government for the Council of Australian Government's review of hazardous CBR materials

PROTECTING CRITICAL INFRASTRUCTURE

ASIO supports the Australian Government's national counter-terrorism planning for protection of our critical infrastructure. With the assistance and cooperation of Commonwealth, State and Territory agencies and the private sector, ASIO:

- maintains the National Critical Infrastructure Database on behalf of the National Counter-Terrorism Committee;
- analyses and advises government and private sector stakeholders on security threats to Australia's 11 critical infrastructure sectors (see Appendix B);
- produces threat assessments for critical infrastructure sectors and sub-sectors (sectoral threat assessments); and
- undertakes threat assessments for specific individual assets categorised as 'nationally vital'.

ASSESSING THE THREAT TO CRITICAL INFRASTRUCTURE

Nationally vital and sectoral threat assessments are key elements in Australia's coordinated protective security arrangements. They underpin critical infrastructure protection activities by government and support the risk context analyses undertaken by Commonwealth, State and Territory Departments and the private sector which in turn help shape business continuity planning.

During 2005–06, the ongoing process of assessment and review resulted in the release of new and updated sectoral threat assessments.

Sectoral threat assessments were prepared in consultation with relevant departments, agencies and authorities, and with the owners and operators of critical infrastructure.

ASIO will continue to revise and update threat assessments for nationally vital critical infrastructure assets.

The National Critical Infrastructure Database was reviewed and updated in consultation with Federal Government departments and all jurisdictions.

INFORMATION SHARING AND ENGAGEMENT WITH INDUSTRY STAKEHOLDERS

ASIO's critical infrastructure work relies on strong relationships with Commonwealth, State and Territory agencies and industry stakeholders. Threat assessment research and the dissemination of threat-related information are cooperative endeavours, exemplifying the whole-of-government approach.

ASIO provides assessments and other security advice directly to government operators of nationally vital assets and shares relevant information with private industry through its Business Liaison Unit.

The Business Liaison Unit was established during 2005–06 to provide a direct interface between the private sector and the Australian Intelligence Community. The unit will produce unclassified national security-related information on each industry sector in the form of Business Security Reports, which aim to assist businesses' risk-management planning processes. These reports will be disseminated directly to businesses and also will be accessible on a secure website from July 2006.

Where there is urgency, ASIO will communicate directly with infrastructure owners/operators, the Protective Security Coordination Centre and relevant police and government organisations in advance of dispatch of the written assessment.

ASIO is a member of the Critical Infrastructure Advisory Council and works with government and industry to support key established initiatives including the Trusted Information Sharing Network

The Business Liaison Unit was established during 2005–06 to provide a direct interface between the private sector and the Australian Intelligence Community

coordinated by the Attorney-General's Department.

On completion of individual sectoral threat assessments, and in accordance with National Counter-Terrorism Committee arrangements, briefings were given to representatives of the relevant sectors.

In May 2006, the Director-General addressed the National Workshop on Protecting the Food Chain, a conference held to launch the national food chain safety and security strategy. In June 2006, the Director-General addressed the Plastics and Chemicals Industry Association on *Security Issues in a Sustainable Industry*.

The National Information Infrastructure includes the electronic systems that underpin critical services infrastructure

MONITORING EMERGING THREATS TO NATIONAL INFORMATION INFRASTRUCTURE

National Information Infrastructure includes the electronic systems that underpin critical services infrastructure such as telecommunications, banking and finance, transport and distribution, energy and utilities.

ASIO, the Defence Signals Directorate and the Australian Federal Police are engaged in formal, classified, *Joint Operating Arrangements* supporting threat and vulnerability assessment and the analysis of, and the response to, critical incidents affecting the integrity of Australia's information infrastructure. A critical incident is defined as 'an attack or system failure on some part of the National Information Infrastructure that supports or underlies systems or delivery of services whose loss for more than a short period would:

- be nationally significant (i.e. the loss would be felt nationally);
- damage the economic well-being of the nation;
- seriously damage public confidence in the information infrastructure;
- threaten life or public health;
- threaten public order;
- impair national defence; or
- impair national security'.

Under the *Joint Operating Arrangements*, ASIO monitors potential threats to the National Information Infrastructure from computer network attack, where such attacks are, or may be, relevant to security. This includes the threat of computer network attack by terrorists.

ASIO is also a member of the Information Infrastructure Protection Group and the Electronic Security Coordination Group. During 2005–06, we participated in Exercise Cyber Storm, a multilateral exercise designed to test the response to complex attacks against infrastructure.

BORDER SECURITY

Australia's universal visa system is used to manage the entry of non-citizens to the country and is an essential element in the nation's overall security strategy.

The volume of ASIO's border security work continued to grow in 2005–06. ASIO remained a key source of advice for the Department of Immigration and Multicultural Affairs on border security matters, including providing security assessments on selected visa applicants and on unauthorised arrivals.

VISA SECURITY ASSESSMENTS

The Department of Immigration and Multicultural Affairs refers individuals to ASIO for security checking under Public Interest Criterion 4002 of the *Migration Act 1958*. ASIO makes an assessment on whether the entry or continued stay of individual non-citizens would pose a direct or indirect threat to security. Visa security checking processes are generally managed in order of referral from the Department of Immigration and Multicultural Affairs, taking into account agreed prioritisation issues.

The increasing complexity of the security environment and the increasing volume of intelligence (which is often incomplete) complicates the assessment process and can make it time-consuming, particularly for complex assessments. In making a security assessment ASIO takes into account all relevant information and considers the impact on security of taking or not taking prescribed administrative action before providing advice to the Department of Immigration and Multicultural Affairs.

Publicly available and classified information is used to make assessments. Factors taken into consideration include:

- the nature and type of the applicant's activities;
- the credibility of the information available to ASIO and whether it can be corroborated; and
- the honesty of the applicant.

The assessment also may include an ASIO interview of the applicant. Interviews are undertaken to accelerate the assessment process and to provide the applicant with an opportunity to resolve issues of concern.

Individuals who are not Australian citizens or holders of a valid permanent visa, special category visa or special purpose visa cannot apply to the Administrative Appeals Tribunal for review of an ASIO security assessment.

ASIO remained the key source of advice for the Department of Immigration and Multicultural Affairs on border security matters, including providing security assessments on selected visa applicants and on unauthorised arrivals

Type of entry	2001–02	2002–03	2003–04	2004–05*	2005–06*	% increase
Temporary	29 437	27 534	30 841	39 015	39 973	2.5%
Permanent	9 584	12 355	13 881	13 402	13 174	-1.7%
Total	39 021	39 889	44 722	52 417	53 147	1.4%

* From 2004–05, figures include unauthorised arrivals

Table 3: Visa security assessments 2001–02 to 2005–06

The number of assessments conducted by ASIO on individuals seeking temporary visas to enter Australia continued to increase, a trend evident since 2003–04.

Unauthorised arrivals

During 2005–06, ASIO completed 3 005 assessments on unauthorised arrivals who were applicants for a Protection Visa.

Amendments to section 65a of the *Migration Act 1958* require the Minister for Immigration to make a decision on protection visa applicants within 90 days of their application. To help the Department of Immigration and Multicultural Affairs meet the new legislative timelines ASIO established a taskforce to manage the increase in applications referred for assessment.

Visa security assessments

In 2005–06, the Department of Immigration and Multicultural Affairs denied the entry into Australia of 12 individuals – from a range of nationalities – on the basis of ASIO security assessments. The visa applicants were assessed to pose security risks due to links to politically motivated violence, terrorism or foreign intelligence services.

Initiatives

In December 2005 ASIO implemented a 24/7 border security response capability to provide continuous support to the Department of Immigration and Multicultural Affairs and Australian Customs Service. The team is the first point of contact for the Department of Immigration and Multicultural Affairs Entry Operations Centre and has enhanced inter-agency relationships and responsibilities.

ASIO and the Department of Immigration and Multicultural Affairs are working closely at the operational, policy and management levels to identify other initiatives to improve processes for managing continually increasing caseloads, improving service standards and developing policies and procedures to meet new requirements such as citizenship checking.

The number of assessments conducted by ASIO on individuals seeking temporary visas to enter Australia continued to increase, a trend evident since 2003–04

	2001–02	2002–03	2003–04	2004–05	2005–06
Security assessments	5	8 [1]	3	12 [2]	13 [3]

[1] includes one diplomat expelled on advice from ASIO

[2] includes two assessments on unauthorised arrivals

[3] two assessments related to the same individual who applied on two separate occasions

Table 4: Number of security assessments issued from 2001–02 to 2005–06 where the individual is assessed to be a risk to national security

DETERRENCE ACTION

Under section 17(1)(c) of the *ASIO Act 1979* (the Act) it is a function of ASIO to 'advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities'.

Section 17(2) of the Act states that 'it is not a function of the Organisation to carry out or enforce measures for security within an authority of the Commonwealth'.

PASSPORT CANCELLATIONS

In 2005–06 the Minister for Foreign Affairs cancelled or refused to issue eight Australian passports following the issue by ASIO of security assessments.

During the reporting period, the Administrative Appeals Tribunal resolved two review applications in respect of adverse security assessments. In one matter the assessment was upheld. In the other matter, the Tribunal had not released its ruling by the end of the reporting period.

At the end of the reporting period, 14 persons were exercising their right of review of the assessment by the Tribunal.

PROSECUTIONS

The prosecution of 24 persons for alleged terrorism-related offences was underway at the end of the reporting period. In addition, during the reporting period, the trial of Joseph 'Jack' Thomas on terrorism charges was heard.

These prosecutions drew heavily on ASIO's resources. In a number of the prosecutions subpoenas were issued on behalf of the accused.

During the reporting period, Faheem Khalid Lodhi was convicted on three of four terrorism charges. Again, conduct of this prosecution drew heavily on ASIO's resources.

ASIO also has a necessary involvement in prosecutions under subsection 34G(5) of the ASIO Act for the alleged provision of false or misleading information under a questioning warrant.

CIVIL PROCEEDINGS

ASIO can become involved in appeals and challenges through the Courts to immigration decisions based on security assessments.

In the case of Iranian cleric Mansour Leghaei, ASIO has responded to successive legal challenges to a security assessment since 2002. During the reporting period, the assessment was upheld by the Federal Court and was subsequently the subject of an appeal to the Full Federal Court.

Also instituted during the reporting period were Federal Court applications on behalf of Scott Parkin (removed from Australia at his request pursuant to section 198(1) of the *Migration Act 1958* and Mohammed Qassim Yussef Sagar and Muhammed Faisal Al Delimi (unauthorised arrivals detained on Nauru) following ASIO security assessments.

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

In 2005–06 the Minister for Foreign Affairs cancelled or refused to issue eight Australian passports following the issue by ASIO of security assessments

PROSCRIPTION

The process for proscription of a group as 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); or
- advocates the doing of a terrorist act (whether or not a terrorist act has occurred or will occur).

The listing of the Kurdistan Workers' Party on 17 December 2005 increased the total number of terrorist organisations proscribed by the Australian Government to 19

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 2005–06, ASIO recommended the proscription of the Kurdistan Workers' Party. The listing of the Kurdistan Workers' Party on 17 December 2005 increased the total number of terrorist organisations proscribed by the Australian Government to 19.

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 the 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 the 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.

Performance

In 2005–06, 68 percent of applications were finalised within 90 days, which is below the benchmark of 80 percent. This was attributable to the impact of several ongoing requests made during the previous reporting periods – which covered a broad range of issues requiring extensive research and careful assessment – and to a large number of requests received in the second half of 2005–06.

Trends

During 2005–06, we received 338 applications for access to separate items or subjects, compared to 326 in 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.

In 2005–06, 132 family requests were completed, compared to 68 in 2004–05. All of these requests were completed within the statutory benchmark period of 90 days (compared to 83 percent last year).

Several large requests from individual/non-family researchers, received in the past, continued to be processed.

The total number of folios examined during 2005–06 was 43 222 compared to 41 181 in 2004–05.

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 the National Archives.

In 2005–06, there were six internal reconsiderations. In each case the National Archives upheld the ASIO exemptions.

Applicants still dissatisfied may then appeal to the Administrative Appeals Tribunal, 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.

Parts of this performance report have been excluded from the unclassified *Report to Parliament* for reasons of national security.

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

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

During 2005–06, ASIO continued to manage and chair the Inter-Agency Security Forum (IASF) and its permanent working groups. The IASF drives development and implementation of best practice security policies and procedures across the Australian Intelligence Community and related policy departments.

The IASF has representatives from all agencies on the Secretaries' Committee on National Security and the National Security Committee of Cabinet as well as the Department of Immigration and Multicultural Affairs. The Protective Security Coordination Centre is represented to ensure security policies and procedures are applied across government where relevant and to ensure that where possible the aims and objectives of the Protective Security Policy Committee are assisted.

The IASF and its multi-agency working groups provide a consultative whole-of-government mechanism for ensuring best practice security, timely and comprehensive consideration of security issues of mutual interest and the acquisition and sharing of information about new and emerging security methods and techniques. The IASF provides a contribution to government and Australia's security – similar arrangements are rare in other countries.

ANNUAL SECURITY STATUS REPORT

ASIO's annual (classified) *Security Status Report* – completed in August 2005 – was submitted to the Department of the Prime Minister and Cabinet for consideration by the Secretaries' Committee on National Security and the National Security Committee of Cabinet.

ANNUAL SECURITY STATUS REPORTS – OVERVIEW REPORT

ASIO is tasked with providing the Secretaries' Committee on National Security with an annual overview report of the status of security in IASF member organisations. The objective of this report is to advise government on overall security and significant trends in the IASF community. The overview report went to the Secretaries' Committee on National Security in November and to the National Security Committee of Cabinet in December 2005.

POLYGRAPH TRIAL

ASIO completed a polygraph trial on behalf of the Australian Intelligence Community in 2003 – as recommended by the *Inquiry into Security Issues* in 2000 – and results of the trial were presented to the Secretaries' Committee on National Security in August 2005.

CONTACT REPORTING SCHEME

In accordance with the policies outlined in the *Australian Government Protective Security Manual*, Australian government employees are required to report suspicious, unusual, persistent or on-going contact with foreign nationals. Through the Contact Reporting Scheme ASIO seeks to identify potential threats to security by exposing attempts to seek sensitive information through unauthorised means.

Through the Contact Reporting Scheme ASIO seeks to identify potential threats to security by exposing attempts to seek sensitive information through unauthorised means

ASIO will continue to use presentations and other promotional strategies to encourage more contact reports to be submitted.

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 determine whether anything in a candidate's background or activities gives cause for security concern. In broad terms, ASIO does not assess general suitability for the access proposed, nor 'issue' security clearances; these remain the responsibility of the requesting agency.

Security assessments are based primarily on material provided by the requesting agency. However, to resolve issues of security concern, ASIO may conduct interviews or make other enquiries.

On completion of an assessment, ASIO provides advice that it does not recommend against a security clearance, or issues an adverse or qualified assessment:

- an adverse assessment is a recommendation not to grant the proposed access;
- a qualified assessment does not recommend against access, but provides information to the agency that ASIO considers may be relevant to its decision-making, and appropriate information to help agencies minimise the identified potential security risk.

In instances where ASIO has issued a qualified or adverse assessment, candidates are notified and have a right of appeal to the Administrative Appeals Tribunal.

COUNTER-TERRORISM CHECKING

Counter-terrorism security checks are limited to enquiring whether an individual has any known links to terrorism.

