Australian Government

Australian Security Intelligence Organisation

ASIO Report to Parliament

2006–2007

OUR VISION

The intelligence edge for a secure Australia.

OUR MISSION

To identify and investigate threats to security and provide advice to protect Australia, its people and its interests.

OUR VALUES

Excellence

Integrity

Cooperation

Accountability

Australian Security Intelligence Organisation

REPORT TO PARLIAMENT 2006–07

ISSN 0815-4562
ISBN 0978-0-9751485-4-9

Produced and printed by the Australian Security Intelligence Organisation.

Australian Government

Australian Security Intelligence Organisation

Director-General of Security

Reference: eA1060591

18 September 2007

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 have separately submitted to you the classified Annual Report on ASIO for the year ending 30 June 2007.

The distribution of that classified Annual Report is limited. Under cover of this letter, I present to you an unclassified version for tabling in the Parliament.

In addition, as required by the *Commonwealth Fraud Control Guidelines 2002*, I certify that I am satisfied that ASIO has in place appropriate fraud control mechanisms that meet the Organisation's needs and that comply with the Guidelines applying in 2006–07.

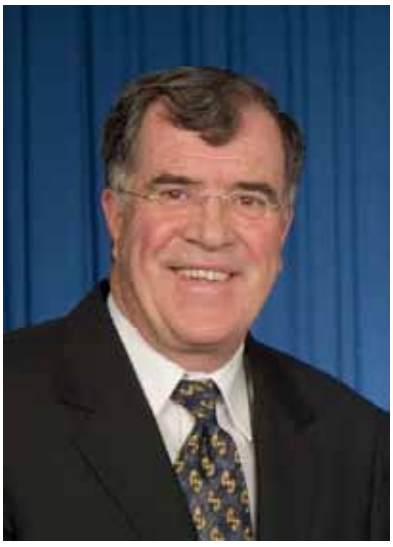
Yours sincerely,

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



Mr Paul O'Sullivan
Director-General of Security

A MESSAGE FROM THE DIRECTOR-GENERAL

In the years since 2001, ASIO's capabilities have been stretched – at times to challenging levels – by the demands of the heightened security environment. As a consequence we have, of necessity, given even greater emphasis to prioritisation and risk management, we have slowed growth on some non counter-terrorism related functions and our focus has been largely, but not exclusively, fixed on known threats. Such measures are not taken lightly and are not without consequence.

Since 2001, Government has committed significant budgetary and staffing increases to ASIO and the broader whole-of-government counter-terrorism effort. While the benefits of these resource increases have been felt incrementally in ASIO over recent years, it was in 2006–07, with the injection of resources following the 2005 Taylor Review, that the breadth and depth of the growth in capability was realised across the Organisation.

In 2006–07, we were more capable, more effective and more productive than in any year since 2001. We recruited more staff than in any previous year. We improved our complex analysis capability and strengthened engagement with Australian agencies and international partners. Our surveillance capacity grew, we bolstered the number of well trained and highly skilled intelligence officers on the ground, and our in-house technical capabilities and those developed in cooperation with key partners advanced. Consequently, we can manage more effectively multiple high priority investigations in diverse locations and for longer durations.

In 2006–07, we continued to work closely with law enforcement partners in supporting terrorism-related prosecutions – an important component of our work and one that continues to trend upwards in volume and complexity. Border security remained a key focus in 2006–07, with progress on improved processes, including electronic connectivity with key partners. This year we began to build momentum in areas other than counter-terrorism, including counter-espionage and foreign interference. We strengthened engagement with the private sector. Internally, we enhanced governance and accountability frameworks. Externally, scrutiny and oversight by Government, the Parliament and the Inspector