During 2005–06, ASIO completed over 50 percent of counter-terrorism checks inside five days.

In carrying out its counter-terrorism security checking responsibilities, ASIO maintains excellent working relationships with the regulatory authorities involved and with the Australian Federal Police.

Checks continued for people requiring access to security-controlled areas at Australian airports and for pilots and trainee pilots. Regulations initially required that all pilots undergo checking by the end of 2005; however, the deadline was extended to 31 March 2006.

Security assessments are primarily based on material provided by the requesting agency. However, to resolve issues of security concern, ASIO may conduct interviews or make other enquiries

	2003–04	2004–05	2005–06
Aviation[1]	58 147	38 466	62 285
Ammonium Nitrate	–	1 634	7 428
MSICs	–	–	9 448
Commonwealth Games	–	–	56 149
Total	58 147	40 100	135 310

[1] Aviation figures include ASICs, pilot and trainee pilot checking

Table 5: Counter-terrorism assessments

During the period, five jurisdictions commenced security checking of persons seeking access to ammonium nitrate, which can be used as an explosive.

Implementation of the Maritime Security Identification Card scheme has been slower than anticipated. The Maritime Security Identification Card scheme requires an estimated 93 000 security checks and ASIO is working closely with the Department of Transport and Regional Services and the Australian Federal Police to facilitate its introduction.

Security checking of volunteers, participants and officials for the Commonwealth Games was a high priority during 2005–06. Strong working relationships with the Victoria Police, which was responsible for Games security, and with the Melbourne 2006 Commonwealth Games Corporation, resulted in all checking being completed on time.

ASIO works closely with the APEC Taskforce on security checking arrangements for secure area access during APEC which culminates in the Leaders' Meeting in September 2007

ASIO is working closely with the APEC Taskforce on security checking arrangements for secure area access during APEC, which culminates in the Leaders' Meeting in September 2007.

No qualified or adverse security assessments were issued in relation to counter-terrorism security checking during 2005–06.

ACCESS CHECKING

There was a 5.2 percent increase in access assessments during 2005–06, in comparison with the previous year and a 61 percent increase since 2000–01 due to more people working in the counter-terrorism field who require access to classified information.

Benchmarks were not achieved during 2005–06, due to the increasing number of requests for checks and resource-sharing between access and counter-terrorism assessments. The Melbourne Commonwealth Games and flight crew checks had a particular impact.

APPEALS

There were no appeals lodged or outstanding in 2005–06.

Level of access	2000–01	2001–02	2002–03	2003–04	2004–05	2005–06
Confidential	969	1 431	1 542	1 611	1 951	2 310
Secret	5 803	6 595	7 618	9 577	9 372	10 255
Top Secret	4 335	4 329	5 112	5 018	5 694	5 343
Total	11 107	12 355	14 272	16 206	17 017	17 908

Table 6: Access assessments

	2001–02	2002–03	2003–04	2004–05	2005–06
Qualified assessments	6	3	2	1	0
Adverse assessments	3	2	0	0	0
Total	9	5	2	1	0

Table 7: Adverse and qualified personnel security assessments

PROTECTIVE SECURITY

ASIO provides protective security advice to Commonwealth departments and agencies. With the Attorney-General's authorisation, we also may advise the State and Territory governments and private sector clients on matters of national security, including in connection with critical infrastructure.

ASIO provides protective security advice on a cost-recovery basis. During the reporting period, we recovered just over $1 million for the provision of protective security advice to external clients, an 11 percent increase from last year.

TOP SECRET CERTIFICATIONS

ASIO is responsible for inspecting and certifying sites to store and handle Top Secret information. Re-certification is required every five years. During the year, 28 inspections were undertaken with 21 sites receiving certification.

The remaining seven sites required physical security improvements to reach the minimum standards required for certification.

ACCREDITATION AND TRAINING

In 2005–06 the refurbishment of ASIO's physical security testing facility was largely completed, including the replacement of obsolete equipment and the improvement of facilities to provide training and accreditation services.

ASIO participated in a review of the inter-departmental Security Construction and Equipment Committee (SCEC). The committee promotes best technical practice in the implementation of security measures by evaluating protective security products for use by Australian government agencies and providing advice on technical standards for protection of official resources and information.

Outcomes of the review included recommendations to update the SCEC mission and objectives to reflect the current security environment and suggested refinements to security equipment evaluation processes.

ASIO continued to provide accreditation to security practitioners on behalf of the SCEC in addition to the provision of protective security and risk management training:

- 18 presentations to clients on behalf of the Protective Security Coordination Centre; and
- 22 locksmiths were accredited to install, repair and maintain locking hardware for government agencies.

A major review of the SCEC security practitioners' course commenced during the year. A revised course will be implemented in 2006–07.

SECURITY EQUIPMENT

On behalf of the SCEC, ASIO evaluates security products for inclusion in the *Security Equipment Catalogue* and for use by government agencies. During the period, 97 products underwent stringent evaluation with 74 assessed as suitable for inclusion in the catalogue, including locking hardware, fencing products and movement detectors.

TECHNICAL SURVEILLANCE COUNTER-MEASURES

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

Parts of this performance report have been excluded from the unclassified *Report to Parliament* for reasons of national security.

With the Attorney-General's authorisation, we also may advise the State and Territory governments and private sector clients on matters of national security, including in connection with critical infrastructure

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**
- **special powers operations**
- **technical research and development**
- **covert surveillance**
- **monitoring and alert functions**
- **complex analysis**
- **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 – in support of Output 1 (Security Intelligence Analysis and Advice) and Output 2 (Protective Security Advice); and
- developing investigative capabilities and building partnerships within Australia and internationally.

OPERATING ENVIRONMENT

Security intelligence agencies around the world, including ASIO, must operate in a dynamic environment that continues to evolve in both its diversity and its complexity.

Subjects of investigation have become more adept at concealing their activities and intentions from security and law enforcement agencies and indeed from other members of their community.

Security intelligence agencies must anticipate potential sources of threat, including from previously unknown or unexpected sources. They also must translate the lessons drawn from past experience into future possibilities and actively seek out information that will enable the prevention of harm.

In the case of terrorists, the speed of the radicalisation process can see a person transform from being an otherwise ordinary member of the community into a person willing to engage in politically motivated violence in a short space of time. Similarly, the time taken to plan and

conduct a deadly terrorist attack can be alarmingly short, making it difficult for security and law enforcement agencies to detect and disrupt.

The challenge for intelligence agencies is to identify those who would do harm, particularly those who are intent on the indiscriminate killing of innocent civilians, and, working with other agencies, to prevent them from achieving their objectives. This necessarily involves risk-management decisions and the prioritisation of investigative tasks.

At times, intervention by intelligence and law enforcement agencies may have to occur on the basis of partial or imperfect knowledge or information, particularly when lives are at stake. While this may be necessary to ensure the protection of Australians and Australian interests, it may have implications for subsequent legal processes.

The challenge for intelligence agencies is to identify those who would do harm, particularly those who are intent on the indiscriminate killing of innocent civilians

To stay ahead of these challenges ASIO must continue to develop its intelligence collection and analytical capabilities while continuing to operate strictly within the legislative framework.

LEGISLATIVE FRAMEWORK

Anti-terrorism Act (No.2) 2005

The *Anti-terrorism Act (No.2) 2005* (the Anti-terrorism Act) commenced in December 2005 and amended the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). In particular, the Anti-terrorism Act enhanced ASIO's special powers warrant regime by clarifying the scope of computer access warrants, extending the time period of the validity of search warrants and the inspection of postal and delivery service warrants (and extending the equivalent periods for foreign intelligence collection warrants) and extending computer access warrants allowing entry on to premises.

The Anti-terrorism Act also provided ASIO with access to aircraft and vessel information, strengthened the offence for providing false or misleading information under an ASIO questioning warrant and provided that any obligations, prohibitions or restrictions imposed by a control order issued under the *Criminal Code Act 1995* would not be 'prescribed administrative action' for the purposes of Part IV of the ASIO Act.

ASIO Legislation Amendment Act 2006

The *ASIO Legislation Amendment Act 2006* amended the ASIO Act. It responded to a number of recommendations of the Parliamentary Joint Committee on ASIO, ASIS and DSD (now the Parliamentary Joint Committee on Intelligence and Security) which were made in November 2005. The Committee's recommendations concerned the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act containing ASIO's questioning and detention powers in relation to terrorism. Warrants issued under Division 3, Part III of the ASIO Act permit ASIO to question, and in limited circumstances, detain a person where there are reasonable grounds for believing that doing so will substantially assist the

collection of intelligence in relation to a terrorism offence.

The amendments extended the existing sunset provision and review by the Committee by 10 years to require review by 22 January 2016 and to provide that Division 3 ceases to have effect on 22 July 2016. The amendments also strengthened and clarified rights under the warrant regime, clarified the role of the prescribed authority and how information is to be recorded and pointed to the legal bases for judicial review.

The ASIO Legislation Amendment Bill 2006 was introduced into the House of Representatives on 29 March 2006, and passed the House on 11 May 2006. The Bill received assent on 21 June 2006.

INTELLIGENCE COLLECTION

ASIO conducts its investigations in accordance with legislation, guidelines issued by the Attorney-General and internal procedures and protocols which require that the level of any intrusion into the privacy of individuals must be commensurate with the assessed level of threat. More intrusive methods of investigation are used only in cases when they are justified by the magnitude of the threatened violence, the likelihood it will occur and the immediacy of the threat.

In most cases, investigations are resolved through less intrusive means. ASIO has a rigorous internal regulatory and approvals framework that governs the conduct of investigations. ASIO investigations are subject to external oversight and review by the Inspector-General of Intelligence and Security (see page 61).

ASIO's intelligence collection work is governed by the priorities determined by ASIO's Intelligence Coordination Committee (see page 57). The Intelligence Coordination Committee monitors the security environment and makes adjustments to resource allocations within a risk-management framework.

MANAGEMENT ARRANGEMENTS

In response to the emerging challenges of the security environment, in January 2006, ASIO's Collection Division was restructured to comprise three geographically defined branches managed by Senior Executive Service officers in Sydney, Melbourne and Canberra.

A fourth branch – Collection Resource Coordination managed from Sydney – was established to provide for the more flexible national coordination of specialised resources.

The increased number of Senior Executive officers within Collection Division – including those based outside Canberra – allows for a closer focus by senior staff on the management of complex operational and organisational issues.

The increased number of Senior Executive officers within Collection Division – including those based outside Canberra – allows for a closer focus by senior staff on the management of complex operational and organisational issues

COLLECTION ACTIVITIES

A major joint investigation with the Australian Federal Police and New South Wales Police in Sydney resulted in the arrest of ten individuals who were charged under sections 11.5(1) and 101.6 of the *Criminal Code Act 1995*.

A joint ASIO, Australian Federal Police and Victoria Police investigation was conducted in Melbourne. In concert with the Sydney investigation, coordinated entry and search operations were conducted on 8 November 2005, resulting in the arrest by the Australian Federal Police and Victoria Police of nine individuals, all of whom were charged under the *Criminal Code Act 1995*. A tenth Melbourne-based individual was arrested in Sydney during the operation, and a further three individuals were arrested and charged with similar offences in March 2006.

ASIO worked closely with Federal, State and Territory police forces to reduce the threat of politically motivated or communal violence

ASIO worked closely with Federal, State and Territory police forces to reduce the threat of politically motivated or communal violence, particularly in connection with:

- the 2006 Commonwealth Games;
- the Forbes CEO Conference in Sydney in August and September 2005;
- the communal violence around Cronulla and environs in late 2005; and
- right-wing nationalist extremist and racist extremist issues in Western Australia.

Developing our engagement with the Australian community

ASIO continued to increase its contact with members of the community. This enhanced dialogue assists ASIO to carry out its functions.

Community engagement supplements warning systems already in place, including the National Security Hotline and work performed by other departments.

The Community Contact Program

ASIO has implemented a program of engagement with leading members of the Islamic community.

Similarly, ASIO engages with the leaders of the Jewish community across Australia.

Improved use of technology to identify and investigate emerging threats

Being at the leading edge of technological developments continues to be central to the ability of ASIO to achieve its objectives.

SPECIAL POWERS – WARRANT 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 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.

Proposals to use special powers are subject to rigorous internal consideration and approvals at a senior level. Documentation is reviewed by senior lawyers in ASIO's legal area before the Director-General gives approval to request a warrant from the Attorney-General.

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

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

Questioning 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 this 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 one questioning warrant issued in 2005–06. This warrant did not authorise detention.

The following information is provided in accordance with the reporting requirements of section 94(1A) 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: 1
- The total number of warrants issued during the year under section 34D: 1
- The number of warrants issued during the year that met the requirement in paragraph 34D(2)(a) (about requiring a person to appear before a prescribed authority): 1
- 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: 4 hours, 20 minutes.
- The number of warrants issued during the year that met the requirement in paragraph 34D(2)(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: 1 person appeared before 1 prescribed authority.

Proposals to use special powers are subject to rigorous internal consideration and approvals at a senior level

The Inspector-General of Intelligence and Security – or a member of his staff – attended during ASIO's questioning of the individual under warrant. The Inspector-General reported that the questioning was conducted in a proper and professional manner. Further detail is provided in the Inspector-General's Annual Report, which is located at www.igis.gov.au.

TELECOMMUNICATIONS INTERCEPTION

Regulatory framework

The *Telecommunications (Interception and Access) Act 1979* empowers ASIO to intercept telecommunications under warrants issued by the Attorney-General. To facilitate interception, the *Telecommunications Act 1997* requires that all carriers and carriage service providers (C/CSPs) – including Internet service providers (ISPs) – give such help as is reasonably necessary to, among other things, safeguard national security.

C/CSPs, at their cost, are required to develop, install and maintain interception capabilities unless specifically exempted, and, on a cost-recovery basis, to develop, install and maintain delivery capabilities to enable the intercepted communications to be transmitted to ASIO's monitoring facilities. ASIO must develop and maintain its own processing and monitoring capabilities.

The Telecommunications (Interception and Access) Act 1979 empowers ASIO to intercept telecommunications under warrants issued by the Attorney-General

Commercial environment

Since 1 July 1997 the Australian Communications and Media Authority has issued licences to 207 carriers. Approximately 160 carriers provide telecommunications services in the Australian market. There are some 1 569 CSPs registered with the Telecommunications Industry Ombudsman. Of these, approximately 975 are listed as ISPs.

Technological environment

With the ongoing introduction of diverse and publicly accessible technology by the telecommunications industry, the volume of data to be captured and processed is growing. A single telecommunications channel may include voice, video, documents, e-mail and executable programs and the security risks associated with capturing such data – which can

include hidden malicious programs – are increasing.

Telecommunications Interception Policy

ASIO participated in the development of legislation impacting on interception, including legislation to implement recommendations of the Blunn Review. As a result, amendments were made to the *Telecommunications (Interception) Act 1979,* now the *Telecommunications (Interception and Access) Act 1979*.

'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. ASIO develops technical specifications, negotiates statements of compliance with C/CSPs, manages interception capability and delivery system development projects with C/CSPs, negotiates and manages associated contracts with C/CSPs, and tests and accepts new capabilities on behalf of all Commonwealth, State and Territory intercepting agencies.

TECHNICAL CAPABILITY DEVELOPMENT

The ASIO engineering and development group provides technical support to our wider technical collection capability. The group provides both strategic and tactical engineering solutions through a mix of in-house design and production and out-sourced projects,

Cooperation with Australian agencies

ASIO has well-developed relationships on technical matters with a range of agencies including the Australian Federal Police, Australian Secret Intelligence Service, Defence Signals Directorate, and the Defence Science and Technology Organisation.

ASIO also has a strong relationship with the Department of the Prime Minister and Cabinet's National Security, Science and Technology Unit. ASIO has an officer seconded to the Unit and is represented on its steering committee.

SURVEILLANCE

Surveillance plays a vital role within ASIO and is a key investigative tool. The duties of a Surveillance Officer may involve planning and conducting surveillance activities, reporting on surveillance investigations and operations, using photographic and other technical and information technology equipment, formulating and presenting advice and undertaking other activities associated with the collection of intelligence.

The primary role of ASIO surveillance teams is to report on people of security interest, with specified objectives for each targeting requirement. This includes identifying the movements, contacts and activities of subjects of investigation.

In February 2006, ASIO started a major nation-wide recruiting campaign to begin the expansion of the surveillance capability.

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

MONITORING AND ALERTING

ASIO's Research and Monitoring Unit provides 24/7 monitoring of the global and domestic security environment.

The work of the Unit ensures real time responsiveness for ASIO's investigative, assessment and reporting functions. The Unit also provides a specialised open source research capacity to meet the requirements of all areas of ASIO.

The Unit produces a daily unclassified compilation of security reporting to raise counter-terrorism awareness in relevant agencies.

In addition to monitoring and alerting, the Unit:

- screens National Security Hotline calls referred to ASIO by the Protective Security Coordination Centre;
- processes 'out of hours' public line calls; and
- provides advice internally of media reporting relevant to ASIO and its functions.

Since it was established in December 2002, the Protective Security Coordination Centre's National Security Hotline has referred approximately 42 000 calls to ASIO

Open-source research

The Research and Monitoring Unit's open-source research capability was increased with the recruitment of additional researchers to allow the Unit to operate for extended hours through the week. For the remaining time and on weekends, the 24-hour monitoring staff process urgent research requests to meet the needs of State offices, overseas liaison posts operating in different time zones and the 24/7 work units in Canberra.

COMPLEX ANALYTICAL CAPABILITIES

The volume, pace and diversity of information flowing to ASIO has continued to increase.

This has required ASIO to acquire and develop new capabilities and techniques to:

- better collate, search and sort data;
- access and analyse material in a variety of formats; and
- visualise complex information sets.

This work was undertaken by a number of parts of ASIO and involved a combination of innovative data-analysis methods and the use of advanced information technology.

Some progress was made on better ways of collating, searching and sorting data, and work is progressing on improving and extending these capabilities across ASIO's information holdings.

National Security Hotline

Since it was established in December 2002, the Protective Security Coordination Centre's National Security Hotline has referred approximately 42 000 calls to ASIO. Of these referrals, approximately 11 500 have been assessed as requiring further investigation.

While not all National Security Hotline calls provided useful intelligence, those that do can be significant.

WORKING WITH FEDERAL, STATE AND TERRITORY POLICE

ASIO has worked closely with Federal, State and Territory police over many years. During 2005–06, we continued to refine the model for working together.

The working model we have with police recognises ASIO's lead role in conducting broad-based intelligence investigations aimed at identifying threats to security. Should investigations identify significant criminality (in terms of terrorism offences), the model calls for early police involvement in evidence collection as a parallel to ASIO's intelligence collection activities. This structure aims to maximise the opportunity for police agencies to collect evidence.

ASIO-police working relationships have generated significant resource savings and, at times, increased the type and amount of resources available for investigations.

ASIO's joint investigative activity with police services is not limited to the threat of terrorism. Across Australia, ASIO works closely with State and Territory police to manage the threat of violent protest actions and more generally the threat posed by nationalist extremists/racist extremists. In addition, across Australia ASIO has cooperative arrangements with police to manage joint investigations into leads generated from the National Security Hotline and other warning systems such as 'Crime Stoppers' and '000' calls.

Security of major events

The security of major events, including the 2006 Melbourne Commonwealth Games, the Forbes CEO Conference in Sydney and other events attracting the convergence of issue motivated groups was a focus for ASIO in 2005–06.

The Melbourne Commonwealth Games drew heavily on ASIO resources across the board. ASIO deployed staff to Melbourne to enable 24/7 operations and to provide an immediate response capability.

During the year, we established and implemented the framework for our APEC 2007 planning.

ASIO-police working relationships have generated significant resource savings and, at times, increased the type and amount of resources available for investigations

LIAISON WITH INTERNATIONAL PARTNERS

ASIO's responsibilities extend to wherever threats to Australians and Australian interests occur in the world – our function is defined by subject matter, not geography, so our focus and reach must necessarily be global. ASIO's international liaison network provides access to intelligence and shared capabilities which are vital in progressing investigations.

As at 30 June 2006, ASIO had 268 approved liaison relationships in 113 countries. ASIO manages these liaison relationships through its international liaison offices located around the world or through foreign representatives posted to Australia or who visit on a regular basis.

This network is complemented by communication links with counterpart agencies, visits by ASIO officers and managers to foreign intelligence services and reciprocal visits to Australia by heads of agencies and staff at all levels.

The Counter-Terrorism Intelligence Training Program delivers counter-terrorism training and capacity building to Australia's regional partners and, more generally, enhances international cooperation on security matters

ASIO LIAISON OFFICES

Prior to being posted to countries where English is not the primary language, ASIO liaison officers are provided with intensive language training ranging from several months to two years.

Liaison officers travel regularly within their region to engage with other intelligence services so that we continue to receive a wide range of reporting or to pursue particular lines of investigation.

ASIO liaison officers have facilitated engagement with liaison partners by other Australian agencies or departments.

VISITS AND CONFERENCES

The Director-General visited the heads of a number of international liaison partners in 2005-06. The Director-General also represented ASIO at the 2005 Bali Commemoration.

ASIO senior managers made a number of visits to liaison partners.

COUNTER-TERRORISM INTELLIGENCE TRAINING PROGRAM

The Counter-Terrorism Intelligence Training Program (CTITP) delivers counter-terrorism training and capacity-building assistance to Australia's regional partners and, more generally, enhances international cooperation on security matters.

The CTITP can bring together resources, people and counter-terrorism expertise to assist other countries where requested. The Program also recognises the experience and talent our regional partners are able to share with us. The CTITP formally commenced its activities in July 2005 and has worked effectively to achieve its objectives during 2005–06.

COUNTER-TERRORISM RESPONSE CAPABILITIES

During 2005–06, ASIO continued to contribute to whole-of-government counter-terrorism policy coordination and national counter-terrorism arrangements. As detailed in Australia's National Counter-Terrorism Plan (NCTP), this work focused on the four key phases: preparation, prevention, response and recovery. The NCTP can be found at www.nationalsecurity.gov.au.

ASIO participated in working groups responsible for progressing work on behalf of the National Counter-Terrorism Committee (NCTC) and the Australian Government Counter-Terrorism Policy Committee (AGCTPC), covering a broad range of topics, including:

- critical infrastructure protection;
- border security;
- transport security; and
- science and technology.

ASIO also participated in two major Australian Government initiatives during the reporting period – contributing to the *Independent Review of Airport Security and Policing for the Government of Australia* (conducted by the Right Hon. Sir John Wheeler, DL) and the specially convened Council of Australian Governments meeting to address and implement lessons learned from the July 2005 bombings of London's transport system.

Support to the National Counter-Terrorism Committee

As a member of the NCTC, ASIO participates in the coordination of Australia's national counter-terrorism arrangements by contributing to strategic policy advice, development of an effective nation-wide counter-terrorism capability, and ensuring effective arrangements are in place for sharing relevant security intelligence between agencies and jurisdictions.

The Australian Government relies on high-quality intelligence to prevent and disrupt attacks against Australians or Australian interests at home and abroad. It is important to ensure ASIO's counter-terrorism response capabilities are readily deployed in the event of any terrorist incident.

Under the NCTP, ASIO has responsibility for the inter-agency operations centre, the National Intelligence Group (NIG). The NIG, located in ASIO's Central Office, coordinates and disseminates intelligence to inform and support policy makers and operational commanders. ASIO also provides support to police operational commanders through deployment of intelligence officers and supporting staff to Joint Intelligence Groups and Police Forward Command Posts, both located at, or near, the scene of a terrorist incident.

It is important to ensure ASIO's counter-terrorism response capabilities are readily deployed in the event of any terrorist incident

Counter-terrorism exercises

To ensure it remains prepared to respond to a terrorist incident, ASIO participates in the NCTC exercise and training program. This comprehensive schedule of exercises brings together Commonwealth, State and Territory security, law enforcement, intelligence and emergency management agencies and is designed to test, strengthen and maintain effective working relationships and capabilities across and between jurisdictions and organisations.

During the reporting period ASIO participated in the planning and execution of counter-terrorism exercises designed to test security preparations for the 2006 Melbourne Commonwealth Games. The largest counter-terrorism exercise ever held in Australia, Mercury 05, was conducted over a four-day period in five jurisdictions – Victoria, South Australia, New South Wales, the Australian Capital Territory and Western Australia. The exercise scenario focused on a series of terrorist attacks in Australia during the 2006 Melbourne Commonwealth Games

and thoroughly tested security preparations as well as practising national counter-terrorism arrangements.

ASIO also participated in Investigation and Consequence Management Exercises Orchid Alert in Queensland and Western Explorer in Western Australia, and Tactical Response Exercise Neptune's Treasure in NSW.

Support to the Australian Government Counter-Terrorism Policy Committee

The Australian Government Counter-Terrorism Policy Committee, chaired by the Department of the Prime Minister and Cabinet, comprises senior officials from 22 Australian government departments and agencies. ASIO provides regular security environment briefings to this key interagency body, which has responsibility for coordination of strategic policy on counter-terrorism issues.

ASIO is a permanent member of the Australian Government Counter-Terrorism Committee. Chaired by the Protective Security Coordination Centre, the Committee regularly reviews the national counter-terrorism alert level to advise ministers on whether changes to the alert level should be considered.

ASIO also participates in Interdepartmental Emergency Task Force (IDETF) arrangements, which plans a response to any terrorist incident overseas involving Australians or Australian interests. ASIO supports IDETF arrangements by hosting the NIG and maintaining a capability to deploy intelligence support overseas.

TECHNICAL SUPPORT UNIT

ASIO's Technical Support Unit (TSU) can be called upon to assist the Federal, State and Territory police manage a terrorist or siege incident. Its role is to provide technical support to the police commander managing the incident and the police technical units in gathering covert intelligence at the scene.

The TSU – comprising technical officers with a broad range of technical operations skills – is maintained in a high state of readiness and is regularly exercised.

An important role for the TSU is to provide unique and specialised technical capabilities to support the Police and assisting Australian Defence Forces in resolving a counter-terrorism incident.

During 2005–06 the TSU participated in the following exercises:

- deployment of two TSU teams to Bendigo and Adelaide for the Mercury 05 exercise;
- February – March 2006 pre-deployment to Melbourne for the Commonwealth Games; and
- deployment of two TSU teams to Sydney in May 2006 for the counter-terrorism tactical exercise Neptune's Treasure.

A large part of this performance report is excluded from the unclassified *Report to Parliament* for reasons of national security.

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 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 from liaison with overseas partners

This performance report has been excluded in its entirety from the unclassified *Report to Parliament* for reasons of national security.

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 performance for intelligence agencies**
- **the Parliamentary Joint Committee on Intelligence and Security**
- **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 available publicly on ASIO's website.**

CORPORATE GOVERNANCE

ASIO's corporate governance framework supports the management of risk, flexible allocation of resources to meet changing business needs, regular critical review of performance across all functions as well providing for transparency and accountability

ASIO's corporate governance framework supports the management of risk, flexible allocation of resources to meet changing business needs, regular critical review of performance across all functions as well providing for transparency and accountability.

Corporate governance in ASIO is exercised through the Corporate Executive, comprising the Director-General, Deputy Director-General, First Assistant Directors-General and two managers on rotation, with the Staff Association President attending as an observer.

The Corporate Executive meets twice monthly and is the main forum for managing strategic corporate priorities and resource issues. It also conducts detailed quarterly reviews of the performance of the Organisation. The results of these reviews feed into the *Annual Report*.

The Corporate Executive is supported by six corporate committees, including the:

- Intelligence Coordination Committee (ICC), which is chaired by the Deputy Director-General and includes all Division Heads. The ICC uses a risk-management approach to set investigative priorities, consider operational policy issues and review performance against objectives. It monitors the security environment and recommends resource adjustments accordingly;
- Audit and Evaluation Committee, which is chaired by the Deputy Director-General and includes a senior executive from the Australian National Audit Office. This committee sets the audit and evaluation program for ASIO, reviews the outcomes of audits and evaluations and oversees the implementation of recommendations;
- Human Resource Development Committee, which is chaired by a Division head and includes representatives from the Staff Association. This committee provides guidance on staff development issues, including the implementation and provision of training programs to ensure that the Organisation's human resource capabilities are developed across all functions;
- Security Committee, which is chaired by the head of Security Division and includes representatives from the Staff Association. It promotes sound

practice by ensuring that security is considered appropriately in all major developments and initiatives;

- Information Management Committee, which is chaired by the Deputy Director-General. It provides guidance and sets priorities for the development of information management capabilities and monitors and reviews the implementation of projects; and
- ASIO Consultative Council, co-chaired by the head of the Corporate Management and Liaison Division and the President of the Staff Association. It comprises representatives from management and the ASIO Staff Association. The ACC provides a forum for discussion and negotiation on employment and conditions of service issues. It is an advisory body with no decision-making authority (see also page 63).

Figure 3: ASIO's Corporate Governance Structure

CORPORATE PLANNING

ASIO's *Corporate Plan 2002–2006* sets the broad framework for how ASIO does its business, measures its performance and achieves outcomes. In 2005–06, ASIO's business focus remained:

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

The *Corporate Plan 2007–2011* is scheduled for completion in late 2006.

The *Corporate Plan 2002–2006* is available publicly at www.asio.gov.au.

ACCOUNTABILITY AND EXTERNAL SCRUTINY

ASIO operates under an extensive oversight and accountability framework which includes the Government, the Parliament and the Inspector-General of Intelligence and Security.

NATIONAL SECURITY COMMITTEE OF CABINET

The National Security Committee of Cabinet sets policy and decides intelligence agencies' budgets. The Committee considers the performance of ASIO each year, including by reviewing ASIO's *Annual Report*. The Director-General is a member of the Committee.

ATTORNEY-GENERAL

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

ASIO operational activity must comply with the *Attorney-General's Guidelines for the Collection of Intelligence*, which require the use of methods commensurate with the assessed risk. The Attorney-General is kept informed of ASIO's operations, including through his role in considering the grounds for warrants authorising the use of ASIO's special powers.

ASIO briefs the Attorney-General on all major issues affecting security and other matters in connection with ASIO. In 2005–06, ASIO provided 304 briefings and submissions to the Attorney-General, compared to 237 in 2004–05.

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

ASIO operates under an extensive oversight and accountability framework

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

A Parliamentary Joint Committee has been part of ASIO's oversight and accountability framework since 1988.

Review of administration and expenditure

The Committee has a mandate under section 29(1)(a) of the *Intelligence Services Act 2001* to review the administration and expenditure of ASIO and the other intelligence agencies. It also can inquire into other matters referred to it by the Government or by the Parliament.

The Committee reviews ASIO's administration and expenditure within the life of each Parliament, with specific reviews focused on different aspects each year. In 2005–06 the *Review of Administration and Expenditure Number 4*, focused on recruitment and training. On 2 February 2006, ASIO submitted a written brief (available publicly at www.asio.gov.au) and on 23 March 2006 the Director-General appeared (in camera) before the Committee in connection with this review.

A Parliamentary Joint Committee has been part of ASIO's oversight and accountability framework since 1988

Proscription of Terrorist Organisations

Under section 102.1A of the *Criminal Code Act 1995* (as amended by the *Criminal Code Amendment (Terrorist Organisations) Act 2004),* the Committee can review the listing of an organisation as a terrorist organisation (see also page 32).

ASIO appeared (in camera) before the Committee on:

- 8 August 2005 in connection with the *Review of the Re-listing of Four Terrorist Organisations*; and
- 6 February 2006 in connection with the *Review of the Listing of the Kurdistan Workers' Party (PKK).*

Review of ASIO's questioning and detention powers

Section 29(1)(bb)(i) of the *Intelligence Services Act 2001*, required the Committee to review, by 22 January 2006, the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act. On 8 August 2005, ASIO provided a classified briefing to the Committee in connection with this review.

On 15 June the Parliament re-enacted these provisions of the ASIO Act.

Other briefings

The Director-General also provided the Committee with private briefings on 6 October 2005, 9 February and 22 June 2006.

OTHER PARLIAMENTARY OVERSIGHT

The Director-General appeared before other Parliamentary committees, including:

- 17 November 2006, before the Senate Legal and Constitutional Legislation Committee in relation to the *Inquiry into the Provisions of the Anti-terrorism Bill (Number 2) 2005*;
- 8 February 2006, before the Joint Committee of Public Accounts and Audit in connection with the *Review of Aviation Security in Australia*;
- 14 February and 25 May 2006 before the Senate Legal and Constitutional Legislation Committee as part of the estimates process; and
- 8 March 2006 before the Security Legislation Review Committee.

ASIO also responded to 78 Questions on Notice from Members and Senators.

INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The role of the Inspector-General of Intelligence and Security 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 Inspector-General 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 Inspector-General 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.

Based on the various monitoring, inspection and inquiry activities undertaken by the Office of the Inspector-General of Intelligence and Security in 2005–06, Mr Carnell was satisfied that there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or the human rights of Australians.

Further details can be found in the Inspector-General's *Annual Report* at www.igis.gov.au.

AUDIT, EVALUATION AND FRAUD CONTROL

Fraud Control Plan

A review of ASIO's *Fraud Control Plan 2004–2006* commenced in late 2005 and will be completed by the end of 2006.

ASIO's fraud prevention strategies include the requirement for all staff 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. All new staff are provided with the (classified) *Guide to Fraud Prevention, Detection and Reporting Procedures in ASIO,* and the *Fraud Control Plan* is available on ASIO's Intranet.

No fraud investigations were undertaken in 2005–06.

Internal audits and evaluations

Throughout the year nine internal audits and one evaluation were completed and were the subject of (classified) reporting to the Audit and Evaluation Committee.

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

Assumed identities

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

Figure 4: The Inspector-General of Intelligence and Security, Mr Ian Carnell

As required under the Act, audits were conducted in July 2005 and January 2006 of records of authorisations under the Commonwealth scheme with no discrepancies detected.

New South Wales legislation

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 2006 for the preceding financial year. The audit did not disclose any fraudulent or other criminal behaviour.

Identity security regimes

The Commonwealth, States and Territories jointly are seeking to progress a whole-of-government solution to the various problems posed by identity misuse, identity crime and identity fraud. The proposed regime includes:

- establishing a common set of key identifying documents of integrity;
- implementing advanced security features, including biometric identifiers where appropriate, on identity-related documents to reduce the risk and incidence of forgery;
- establishing secure electronic mechanisms to enable participating organisations to verify data on key proof-of-identity documents;
- improved accuracy of personal identity information held on organisations' databases; and
- enabling post-registration contacts between individuals and organisations to occur with the confidence that each party is accurately authenticated.

ACCESSIBILITY TO THE PUBLIC

ASIO WEBSITE

The website (www.asio.gov.au) is the main dissemination channel for publicly available information about ASIO.

In 2005–06, ASIO's most popular website pages were the Annual *Report to Parliament* and employment pages.

Redevelopment of the website commenced in 2005–06 with a revised site scheduled for implementation in 2006–07.

MEDIA POLICY

Consistent with long-standing practice ASIO generally does not comment on operational matters.

PUBLIC STATEMENTS

The Director-General delivered 19 addresses in 2005–06, including to business forums, various conferences and institutions. These are available publicly on ASIO's website. The themes and issues highlighted in these statements included:

- the continuing threat of terrorism and other threats to security;
- the risk of complacency;
- the inability to provide a guarantee that there will always be prior intelligence about threats to enable preventative action;
- the importance of ASIO acting ethically and strictly within the legislative framework; and
- the importance of ASIO working effectively with Australian and international partners.

OUR PEOPLE

ASIO has a critical ongoing requirement to attract, integrate, retain and appropriately develop high-calibre people.

WORKPLACE RELATIONS AND REFORMS

Following extensive consultation and negotiation between staff and management, ASIO implemented its Seventh Workplace Agreement. The Agreement was accepted in November 2005 after 78 percent of all eligible staff participated in a ballot, of which 90 percent endorsed the package.

The Agreement commenced on 1 January 2006 and includes annual salary increases to ensure ASIO's salary structure remains attractive and competitive. In addition, the Agreement includes initiatives to assist staff to maintain an appropriate balance between their work and personal lives. It also will support ASIO's efforts to develop and retain quality people to ensure performance and capabilities are sustained, including by:

- aligning the administrative conditions of service for permanent and temporary staff; and
- formalising the requirement for (and past practice of) staff to respond to the need to work additional hours; to be readily available to perform work (on-call); or to return to work in emergency situations.

Workplace relations were further enhanced by the ASIO Consultative Council continuing to meet on a monthly basis to discuss issues of concern to staff and management (see also page 58).

ASIO has a critical ongoing requirement to attract, integrate, retain and appropriately develop high-calibre people

STAFF SURVEY

In June and July 2005 a staff survey measured employee attitudes, concerns and areas of satisfaction across a range of dimensions. Over 75 percent of staff participated with their responses indicating that a number of areas had recorded improvements when compared to previous surveys.

The survey found that ASIO has a highly committed workforce:

- staff feel they know what is expected of them and have the skills and knowledge to do their jobs well;
- there are very good working relations between staff and supervisors and within teams; and
- staff believe their teams provide quality service to clients, and their teams promote and encourage innovation.

The survey found that ASIO has a very highly committed workforce

STAFFING PROFILE

ASIO has continued to engage non-ongoing employees but the focus of recruitment has been the employment of ongoing staff to meet future growth. At 30 June 2006, some 23 percent of staff were non-ongoing employees, the same as 2004–05.

Between April and June 2006, ASIO went through a process to shift many non-ongoing staff to ongoing employment arrangements with implementation from 1 July 2006. This will provide greater certainty for the Organisation and individual staff members.

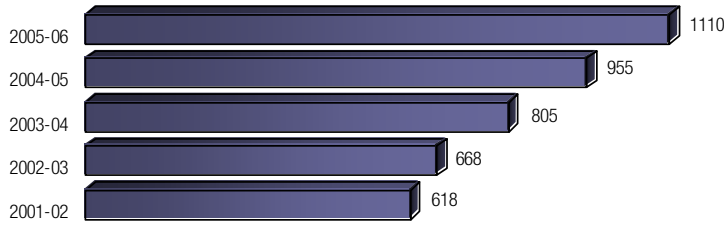


Figure 5: Staffing numbers 2001–02 to 2005–06

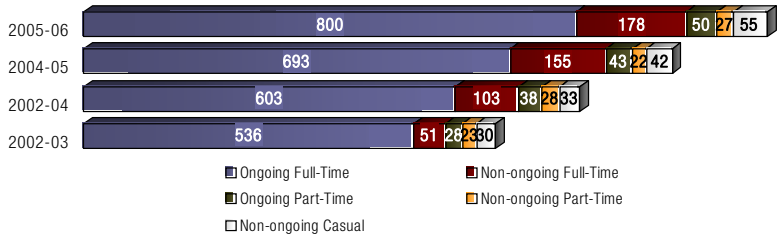


Figure 6: Composition of workforce 2002–03 to 2005–06

RECRUITMENT

Recruitment remains one of ASIO's key challenges as we continue to seek quality staff to fill a broad range of roles. The level of recruitment will remain high into 2006–07 and we are confident of meeting the annual net growth of 170 that has been endorsed by Government. We have bolstered the recruitment area, streamlined processes and enhanced recruitment systems.

During 2005–06 we recruited 247 staff compared to 224 in 2004–05. This was a very credible effort – the most staff ever recruited into the Organisation over a financial year.

We developed a number of strategies to ensure recruitment targets are met without compromising standards:

- a Recruitment Task Force was developed to provide further capability. A small team of trained vetting officers from other parts of the Organisation was seconded to the recruitment area to supplement exisiting resources. This task force will continue to be deployed during future periods of high demand;
- continued use of recruitment agencies to assist in sourcing applicants for specific roles, coordinating assessment centres and on-line testing;
- prioritised 'job family' campaigns will be extended to most ASIO vacancies in 2006–07. This new approach will minimise the number of separate recruitment processes and allow us to streamline selection processes. It also will enable more effective forward planning to ensure the availability of resources;
- the upgrading of our recruitment data management which will result in more efficient monitoring and reporting of applicant progress through the security clearance process;
- having a strong presence on the Internet and at Career Advisory Days at universities; and
- positioning ASIO as a unique and dynamic organisation.

Recruitment remains one of ASIO's key challenges as we continue to seek quality staff to fill a broad range of roles

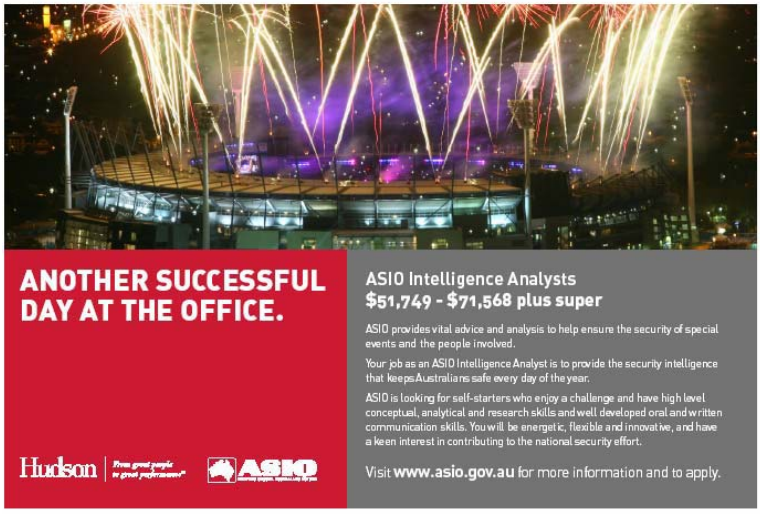


Figure 7: Advertisement for the Intelligence Analyst recruiting campaign

ADVERTISING

ASIO ran a series of innovative advertising campaigns in 2005–06 aimed at attracting high-calibre applicants from various backgrounds to fill a range of vacancies.

To ensure our approach was fresh and contemporary we worked with several recruitment and advertising agencies. We redesigned our campaign to feature case studies to attract applicants who normally would not consider a career with ASIO.

The challenge for ASIO was to shift public perceptions of the Organisation from being 'outdated and formal' to 'a place I'd like to work' and to remove the uncertainty about a career with ASIO.

The media was responsive to the approach with the metropolitan press running a number of the case studies.

Other advertising initiatives included targeted campaigns in relevant industry publications (such as legal and engineering magazines) and Internet advertising, including career websites and Google.

The overall cost of ASIO's recruitment advertising for 2005–06 was $2 044 018.

Figure 8: Intelligence Officer recruitment campaign

Figure 9: Surveillance Officer recruitment campaign

STAFF RETENTION

ASIO's separation rate for 2005–06 increased slightly to 6 percent compared to 5.8 percent in 2004–05. Nonetheless, ASIO's separation rate remains in the reasonable range. The rate is monitored to ensure that it remains at a level which will achieve a healthy turnover while retaining skilled and experienced staff.

In separation interviews staff cited increased remuneration, promotional/career opportunities, personal/family commitments and greater job satisfaction as principal reasons for their departure.

PERFORMANCE PAY

Members of the Senior Executive Service are eligible to receive performance pay which is based on a percentage of gross salary. In the reporting period, 14 officers received performance pay for the 2004–05 financial year with amounts ranging from $3 670 to $25 480. The average payment was $10 201 and the total amount paid was $142 822.

DEVELOPING OUR PEOPLE

ASIO is committed to the learning and development of its staff and continues to invest in developing leadership, management, administrative, technical and intelligence capabilities. In 2005–06, we invested $3 523 899 (about 1.9 percent of our budget) in training and development.

Management and leadership skills

ASIO places a strong emphasis on the development of the leadership and management skills of all its senior officers. The *Learning and Development Strategy for Leadership in ASIO* provides a benchmark that aligns capability development with national public sector standards and offers a framework for individual development planning.

Senior officer leadership and management skills are developed formally through a five day Management to Leadership course – four days residential with a one day follow-up session. In 2005–06 senior officers attended this course which is provided by an external consultant but tailored to ASIO's specific requirements.

The Diploma of Business (Frontline Management) course, now with a flexible self-paced learning option as well as the traditional classroom-based course, was completed by staff at or just below the senior officer level.

A new Senior Officer Orientation Workshop also was developed to provide senior officers with a solid understanding of their management responsibilities and accountabilities within ASIO.

Leadership and management learning and development also involved:

- four Senior Executive Service time-outs (one residential) which focused on implementing the Taylor Review recommendations, organisational restructure, workforce planning, corporate planning, managing organisational growth, corporate governance and individual development; and
- two combined Senior Executive Service and Senior Officer time-outs, which considered corporate issues such as Taylor Review implementation and organisational restructure, business continuity planning, information management, occupational health and safety issues and legislative developments.

Intelligence Officer Traineeship

In January 2006 Intelligence Officer Trainees graduated from the 2005 Intelligence Officer Traineeship. More Intelligence Officer Trainees commenced the first of two traineeships to be run in 2006. The second traineeship started in July and will run until June 2007.

The competencies required of ASIO's Intelligence Officers were reviewed in 2005 with the revised competencies applied to subsequent assessment centre selection processes. Minimum academic qualifications were changed from a four year degree or equivalent to a minimum three year degree. This change is intended to broaden the recruitment pool of applicants with work and life experience.

We continue to draw Intelligence Officer Trainees from diverse backgrounds and experiences. The current Intelligence Officer Trainees are drawn from all mainland States and the Australian Capital Territory with some born overseas. Their academic and professional backgrounds range across Law, Journalism, Education, Defence, Engineering, Science, Philosophy and Commerce.

We continue to draw Intelligence Officer Trainees from diverse backgrounds and experiences

Analytical and operational skills

A review of ASIO's training in analytical skills was conducted in 2005–06. Analytical training is undertaken by both Intelligence Officers and Intelligence Analysts and incorporates a mixture of training modules and workplace learning with a particular emphasis on the development of critical analysis skills.

Additional operational training is provided to new Intelligence Officer graduates posted into Collection Division and for experienced Intelligence Officers being posted to Collection Division from other parts of the Organisation. The courses are designed to enhance the basic skills established during the Intelligence Officer Traineeship, with a particular focus on current challenges and specific operating requirements.

ASIO also seeks to enhance the ability of more experienced operational officers through advanced training.

During 2005–06, ASIO continued its program of courses developed and facilitated by leading academics to enhance staff development in relevant areas

We also conducted joint training with police services to ensure that, where necessary, ASIO's collection of intelligence is done in a manner consistent with legal evidentiary requirements.

In 2005–06, ASIO continued to invest in the development of language skills

Linguistic capability

In 2005–06, ASIO continued to invest in the development of language skills, including:

- a full-time, one–two year training program for selected officers in languages most relevant to ASIO's investigative work**.** This training includes formal classroom instruction in Australia and in-country components;
- ASIO liaison officers requiring language training are provided access to Department of Foreign Affairs and Trade courses, including one-on-one tutorials and small group learning; and
- ASIO's linguists also are provided with training to refine and enhance their skills.

Further language learning opportunities are offered to all ASIO officers through the Studies Assistance Program.

Corporate training

Officers below the Senior Executive Service level are provided learning opportunities under the (classified) *ASIO Officer Capability Development Strategy*. This strategy provides a framework aligned to national public sector behaviours and capabilities, and ensures that appropriate career development training is ongoing across the Organisation.

Programs offered include:

- an initial orientation course for all new staff and seconded officers;
- administrative training, including contract management, project management, selection panel skills, presentation skills, trainer training, interviewing, effective reading and writing, finance and budgeting;
- initial and refresher training in the use of ASIO's administrative and intelligence computer systems and applications;
- an annual series of courses in ethics and accountability that all ASIO officers are requried to attend at least once every three years; and
- support to individual officers for tertiary study through the Studies Assistance Program. Additional support for those officers who achieve outstanding results in their studies while maintaining high levels of performance in the workplace is provided through annual Director-General's Bursaries.

Seminar series

The Seminar Series consists of monthly presentations on topics of general professional interest to all staff. The series fosters a sense of team-work and seeks to improve professionalism and to broaden the knowledge and skills of staff. Some seminars are especially useful for newer staff in the Organisation.

In 2005–06 presentations were delivered on ASIO's counter-terrorism response arrangements, intelligence communication methods, the history of ASIO, the *Business Continuity Plan*, and ASIO's role in the security arrangements for the Commonwealth Games.

External guest speakers participated in the program, which further enhances our relationships with our strategic partners.

SECONDMENTS

Secondments and personnel exchanges with other agencies in Australia and overseas provide additional professional development opportunities and reflect the long-standing cooperation that exists between ASIO and its domestic and international partners.

In addition to long-standing exchange programs with some of our overseas counterparts, working within ASIO are seconded officers from:

- Australian Federal Police;
- Australian Secret Intelligence Service;
- AUSTRAC;
- Department of Defence;
- Department of Foreign Affairs and Trade;
- Defence Imagery and Geospatial Organisation;
- Defence Intelligence Organisation;
- Department of Transport and Regional Services;
- Defence Signals Directorate;
- Defence Science and Technology Organisation; and
- Office of National Assessments.

Further, in 2005–06 ASIO had officers seconded to:

- Australian Federal Police;
- Australian Secret Intelligence Service;
- Department of Foreign Affairs and Trade;
- Department of the Prime Minister and Cabinet;
- Department of Transport and Regional Services; and
- Office of National Assessments.

This increased breadth of cooperation is a further reflection of a whole-of-government approach to addressing the challenges posed by the security environment.

WORKPLACE DIVERSITY

ASIO continued to implement and monitor the (classified) *Workforce Diversity Program 2005 to 2009*. The program encouraged the recognition and appreciation of individuals and their contribution to the corporate mission and objectives.

Diversity statistics

The percentage of female staff has increased to approximately 46 percent and the percentage of senior officers who are female has increased to approximately 33 percent.

The representation of ethnically diverse staff has increased in 2005–06.

Statistical data on the workforce profile and the ethnic diversity are contained in Appendix C.

The percentage of female staff has increased to approximately 46 percent and the percentage of senior officers who are female has increased to approximately 33 percent

Diversity and harassment contact officers

The Diversity and Harassment Contact Officer networking group continued to raise the profile of diversity, harassment and bullying issues within the workplace by informing and supporting staff and managers. The Organisation supported the work of the group by providing training, guidance and information to the Diversity and Harassment Contact Officers.

DISABILITY STRATEGY

ASIO's (classified) *Disability Action Plan* is focused on addressing the needs of people with disabilities through the provision of services and dissemination of information about disability issues. The Organisation has tailored the recruitment process to address needs identified by recruits and provide opportunities to applicants with disabilities.

ASIO aims to achieve the highest practical occupational health and safety standards for its staff and to foster attitudes and work practices that sustain healthy and safe work environments

OCCUPATIONAL HEALTH AND SAFETY

ASIO aims to achieve the highest practical occupational health and safety standards for its staff and to foster attitudes and work practices that sustain healthy and safe work environments.

During 2005–06 ASIO broadened its focus to include the establishment and refinement of systems to manage health and safety for a rapidly growing workforce (that is, injury prevention, risk management and early intervention).

This included a SafetyMAP audit of all the work groups within the Organisation. The use of SafetyMAP is endorsed by Comcare and issues identified by the audit will form the basis for improvements to the current occupational health and safety management systems.

Consistent with this strategy, other initiatives that were undertaken included:

- Occupational Health and Safety Sub-Committee meetings every six weeks to discuss and prioritise action for key health and safety issues;
- reviewing and establishing work groups and electing and training Health and Safety Representatives for each group; and
- offering influenza vaccinations to all staff to promote health and well-being and reduce absenteeism.

During 2005–06, there were thirty-eight incidents reported to ASIO's Occupational Health and Safety section. Of these, six resulted in serious personal injury requiring emergency medical treatment and two incidents were categorised as a dangerous occurrence. One incident was reported to Comcare under Section 68 of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*. Control measures have been put in place where appropriate to minimise the likelihood of similar incidents occurring in the future.

Notices and investigations

There were no Provisional Improvement Notices issues under section 29 of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*.

There were no investigations conducted under section 41, or any notices issued under sections 46 and 47, of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*.

Workers' compensation claims

There were thirteen claims for workers' compensation submitted in 2005–06; liability was accepted for ten claims and three remained under consideration at the end of the reporting period. In contrast, fourteen claims were submitted in 2004–05.

INFORMATION MANAGEMENT

ENABLING ORGANISATIONAL GROWTH

Sustained high volumes of information flow and the demands of the Melbourne Commonwealth Games 2006, continued to put pressure on information management systems. ASIO upgraded a number of its systems to improve performance and reliability.

Connectivity improvements

Key enhancements to ASIO's information technology platforms focused on enhanced connectivity with Australian and international partners.

ASIO implemented a pilot electronic link with the Department of Immigration and Multicultural Affairs that allowed the automated transfer of visa security assessments across a secure data gateway.

ASIO upgraded a number of its systems to achieve improved performance and reliability

IDENTITY MATCHING

ASIO upgraded its identity matching software.

ASIO's capacity to complete large volumes of security assessments has been enhanced by the implementation of multi-queue batch processing. This facility accepts batches and automatically scans our database for potential matches. These potential matches are stored, ready for examination by ASIO officers who make the assessments. This approach reduces the need for manual data entry, reduces transaction response times and improves the productivity and work value of our staff.

ASIO expanded its applications framework substantially during 2005–06. New, sophisticated analytical tools are available for analysts' use on the corporate network, improving analytical processes and the swiftness of results. Additional analytical tools are undergoing test or evaluation.

ASIO's capacity to complete large volumes of security assessments has been enhanced by the implementation of multi-queue batch processing

RECORDS MANAGEMENT

Improvements to ASIO's records management systems continued throughout 2005–06. The electronic document and records management software has been extended to each desktop and testing of the full document management and electronic records capabilities was underway at the end of the period.

A new intelligence document distribution system was developed. The system will accept documents from published sources and classified feeds through secure inter-agency feeds and make them available within ASIO. It will replace the current system which is no longer capable of meeting the large volumes of electronic documents received by ASIO.

PROCESSING BACKLOGS

The rate and volume of information flowing to ASIO, including new streams of intelligence, continued to increase. ASIO processed all priority material quickly but the backlog of routine information continued to grow.

IT BUSINESS CONTINUITY

ASIO commenced the re-development of its (classified) *Business Continuity Plan* during 2005–06. Responsibilities for all aspects of the plan have been identified and assigned to teams of staff drawn from across the Organisation. These responsibilities include staff welfare, security, building restoration and IT recovery. Remote contingency sites have been selected. A dedicated project team has coordinated the documentation of recovery procedures and conducted desk-based hypothetical testing. The test regime will be ongoing, to ensure the plan remains functional.

SECURITY OF ASIO

In 2005–06 we continued to build on our strong security culture by focusing on security awareness training and the implementation and review of security polices and practices.

SECURITY MANAGEMENT PLAN

The (classified) *ASIO Security Plan 2005–2009* was reviewed and updated. The Plan identifies ASIO's security risks and outlines objectives, policies and strategies. It is based on the principles and minimum standards required by Government as set out in the *Protective Security Manual*, in addition to those endorsed by the Inter-Agency Security Forum for application within the Australian Intelligence Community and related policy departments. The Plan is available to staff on the ASIO Intranet.

SECURITY AUDITS

Security audits are designed to ensure adherence to relevant security standards, to identify areas where improvement is needed or desirable and to enhance security in line with ASIO's commitment to security best practice.

During the year, ASIO conducted security audits resulting in the identification of some minor issues. A (classified) security awareness bulletin was issued to remind staff of their responsibilities.

SECURITY POLICIES

ASIO's security policies are consistent with Inter-Agency Security Forum best practice guidelines and conform to the minimum standards identified in the *Protective Security Manual* and the *Australian Government Information and Communications Technology Security Manual* (ACSI33). Policies are circulated to staff and placed on the corporate Intranet site.

The security awareness and education campaign continued throughout the period. Security briefings and presentations were undertaken and an unclassified (internal distribution only) security desk aid was distributed to all staff as part of the campaign.

PERSONNEL SECURITY

Security clearance re-evaluations

ASIO continues to re-evaluate the clearances of its staff, contractors and appropriate associates at intervals not exceeding five years in accordance with the *Protective Security Manual* and its (classified) Supplement. Staff security is monitored between re-evaluations through annual appraisals completed by staff and their supervisors with a more detailed examination after 30 months.

In addition to these formal review structures, ASIO has a culture that encourages staff members to advise security or psychological services staff of changes in circumstances, either for themselves or colleagues about whom they are concerned.

Where risk factors are identified, strategies to assist staff are implemented through the Employee Assistance Program (EAP), which promotes active problem solving within a confidential setting.

Security audits are designed to ensure adherence to relevant security standards, to identify areas where improvement is needed or desirable and to enhance security in line with ASIO's commitment to security best practice

IT SECURITY

ASIO continues to monitor its computer networks for insecure, unauthorised and inappropriate usage. ASIO's Information and Communication Technology (ICT) audit capability has been upgraded to address the growth of both ICT capability and staff numbers.

BUILDING MANAGEMENT

In April 2005, to allow for the growth of ASIO and the Office of National Assessments and their continued co-location as recommended in the Flood Report, the Government committed $132.6 million over four years for an extension to ASIO's Central Office building in Canberra. However, construction of the extension was subsequently delayed pending the outcome of the Taylor Review.

In October 2005 the Government agreed to the Taylor Review recommendation to increase ASIO's staffing level to 1860 by 2010–11. As a consequence of this growth Government agreed that ASIO and the Office of National Assessments needed more adequate space and a new Central Office building was appropriate.

A number of options for the new building remained under consideration at the end of the period. The funding for the project is subject to normal budget processes and will be offset against the funding already provided for the superseded extension.

ASIO's growth also has put pressure on accommodation in our State and Territory offices.

ASIO's growth also has put pressure on accommodation in our State and Territory offices

ECOLOGICALLY SUSTAINABLE DEVELOPMENT AND ENVIRONMENTAL PERFORMANCE

ASIO monitors environmental performance and incorporates energy consumption measures into all its refurbishment works. Our most recently established office incorporates a range of energy management features including automatic self-dimming light fittings, timer controlled air-conditioning and lighting, waterless urinals and the use of grey water for toilet flushing. Double-glazing and insulation contribute to a high thermal performance.

Recycling of paper and cardboard waste was extended and the Uninterruptible Power Supply system was replaced with a more efficient system which incorporated power factor correction modules in the design. However, energy demand in our Central Office remained high as a result of the increased operational tempo, higher staffing levels, and expanded 24/7 operations.

PURCHASING

All purchasing activity in ASIO is conducted in accordance with the (classified) *Chief Executive's Instructions*, which require officers to have regard to 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 *Chief Executive's Instructions* are available to all staff via the Organisation's Intranet. The Instructions give direction on purchasing goods and services and entering into and managing contracts, agreements and arrangements. Staff members are provided with supporting guidance on procurement policy and practice, together with standard document templates.

In 2005–06 ASIO's annual investment program continued. Purchasing objectives focused on investment in key business areas, including technical capabilities and protective security measures. Additionally, procurement was conducted in relation to the enabling functions of information and communications technology infrastructure and office accommodation.

COMMONWEALTH PROCUREMENT GUIDELINES

To undertake ASIO's functions in relation to protecting Australia's security interests, ASIO's *Chief Executive's Instructions* direct officials to refrain from the mandatory procurement requirements where the protection of national security is in the public interest.

The Instructions also direct ASIO officers to refrain from publishing details relating to the Organisation's procurement activities and contracts, the disclosure of which could reasonably be expected to cause damage to national security.

Notwithstanding these specific exemptions, officers involved in procurement must have regard to the Commonwealth Procurement Guidelines.

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 Intelligence and Security.

CONSULTANTS

During 2005–06 ASIO let 8 consultancy contracts, down from 11 in 2004–05. The total expenditure during the year on consultancy contracts valued at $10 000 or more (including contracts let during the previous year) totalled $0.369 million, up from $0.158 million in 2004–05.

The decrease in new contracted consultancies during the year resulted from a narrower use of out-sourced expertise to inform agency decision making. The increase in total expenditure on consultancies is consistent with the Organisation's growth in size and volume of business activity. The main areas for consultancies were in corporate management, information technology and accommodation services.

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 Intelligence and Security on request.

Competitive tendering and contracting

ASIO released two Restricted Requests for Tender during 2005–06.

In each case the Requests for Tender were not advertised publicly for security reasons. Instead a restricted set of Government Endorsed Suppliers was invited to tender.

Parts of this performance report have been excluded from the unclassified *Report to Parliament* for reasons of national security.

PART 4: FINANCIAL STATEMENTS

AUDIT REPORT ON THE FINANCIAL STATEMENTS OF THE AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION

Australian National Audit Office

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 of Security;
- Income Statement, Balance Sheet and Statement of Cash Flows;
- Statement of Changes in Equity;
- Schedules of Commitments and Contingencies; and
- Notes to and forming part of the Financial Statements

of the Australian Security Intelligence Organisation for the year ended 30 June 2006.

The Director-General of Security 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 the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, Accounting Standards and other mandatory financial reporting requirements in Australia. The Director-General of Security 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.

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

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

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

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.

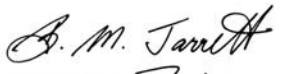
Audit Opinion

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, in accordance with the Finance Minister's Orders, applicable Accounting standards and other mandatory financial reporting requirements in Australia, of the Australian Security Intelligence Organisation's financial position as at 30 June 2006 and of its performance and cash flows for the year then ended.

Australian National Audit Office



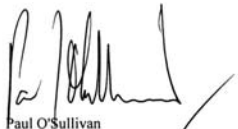
Brandon Jarrett
Executive Director

Delegate of the Auditor-General

Canberra
14 September 2006

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2006 have been prepared based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.



Paul O'Sullivan
Director-General of Security

14 September 2006

INCOME STATEMENT FOR THE YEAR ENDED 30 JUNE 2006

	Notes	2006 $'000	2005 $'000
INCOME			
Revenues			
Revenues from Government	4A	**174,845**	137,456
Goods and services	4B	**3,224**	2,624
Total Revenue		**178,069**	140,080
Gains			
Other gains	4C	**3,030**	2,369
Total Gains		**3,030**	2,369
TOTAL INCOME		**181,099**	142,449
EXPENSES			
Employees	5A	**91,430**	73,583
Suppliers	5B	**62,965**	57,291
Depreciation and amortisation	5C	**14,370**	10,847
Finance Costs	5D	**6**	5
Write-down and impairment of assets	5E	**424**	1,058
Net losses from sale of assets	5F	**70**	28
TOTAL EXPENSES		**169,265**	142,812
Operating result before income tax		**11,834**	(363)
Income tax equivalent expense		**–**	–
OPERATING RESULT		**11,834**	(363)

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

BALANCE SHEET AS AT 30 JUNE 2006

	Notes	2006 $'000	2005 $'000
ASSETS			
Financial Assets			
Cash and cash equivalents	6A	**12,742**	18,299
Receivables	6B	**40,738**	3,717
Other financial assets	6C	**165**	–
Total financial assets		**53,645**	22,016
Non-Financial Assets			
Land and buildings	7A,C	**24,643**	25,300
Infrastructure, plant and equipment	7B,C	**51,444**	37,809
Intangibles	7D	**3,363**	3,245
Other non-financial assets	7E	**1,336**	1,299
Total non-financial assets		**80,786**	67,652
TOTAL ASSETS		**134,431**	89,668
LIABILITIES			
Payables			
Suppliers	8A	**6,000**	3,773
Other payables	8B	**3,481**	2,732
Total payables		**9,481**	6,505
Interest bearing liabilities			
Lease Incentives	9	**1,313**	854
Total interest bearing liabilities		**1,313**	854
Provisions			
Employee Provisions	10A	**21,649**	17,274
Other provisions	10B	**2,518**	2,520
Total provisions		**24,167**	19,794
TOTAL LIABILITIES		**34,961**	27,153
NET ASSETS		**99,470**	**62,515**
EQUITY			
Contributed equity		**82,323**	56,714
Reserves		**8,947**	9,436
Retained surpluses or (accumulated deficits)		**8,200**	(3,635)
TOTAL EQUITY		**99,470**	62,515
Current assets		**54,981**	23,315
Non-current assets		**79,450**	66,353
Current liabilities		**27,814**	21,172
Non-current liabilities		**7,147**	5,981

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

STATEMENT OF CASH FLOWS FOR THE YEAR ENDED 30 JUNE 2006

	Notes	2006 $'000	2005 $'000
OPERATING ACTIVITIES			
Cash received			
Goods and services		**2,631**	1,134
Appropriations		**151,913**	137,456
Other Gains		**2,232**	1,214
Net GST received from ATO		**7,237**	6,155
Total cash received		**164,013**	145,959
Cash used			
Employees		**87,055**	73,833
Suppliers		**65,235**	55,890
Total cash used		**152,290**	129,723
Net cash from or (used by) operating activities	**11**	**11,723**	16,236
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		**611**	403
Total cash received		**611**	403
Cash used			
Purchase of property, plant and equipment		**29,054**	28,018
Purchase of intangibles		**1,399**	1,356
Total cash used		**30,453**	29,374
Net cash from or (used by) investing activities		**(29,842)**	(28,971)
FINANCING ACTIVITIES			
Cash received			
Capital injections		**12,562**	23,933
Total cash received		**12,562**	23,933
Cash used			
Repayment of debt		**–**	115
Total cash used		**–**	115
Net cash from or (used by) financing activities		**12,562**	23,818
Net increase or (decrease) in cash held		**(5,557)**	11,083
Cash at the beginning of the reporting period		**18,299**	7,216
Cash at the end of the reporting period	**6A**	**12,742**	18,299

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

STATEMENT OF CHANGES IN EQUITY FOR THE YEAR ENDED 30 JUNE 2006

	Accumulated Results		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2006	2005	**2006**	2005	**2006**	2005	**2006**	2005
	$'000	$'000	**$'000**	$'000	**$'000**	$'000	**$'000**	$'000
Opening Balance	**(3,635)**	(3,272)	**9,436**	9,496	**56,714**	32,781	**62,515**	39,005
Income and Expense								
Revaluation adjustment	**–**	–	**(489)**	(60)	**–**	–	**(489)**	(60)
Subtotal income and expenses recognised directly in equity	**–**	–	**(489)**	(60)	**–**	–	**(489)**	(60)
Net Operating Results	**11,834**	(363)	**–**	–	**–**	–	**11,834**	(363)
Total income and expenses	**11,834**	(363)	**(489)**	(60)	**–**	–	**11,345**	(423)
Transactions with Owners								
Contributions by Owners								
Appropriation (equity injection)	**–**	–	**–**	–	**25,609**	23,933	**25,609**	23,933
Sub-total Transactions with Owners	**–**	–	**–**	–	**25,609**	23,933	**25,609**	23,933
Transfers bewteen equity components	**–**	–	**–**	–	**–**	–	**–**	–
Closing Balance at 30 June	**8,200**	(3,635)	**8,947**	9,436	**82,323**	56,714	**99,470**	62,515

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

SCHEDULE OF COMMITMENTS AS AT 30 JUNE 2006

	Notes	2006 $'000	2005 $'000
BY TYPE			
Capital commitments			
Infrastructure, plant and equipment	A	**9,291**	5,180
Total capital commitments		**9,291**	5,180
Other commitments			
Operating leases	B	**85,603**	77,212
Other commitments		**14,044**	7,028
Total other commitments		**99,648**	84,240
Commitments receivable		**12,738**	2,194
Net commitments by type		**96,201**	87,226
BY MATURITY			
Capital commitments			
One year or less		**9,291**	5,180
From one to five years		**–**	–
Over five years		**–**	–
Total capital commitments		**9,291**	5,180
Operating lease commitments			
One year or less		**10,072**	11,378
From one to five years		**50,834**	45,516
Over five years		**24,698**	20,318
Total operating lease commitments		**85,603**	77,212
Other commitments			
One year or less		**14,044**	7,028
From one to five years		**–**	–
Over five years		**–**	–
Total other commitments		**14,044**	7,028
Commitments Receivable		**12,738**	2,194
Net commitments by maturity		**96,201**	87,226

NB: Commitments are GST inclusive where relevant

A. Plant and equipment commitments are primarily contracts for purchases of furniture and fittings for a new building
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 2006

Contingent liabilities	Claims for damages/costs		Total	
	2006	2005	**2006**	2005
	$ '000	$ '000	**$ '000**	$ '000
Balance from previous period	**200**	40	**200**	40
Re-measurement	**100**	200	**100**	200
Total Contingent Liabilities	**100**	200	**100**	200

Contingent assets	Claims for damages/costs		Total	
	2006	2005	**2006**	2005
	$ '000	$ '000	**$ '000**	$ '000
Balance from previous period	**–**	–	**–**	–
Re–measurement	**–**	–	**–**	–
Total Contingent Assets	**–**	–	**–**	–
Net Contingent Liabilities			**(100)**	(200)

Details of each class of contingent liabilities and assets, including those not included above because they cannot be quantified or are considered remote, are disclosed in Note 12: Contingent Liabilities and Assets.

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 2006

Note 1: Summary of Significant Accounting Policies

1.1 Objective of ASIO

The objective of ASIO is 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.

ASIO activities contributing towards the outcome are classified as departmental. Departmental activities involve the use of assets, liabilities, revenues and expenses controlled or incurred by ASIO in its own right.

The continued existence of ASIO in its present form and with its present programs is dependent on Government policy and on continuing appropriations by Parliament.

1.2 Basis of Preparation of the Financial Statements

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 2006)* 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 2006))*;
- Australian Accounting Standards issued by the Australian Accounting Standards Board that apply for the reporting period; and
- Interpretations issued by the Urgent Issues Group that apply for the reporting period.

This is the first financial report to be prepared under Australian Equivalents to International Financial Reporting Standards (AEIFRS). The impacts of adopting AEIFRS are disclosed in Note 2.

The Income Statement and Balance Sheet have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets and liabilities which, as noted, are at fair value or amortised cost. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position.

The financial report is presented in Australian dollars and values are rounded to the nearest thousand dollars unless disclosure of the full amount is specifically required.

Unless alternative treatment is specifically required by an accounting standard, assets and liabilities are recognised in the Balance Sheet when, and only when, it is probable that future economic benefits will flow and the amounts of the assets or liabilities can be reliably measured. However, assets and liabilities arising under agreements equally proportionately unperformed are not recognised unless required by an Accounting Standard. Liabilities and assets that are unrecognised are reported in the Schedule of Commitments and the Schedule of Contingencies (other than unquantifiable or remote contingencies, which are reported at Note 12).

Unless alternative treatment is specifically required by an accounting standard, revenues and expenses are recognised in the Income Statement when and only when the flow or consumption or loss of economic benefits has occurred and can be reliably measured.

1.3 Significant Accounting Judgements and Estimates

In the process of applying the accounting policies listed in this note, ASIO has made the following judgments that have the most significant impact on the amounts recorded in the financial statements:

- The fair value of land and buildings has been taken to be the market value of similar properties as determined by an independent valuer. In some instances, ASIO buildings are purpose built and may in fact realise more or less than the market.

No accounting assumptions or estimates have been identified that have a significant risk of causing a material adjustment to carrying amounts of assets and liabilities within the next accounting period.

1.4 Statement of Compliance

The financial report complies with Australian Accounting Standards, which include Australian Equivalents to International Financial Reporting Standards (AEIFRS).

Australian Accounting Standards require ASIO to disclose Australian Accounting Standards that have not been applied, for standards that have been issued but are not yet effective.

The AASB has issued amendments to existing standards, these amendments are denoted by the year and the number, for example 2005-1 indicates amendment 1 issued in 2005.

The table below illustrates standards and amendments that will become effective for ASIO in the future. The nature of the impending change within the table, has been, out of necessity, abbreviated and users should consult the full version on the AASB's website to identify the full impact of the change. The expected impact on the financial report of adoption of these standards is based on ASIO's initial assessments at this date, but may change. ASIO intends to adopt all of the standards upon their application.

Title	Standard affected	Application* date*	Nature of impending change	Impact expected on financial report
2005-1	AASB 139	1 Jan 2006	Amends hedging requirements for foreign currency risk of a probable intra-group transaction.	No expected impact.
2005-4	AASB 139, AASB 132, AASB 1, AASB 1023 and AASB 1038	1 Jan 2006	Amends AASB 139, AASB 1023 and ASB 1038 to restrict the option to fair value through profit or loss and makes consequential amendments to AASB 1 and AASB 132.	No expected impact.
2005-5	AASB 1 and AASB 139	1 Jan 2006	Amends AASB 1 to allow an entity to determine whether an arrangement is, or contains, a lease. Amends AASB 139 to scope out a contractual right to receive reimbursement (in accordance with AASB 137) in the form of cash.	No expected impact.
2005-6	AASB 3	1 Jan 2006	Amends the scope to exclude business combinations involving entities or businesses under common control.	No expected impact.
2005-9	AASB 4, AASB 1023, AASB 139 and AASB 132	1 Jan 2006	Amended standards in regards to financial guarantee contracts.	No expected impact.
2005-10	AASB 132, AASB 101, AASB 114, AASB 117, AASB 133, AASB 139, AASB 1, AASB 4, AASB 1023 and AASB 1038	1 Jan 2007 1 Jan 2007	Amended requirements subsequent to the issuing of AASB 7.	No expected impact.
2006-1	AASB121	31 Dec 2006	Changes in requirements for net investments in foreign subsidiaries depending on denominated currency.	No expected impact.
	AASB 7 Financial Instruments Disclosures	1 Jan 2007	Revise disclosure requirements for financial instruments from AASB 132 requirements.	No expected impact.

* Application date is for annual reporting periods beginning on or after the date shown

1.5 Revenue

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 recognised only when it has been earned.

Appropriations receivable are recognised at their nominal amounts.

Other revenue

Revenue from the sale of goods is recognised when:

- the risks and rewards of ownership have been transferred to the buyer;
- the seller retains no managerial involvement nor effective control over the goods;
- the revenue and transaction costs incurred can be reliably measured; and
- it is probable that the economic benefits associated with the transaction will flow to the entity.

Revenue from the rendering of a service is recognised by reference to the stage of completion of contracts at the reporting date. The revenue is recognised when:

- the amount of revenue, stage of completion and transaction costs incurred can be reliably measured; and
- the probable economic benefits with the transaction will flow to the entity.

The stage of completion of contracts at the reporting date is determined by reference to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

Receivables for goods and services, which have 30 days terms, are recognised at 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 no longer probable.

Interest revenue is recognised using the effective interest method as set out in AASB 139.

1.6 Gains

Resources Received Free of Charge

Services received free of charge are recognised as gains 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.

Contributions of assets at no cost of acquisition or for nominal consideration are recognised as gains at their fair value when the asset qualifies for recognition, unless received from other government agency as a consequence of a restructuring of administrative arrangements.

Other Gains

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

1.7 Transactions with the Government as Owner

Equity Injections

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.

1.8 Employee Benefits

As required by the Finance Minister's Orders, ASIO has early adopted AASB 119 Employee Benefits as issued in December 2004.

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.

Liabilities for 'short-term employee benefits' (as defined in AASB 119) and termination benefits due within twelve months of balance date are measured at their nominal amounts.

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

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

Leave

The liability for employee 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 of ASIO 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 long service leave has been determined by reference to *Finance Brief 27* issued by the 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 are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS) or the PSS accumulation plan (PSSap).

The CSS and PSS are defined benefit schemes for the Commonwealth. The PSSap is a defined contribution scheme.

The liability for defined 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.

From 1 July 2005, new employees are eligible to join the PSSap scheme.

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

1.9 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 rewards incidental to ownership of leased non-current assets. An operating lease is a lease that is not a finance lease. 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 either the fair value of the lease property or, if lower, the present value of minimum lease payments at the inception of the contract and a liability recognised at the same time and 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 straight line basis which is representative of the pattern of benefits derived from the leased assets.

1.10 Borrowing Costs

All borrowing costs are expensed as incurred.

1.11 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.

1.12 Financial Risk Management

ASIO's activities expose it to normal commercial financial risk. As a result of the nature of ASIO's business and internal and Australian Government policies dealing with the management of financial risk, ASIO's exposure to market, credit, liquidity and cash flow and fair value interest rate risk is considered to be low.

1.13 Derecognition of Financial Assets and Liabilities

As prescribed in the Finance Minister's Orders, ASIO has applied the option available under AASB 1 of adopting AASB 132 and 139 from 1 July 2005 rather than 1 July 2004.

Financial assets are derecognised when the contractual rights to the cash flows from the financial assets expire or the asset is transferred to another entity. In the case of a transfer to another entity, it is necessary that the risks and rewards of ownership are also transferred.

Financial liabilities are derecognised when the obligation under the contract is discharged or cancelled or expires.

For the comparative year, financial assets were derecognised when the contractual right to receive cash no longer existed. Financial liabilities were derecognised when the contractual obligation to pay cash no longer existed.

1.14 Impairment of Financial Assets

As prescribed in the Finance Minister's Orders, ASIO has applied the option available under AASB 1 of adopting AASB 132 and 139 from 1 July 2005 rather than 1 July 2004.

Financial assets are assessed for impairment at each balance date.

Financial Assets held at Amortised Cost

If there is objective evidence that an impairment loss has been incurred for loans and receivables or held to maturity investments held at amortised cost, the amount of the loss of estimated future cash flows discounted at the asset's original effective interest rate. The carrying amount is reduced by way of an allowance account. The loss is recognised in profit and loss.

Comparative Year

The above policies were not applied for the comparative year. For receivables, amounts were recognised and carried at original invoice amount less a provision for doubtful debts based on an estimate made when collection of the full amount was no longer probable. Bad debts were written off as incurred.

Other financial assets carried at cost which were not held to generate net cash inflows, were assessed for indicators of impairment. Where such indicators were found to exist, the recoverable amount of the assets was estimated and compared to the assets carrying amount and, if less, reduced to the carrying amount. The reduction was shown as an impairment loss.

1.15 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 (irrespective of having been invoiced).

1.16 Contingent Liabilities and Contingent Assets

Contingent Liabilities and Assets are not recognised in the Balance Sheet but are discussed in the relevant schedules and notes. They may arise from uncertainty as to the existence of a liability or asset, or represent an existing liability

or 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 or asset is recognised. A liability or asset is recognised when its existence is confirmed by a future event, settlement becomes probable (virtually certain for assets) or reliable measurement becomes possible

1.17 Acquisition of Assets

Assets are recorded at cost on acquisition except as stated below. The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken. Financial assets are initially measured at their fair value plus transaction costs where appropriate.

Assets acquired at no cost, or for nominal consideration, are initially recognised as assets and revenues at their fair value at the date of acquisition, unless acquired as a consequence of restructuring of administrative arrangements. In the latter case, assets are initially recognised as contributions by owners at the amounts at which they were recognised in the transferor agency's accounts immediately prior to the restructuring.

1.18 Property, Plant and Equipment (PP&E)

Asset Recognition Threshold

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

The initial cost of an asset includes an estimate of the cost of dismantling and removing the item and restoring the site on which it is located. This is particularly relevant to 'makegood' provisions in property leases taken up by ASIO where there exists an obligation to restore the property to its original condition. These costs are included in the value of ASIO's leasehold improvements with a corresponding provision for the 'makegood' taken up.

Revaluations

Basis

Land, buildings, plant and equipment are carried at fair value, being revalued with sufficient frequency such that the carrying amount of each asset is not materially different. Valuations undertaken in each 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	Depreciated replacement cost
Plant & equipment	Market selling price

Following initial recognition at cost, valuations are conducted with sufficient frequency to ensure that the carrying amounts of assets do not materially differ from the assets' fair values as at the reporting date. All ASIO's assets have been revalued at 30 June 2006 to fair value. The regularity of independent valuations depends upon the volatility of movements in market values for the relevant assets.

Revaluation adjustments are made on a class basis. Any revaluation increment is credited to equity under the heading of asset revaluation reserve except to the extent that it reverses a previous revaluation decrement of the same asset class that was previously recognised through profit and loss. Revaluation decrements for a class of assets are recognised directly through profit and loss except to the extent that they reverse a previous revaluation increment for that class. Any accumulated depreciation as at the revaluation date is eliminated against the gross carrying amount of the asset and the asset restated to the revalued amount.

Depreciation

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 rates (useful lives), residual values and methods are reviewed at each reporting date and necessary adjustments are recognised in the current, or current and future reporting periods, as appropriate.

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

	2006	2005
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

Impairment

All assets were assessed for impairment at 30 June 2006. Where indications of impairment exist, the asset's recoverable amount is estimated and an impairment adjustment made if the asset's recoverable amount is less than its carrying amount. The recoverable amount of an asset is the higher of its fair value less costs to sell and its value in use. Value in use is the present value of the future cash flows expected to be derived from the asset. Where the future economic benefit of an asset is not primarily dependent on the asset's ability to generate future cash flows, and the asset would be replaced if ASIO were deprived of the asset, its value in use is taken to be its depreciated replacement cost.

No indicators of impairment were found for assets at fair value.

1.19 Intangibles

ASIO's intangibles comprise internally developed software for internal use. The assets are carried at cost.

Software is amortised on a straight-line basis over their anticipated useful lives. The useful life of ASIO's software is 3 to 4 years (2004–05: 3 to 4 years).

All software assets were assessed for indications of impairment as at 30 June 2006.

1.20 Inventories

ASIO does not hold inventory for resale or distribution.

1.21 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.

1.22 Reporting of Administered Actitivities

ASIO has no administered items.

Note 2: The impact of the transition to AEIFRS from previous AGAAP

Reconciliation of total equity as presented under previous AGAAP to that under AEIFRS

	2005 $ '000	2004 $ '000
Reconciliation of Departmental Equity		
Total Departmental Equity under AGAAP	**60,647**	36,949
Adjustments to accumulated results		2,056
Adjustments to other reserves	**702**	–
Total Equity under AEIFRS	**62,515**	39,005
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)
Make Good	**(667)**	–
Provision for make good	**1,088**	1,088
Total Accumulated Results under AEIFRS	**(3,635)**	(3,272)
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 profit or loss as presented under previous AGAAP to AEIFRS

Prior year profit as previously reported	**526**
Adjustments:	
Depreciation	**(223)**
Suppliers	**(666)**
Prior year profit transalated to AEIFRS	**(363)**

AGAAP – Australian General Accepted Accounting Principles
AEIFRS – Australian Equivalents to International Reporting Standards

The Cash Flow Statement presented under previous AGAAP is equivalent to that prepared under AEIFRS.

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.

While ASIO previously recognised a provision for 'make good' on leased premises, it did not capitalise this cost in the value of the asset.

Note 3: Events after the Balance Sheet date

There were no events occurring after reporting date which had an effect on the 2006 financial statements.

	2006 $'000	2005 $'000
Note 4: Income		
Revenues		
Note 4A: Revenues from Government		
Appropriations for outputs	**174,845**	137,456
Total revenues from Government	**174,845**	137,456
Note 4B: Goods and services		
Goods	**14**	57
Services	**3,210**	2,567
Total sales of goods and services	**3,224**	2,624
Provision of goods to:		
Related entities	**6**	29
External entities	**8**	28
Total sales of goods	**14**	57
Rendering of services to:		
Related entities	**2,997**	2,387
External entities	**213**	180
Total rendering of services	**3,210**	2,567
Gains		
Note 4C: Other gains		
Resources received free of charge	**1,168**	1,154
Rent	**1,273**	807
Miscellaneous	**589**	408
Total other revenue	**3,030**	2,369

	2006 $'000	2005 $'000
Note 5: Operating Expenses		
Note 5A: Employee expenses		
Wages and salary	**66,459**	54,123
Superannuation	**11,970**	10,066
Leave and other entitlements	**3,676**	1,848
Separation and redundancies	**739**	167
Other employee expenses	**8,586**	7,379
Total employee expenses	**91,430**	73,583
Note 5B: Suppliers' expenses		
Provision of goods – related entities	**1,003**	585
Provision of goods – external entities	**6,022**	4,393
Rendering of services – related entities	**15,681**	15,815
Rendering of services – external entities	**30,539**	29,038
Operating lease rentals *	**9,128**	6,954
Workers' compensation premiums	**592**	506
Total supplier expenses	**62,965**	57,291
* These comprise minimum lease payments only.		
Note 5C: Depreciation and amortisation		
Depreciation		
Other infrastructure, plant and equipment	**13,011**	9,560
Buildings	**78**	105
Total Depreciation	**13,089**	9,665
Amortisation		
Intangibles – Computer Software	**1,281**	1,182
Total depreciation and amortisation	**14,370**	10,847
The aggregate amount of depreciation or amortisation expensed during the reporting period for each class of depreciable assets are as follows:		
Buildings on freehold land	**78**	105
Leasehold improvements	**4,431**	1,877
Plant and equipment	**8,580**	7,683
Internally developed software – in use	**1,281**	1,182
Total depreciation and amortisation	**14,370**	10,847

	2006 $'000	2005 $'000
Note 5D: Finance Costs		
Unwinding of discount	**6**	–
Leases	**–**	5
Total	**6**	5
Note 5E: Write down and impairment of assets		
Financial assets		
– Bad and doubtful debts expense	**–**	17
– Foreign exchange variations	**(3)**	5
Non-financial assets		
– Plant and equipment written off at stocktake	**–**	176
– Plant and equipment – other	**146**	28
– Plant and equipment – revaluation decrement	**281**	697
– Intangibles written off at stocktake	**–**	135
Total	**424**	1,058
Note 5F: Net losses from sale of assets		
Proceeds from disposals	**(611)**	(403)
Net book value of assets disposed	**681**	431
Net loss from sale of assets	**70**	28

Note 6: Financial Assets

Note 6A: Cash and cash equivalents		
Departmental	**12,742**	18,299
Total cash and cash equivalents	**12,742**	18,299

	2006 $'000	2005 $'000
Note 6B: Receivables		
Goods and services	**3,653**	2,502
Less allowance for doubtful debts	**–**	(17)
	3,653	2,485
GST receivable from the Australian Taxation Office	**1,106**	1,232
Appropriations Receivable:		
– for existing outputs	**35,979**	–
Total receivables (net)	**40,738**	3,717
Receivables is represented by:		
Current	**40,738**	3,717
Non-current	**–**	–
Total receivables (net)	**40,738**	3,717
All receivables are with entities external to the entity. Credit terms are net 30 days (2005: 30 days)		
Receivables (gross) are aged as follows:		
Current	**39,158**	3,381
Overdue by:		
Less than 30 days	**1,207**	94
30 to 60 days	**277**	20
60 to 90 days	**18**	3
More than 90 days	**78**	219
	1,580	336
Total receivables (gross)	**40,738**	3,717
The allowance for doubtful debts is aged as follows:		
Overdue by:		
More than 90 days	**–**	17
Total provision for doubtful debts	**–**	17
Note 6C: Other Financial Assets		
Accrued Revenue	**165**	–

	2006 $'000	2005 $'000
Note 7: Non-Financial Assets		
Note 7A: Land and buildings		
Freehold land		
–fair value	**1,575**	1,500
Total freehold land	**1,575**	1,500
Buildings on freehold land		
–fair value	**1,950**	2,019
–accumulated depreciation	**–**	–
Total buildings on freehold land	**1,950**	2,019
Leasehold improvements		
–fair value	**22,150**	22,487
–accumulated depreciation	**(1,032)**	(706)
Total buildings on freehold land	**21,118**	21,781
Total land and buildings (non-current)	**24,643**	25,300
Note 7B: Infrastructure, Plant and Equipment		
Infrastructure, plant and equipment		
– work in progress	**7,825**	1,660
– fair value	**43,619**	36,661
– accumulated depreciation	**–**	(512)
Total Infrastructure, Plant and Equipment (non-current)	**51,444**	37,809
All revaluations are conducted in accordance with the revaluation policy stated in Note 1. In 2005–06, an independent valuer from the Australian Valuation Office conducted the revaluations.		
The following amounts were credited (debited) to the asset revaluation reserve by asset class and included in the equity of the balance sheet:		
Land	**75**	160
Buildings	**9**	(7)
Leasehold improvements	**(642)**	296
Plant & equipment	**69**	(1,205)
	(489)	(756)

Note 7C: Analysis of Property, Plant and Equipment

TABLE A – Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment

Item	Land	Buildings	Buildings– Leasehold Improvements	Total Buildings	Total Land & Buildings	Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000	$'000	$'000
As at 1 July 2005							
Gross book value	1,500	2,019	22,487	24,506	26,006	38,321	64,327
Accumulated depreciation / amortisation	–	–	(706)	(706)	(706)	(512)	(1,218)
Opening Net Book Value	1,500	2,019	21,781	23,800	25,300	37,809	63,109
Additions:							
by purchase	–	–	5,442	5,442	5,442	22,977	28,419
Net revaluation increment/(decrement)	75	9	(642)	(633)	(558)	69	(489)
Depreciation/ amortisation expense	–	(78)	(4,430)	(4,508)	(4,508)	(8,580)	(13,089)
Recoverable amount write-downs	–	–	–	–	–	–	–
Disposals:							
from disposal of operations	–	–	–	–	–	–	–
other disposals	–	–	–	–	–	(831)	(831)
As at 30 June 2006							
Gross book value	1,575	1,950	22,150	24,101	25,675	51,444	77,119
Accumulated depreciation / amortisation	–	–	(1,032)	(1,032)	(1,032)	–	(1,032)
Closing Net book value	**1,575**	**1,950**	**21,118**	**23,069**	**24,643**	**51,444**	**76,087**

TABLE B – Property, Plant, Equipment under Construction

Item	Land	Buildings	Buildings– Leasehold Improvements	Total Buildings	Total Land & Buildings	Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000	$'000	$'000
Carrying amount at 30 June 2006	–	–	–	–	–	**7,825**	**7,825**
Carrying amount at 30 June 2005	–	–	–	–	–	1,660	1,660

	2006 $'000	2005 $'000
Note 7D: Intangible Assets		
Computer Software		
Purchased – at cost	**10,320**	8,934
Accumulated amortisation	**(6,957)**	(5,689)
Total intangibles (non-current)	**3,363**	3,245

TABLE A – reconciliation of opening and closing balances of intangibles

Item	Computer software internally developed $'000	Computer software purchased $'000	Other intangibles internally developed $'000	Other intangibles purchased $'000
As at 1 July 2005				
Gross book value	–	8,934	–	–
Accumulated amortisation	–	(5,689)	–	–
Opening Net book value	–	3,245	–	–
Additions:				
Purchase/Internally developed	–	1,401	–	–
Movements:				
Amortisation	–	(1,281)	–	–
Disposals:				
other disposals		(2)		
As at 30 June 2006				
Gross book value	–	10,320	–	–
Accumulated amortisation	–	(6,957)	–	–
Closing Net Book Value	**–**	**3,363**	**–**	**–**

	2006 $'000	2005 $'000
Note 7E: Other non-financial assets		
Prepayments	1,336	1,299
All other non-financial assets are current assets		

Note 8: Payables

Note 8A: Suppliers		
Trade Creditors	6,000	3,765
Operating lease rentals	–	8
Total supplier payables	6,000	3,773
Supplier payables are represented by:		
Current	6,000	3,773
Non-Current	–	–
Total supplier payables	6,000	3,773
Settlement is usually made net 30 days.		
Note 8B: Other Payables		
Accrued expenses	3,481	2,732
Total other payables	3,481	2,732
All other payables are current liabilities		

Note 9: Interest Bearing Liabilities

Lease Incentives	1,313	854
Interest bearing liabilities are represented by:		
Current	657	229
Non-Current	656	625
Total other interest bearing liabilities	1,313	854

	2006 $'000	2005 $'000
Note 10: Provisions		
Note 10A: Employee provisions		
Salaries and wages	**995**	221
Leave	**20,288**	16,607
Superannuation	**108**	47
Other	**258**	399
Total employee provisions	**21,649**	17,274
Current	**17,516**	14,248
Non-current	**4,133**	3,026
Total employee provisions	**21,649**	17,274
Note 10B: Other provisions		
Provision for make good	**2,518**	2,520
Total other provisions	**2,518**	2,520
Carrying amount at beginning of period	**2,520**	
Additional provisions made	**196**	
Revaluations	**(204)**	
Unwinding of discounted amount arising from the passage of time	**6**	
Amount owing at end of period	**2,518**	

ASIO currently has agreements for the leasing of premises which have provisions requiring ASIO to restore the premises to their original condition at the conclusion of the lease. ASIO has made a provision to reflect the present value of this obligation.

	2006 $'000	2005 $'000
Note 11: Cash flow reconciliation		
Reconciliation of Cash per Income Statement to Statement of Cash Flows:		
Cash at year end per Statement of Cash Flows	**12,742**	18,299
Balance Sheet items comprising above cash: 'Financial Asset – Cash'	**12,742**	18,299
Reconciliation of operating result to net cash from operating activities:		
Operating result	**11,834**	526
Depreciation/amortisation	**14,370**	10,624
Net write down of non-financial assets	**427**	1,036
Net loss on disposal of assets	**70**	28
Lease incentives utilised	**459**	951
Lease make good	**2,056**	–
(Increase)/Decrease in receivables	**(23,974)**	(1,872)
(Increase)/Decrease in accrued revenue	**(165)**	–
(Increase)/Decrease in prepayments	**(37)**	148
Increase/(Decrease) in employee provisions	**4,375**	256
Increase/(Decrease) in provision for make good	**(2)**	1,887
Increase/(Decrease) in supplier payables	**2,518**	3,121
Increase/(Decrease) in accrued expenses	**458**	(469)
Net cash from/(used by) by operating activities	**12,389**	16,236

Note 12: Contingent Liabilities and Assets

Quantifiable contingencies

The Schedule of Contingencies in the financial statements reports a contingent liability as at 30 June 2006 in respect of claims for damages/costs of $100,000 (2005: $200,000). The amount represents an estimate of ASIO's liability based on precedent cases. ASIO is defending the claims.

Unquantifiable contingencies

At 30 June 2006, 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 13: Executive Remuneration

The number of executive officers who received or were due to receive a total remuneration of $130,000 or more:

	2006	2005
$130 000 to $144 999	**2**	2
$145 000 to $159 999	**4**	1
$160 000 to $174 999	**1**	1
$175 000 to $189 999	**6**	5
$190 000 to $204 999	**2**	5
$205 000 to $219 999	**5**	1
$220 000 to $234 999	**4**	3
$235 000 to $249 999	**1**	1
$250 000 to $264 999	**1**	2
$265 000 to $279 999	**3**	1
$295 000 to $309 999	**1**	–
$310 000 to $324 999	**–**	1
$325 000 to $339 999	**1**	–
$385 000 to $399 999	**1**	–
$400 000 to $414 999	**–**	1
The aggregate amount of total remuneration of executive officers shown above.	**$6,869,799**	$5,245,105
The aggregate amount of separation and redundancy/termination benefit payments during the year to executive officers shown above.	**nil**	$95,893

Note 14: Remuneration of Auditors

Financial statement audit services are provided free of charge to ASIO.	**2006**	2005
The fair value of audit services provided was:		
Australian National Audit Office (ANAO)	**$69,500**	$60,000

Included in the 2005 amount above, is an amount of auditor remuneration relating to the 2004–05 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 15: Staffing Levels

	2006	2005
Total Full Time Equivalent staffing levels for ASIO at the end of the year were:	**1062**	894

Note 16: Financial Instruments

Note 16A: Interest Rate Risk

Financial Instrument	Note	Non-Interest Bearing		Total		Weighted Average Effective Interest Rate	
		2006	2005	**2006**	2005	**2006**	2005
		$'000	$'000	**$'000**	$'000	**%**	%
Financial Assets							
Cash at bank	6A	**12,742**	18,299	**12,742**	18,299	**–**	–
Receivables for goods and services (gross)	6B	**3,653**	2,502	**3,653**	2,502	**n/a**	n/a
Total		**16,395**	20,801	**16,395**	20,801		
Total Assets				**134,431**	87,800		
Financial Liabilities							
Trade creditors	8A	**6,000**	3,773	**6,000**	3,773	**n/a**	n/a
Total		**6,000**	3,773	**6,000**	3,773		
Total Liabilities				**34,961**	27,153		

Note 16B: Fair Values of Financial Assets and Liabilities

All financial assets and liabilities are carried at fair value.

Note 16C: 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 Balance Sheet.

ASIO has no significant exposures to any concentrations of credit risk.

Note 17: Appropriations

Note 17A: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriation

Particulars	Total	
	2006	2005
	$	$
Balance carried forward from previous year	**13,128,617**	7,215,726
Correction in prior year error in disclosure	**822,138**	(1,739,000)
Unspent prior year appropriation – ineffective s31	**–**	(5,476,479)
Adjusted balance carried forward	**13,950,755**	247
Appropriation Act (No.1)	**171,727,000**	134,729,000
Appropriation Act (No.3)	**3,118,000**	2,727,000
Refunds credited (FMAA s30)	**370,499**	–
Sub-total Annual Appropriation	**175,215,499**	137,456,000
Appropriations to take account of recoverable GST (FMAA *s30A*)	**5,981,173**	4,104,750
Annotations to 'net appropriations' (FMAA *s31*)	**5,104,696**	–
30 June 2005 – variation – s31	**–**	8,254,149
Total appropriations available for payments	**200,252,123**	149,815,146
Cash payments made during the year (GST inclusive)	**168,924,335**	136,686,529
Balance of Authority to draw cash from the CRF for Ordinary Annual Services Appropriations	**31,327,788**	13,128,617
Represented by:		
Cash at bank and on hand	**7,772,139**	13,128,617
Receivables – departmental appropriations	**22,932,654**	–
Receivables – GST receivable from customers	**332,059**	223,000
Receivables – GST receivable from the ATO	**903,544**	1,231,248
Less: Payables – GST payable to suppliers	**(612,608)**	(1,454,248)
Total	**31,327,788**	13,128,617

Note 17B: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriation

Particulars	Total	
	2006	2005
	$	$
Balance carried from previous year	**5,171,091**	–
Correction of prior year error in disclosure	**–**	1,739,000
Appropriation Act (No.2)	**14,201,000**	18,011,000
Appropriation Act (No.4)	**11,408,000**	5,922,000
Sub-total Annual Appropriation	**30,780,091**	25,672,000
Appropriations to take account of recoverable GST (FMAA *s30A*)	**1,256,242**	2,050,091
Total appropriations available for payments	**32,036,333**	27,722,091
Cash payments made during the year (GST inclusive)	**13,818,665**	22,551,000
Balance of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriations	**18,217,668**	5,171,091
Represented by:		
Cash at bank and on hand	**4,968,438**	5,171,091
Appropriation Receivable	**13,046,577**	–
GST receivable from the ATO	**202,653**	–
Total	**18,217,668**	5,171,091

Note 17C: 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 2006 and 30 June 2005, both special accounts had nil balances and there were no transactions debited or credited to them. For the periods 2004–05 and 2005–06 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 2004–05 and 2005–06 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 2004–05 and 2005–06 ASIO has not used section 39 of the FMA Act regarding investments in respect of this Special Account.

Note 18: Compensation and Debt Relief

	2006	2005
	$	$
Eleven payments were made during the reporting period under the 'Defective Administration Scheme'. (2005: No payments made).	**$114,623**	Nil
No payments were made under s73 of the *Public Service Act 1999* during the reporting period. (2005: No payments made).	**Nil**	Nil
No waivers of amounts owing to the Commonwealth were made pursuant to subsection 34(1) of the *Financial Management and Accountability Act 1997*. (2005: No payments made).	**Nil**	Nil

Note 19: Reporting of Outcomes

Note 19A: Net Cost of Outcome Delivery

	Total	
	2006	2005
	$'000	$'000
Total expenses	**169,876**	143,215
Total Costs recovered (from provision of goods and services to the non-government sector)	**221**	208
Other external revenues		
Revenue from disposal of assets	**611**	403
Other	**1,862**	1,215
Goods and services revenue from related entities	**3,003**	2,416
Total Other external revenues	**5,476**	4,034
Net cost / (contribution) of outcome	**164,179**	138,973

ASIO does not report its revenue and expenses at output level.

PART 5: APPENDICES

APPENDIX A
PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

On 2 December 2005 the Parliamentary Joint Committee on ASIO, ASIS and DSD was replaced by the Parliamentary Joint Committee on Intelligence and Security. The size of the committee increased with two additional members. It now comprises nine members, four from the Senate and five from the House of Representatives. Five members are from the Government and four are from the Opposition. Membership of the PJCAAD/PJCIS during the reporting year was:

Hon. David Jull, MP (Chair)	Liberal Party, QLD
Mr Anthony Byrne, MP (Deputy Chair)	Australian Labor Party, VIC
Senator Alan Ferguson	Liberal Party, SA
Senator the Hon. Robert Ray	Australian Labor Party, VIC
Senator the Hon. John Faulkner (from 9 December 2005)	Australian Labor Party, NSW
Senator Fiona Nash (from 9 May 2006)	National Party, NSW
Mr Stewart McArthur, MP	Liberal Party, VIC
The Hon. Duncan Kerr, SC, MP	Australian Labor Party, TAS
Mr Steven Ciobo MP (from 8 December 2005)	Liberal Party, QLD
The following members left the Committee during the reporting period:	
Senator Sandy Macdonald (to 6 July 2005)	National Party, NSW
Senator Julian McGuaran (from 8 September 2005 to 28 March 2006)	Formerly National Party, VIC now Liberal 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 8: National Criticality Categories

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

Table 9: Critical Infrastructure Sectors

APPENDIX C
WORKFORCE STATISTICS

Group	Total staff[1]	Women	Race/ Ethnicity[2]	ATSI[3]	PWD[4]	Available EEO data[5]
SES (excluding DG)	28	6	0	0	0	27
Senior Officers[6]	236	77	26	0	3	220
AO5[7]	358	163	76	1	3	346
AO1–4[8]	427	254	52	2	7	377
ITO1–2[9]	58	9	12	1	1	54
ENG1–2[10]	3	0	0	0	0	3
Total	1 110	509	166	4	14	1 027

[1] Based on staff salary classifications recorded in ASIO's human resource management information system.
[2] Previously Non-English speaking background (NESB1 and NESB2)
[3] Aboriginal and Torres Strait Islander.
[4] People with a disability.
[5] Provision of EEO data is voluntary.
[6] Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications.
[7] ASIO Officer Grade 5 translates to APS Level 6 and includes Intelligence Officers.
[8] Translates to span the APS 1 to 5 classification levels. Intelligence Officer trainees are included in this group (equivalent to APS Level 3).
[9] Information Technology Officers Grades 1 and 2.
[10] Engineers Grades 1 and 2

Table 10: Representation of designated groups within ASIO at 30 June 2006

Group	June 2002	June 2003	June 2004	June 2005	June 2006
Women[1]	40	42	41	43.14	45.86
Race/Ethnicity[2]	11	12	11	14.64	16.16
ATSI[3]	0.75	0.74	0.41	0.45	0.38
PWD[4]	4	4	2	1.59	1.36

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

Table 11: Percentage representation of designated groups in ASIO 2002–2006.

APPENDIX C CONTINUED
WORKFORCE STATISTICS

	2002–03	2003–04	2004–05	2005–06
Ongoing full-time	536	603	693	800
Non-ongoing full-time[1]	51	103	155	178
Ongoing part-time	28	38	43	50
Non-ongoing part-time	23	28	22	27
Non-ongoing casual	30	33	42	55
Total	668	805	955	1 110

[1] Includes 15 secondees and 5 locally engaged staff and 5 contractors/consultants.

Table 12: Composition of workforce 2002–03 to 2005–06

		2001–02	2002–03	2003–04	2004–05	2005–06
Band 1	Female	2	2	2	4	5
	Male	8	9	9	10	17
Band 2	Female	1	1	1	1	1
	Male	2	4	4	4	4
Band 3	Male	1	1	1	1	1
Total		14	17	17	20	28

Table 13: SES equivalent staff classification and gender 2001–02 to 2005–06. (Does not include the Director-General).

APPENDIX D
ASIO SALARY CLASSIFICATION STRUCTURE AT 30 JUNE 2006

ASIO MANAGERS			
SES Band 3	$169 840		minimum point
SES Band 2	$134 242		minimum point
SES Band 1	$112 592		minimum point
AEO 3	$97 831		
AEO 2	$88 751	to	$97 831
AEO 1	$78 258	to	$84 474

INTELLIGENCE OFFICERS			
IO	$59 757	to	$68 160

ASIO OFFICERS			
ASIO Officer 5	$59 757	to	$68 160
ASIO Officer 4	$49 285	to	$53 798
ASIO Officer 3	$42 978	to	$46 310
ASIO Officer 2	$37 848	to	$41 865
ASIO Officer 1	$33 546	to	$36 980

ASIO ITOs			
SITOA	$97 831		
SITOB	$88 751	to	$97 831
SITOC	$78 258	to	$84 474
ITO2	$59 757	to	$68 160
ITO1	$46 310	to	$53 798

ASIO ENGINEERS			
SIO(E)5	$97 831		
SIO(E)4	$88 751	to	$97 831
SIO(E)3	$78 258	to	$84 474
SIO(E)2	$59 757	to	$68 160
SIO(E)1	$46 310	to	$53 798

Table 14: ASIO salary classification structure at 30 June 2006

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

ACC	ASIO Consultative Council
AFP	Australian Federal Police
AGCTPC	Australian Government Counter–Terrorism Policy Committee
AIC	Australian Intelligence Community
APEC	Asia Pacific Economic Cooperation
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
CBR	Chemical Biological and Radiological
CTITP	Counter-Terrorism Intelligence Training Program
DFAT	Department of Foreign Affairs and Trade
DSD	Defence Signals Directorate
EAP	Employee Assistance Program
ESO	External Security Organisation – Hizballah
IASF	Inter-Agency Security Forum
ICC	Intelligence Coordination Committee
ICT	Information and Communication Technology
DETF	Inter-Departmental Emergency Task Force
NCTP	National Counter-Terrorism Plan
NIG	National Intelligence Group
NTAC	National Threat Assessment Centre
PKK	Kurdistan Workers Party
SCEC	Security Construction and Equipment Committee
TSU	Technical Support Unit
WMD	Weapons of Mass Destruction

COMPLIANCE INDEX

GENERAL INDEX

A

B

F

G

H

I

J

K

L

M

R

S

Y

Z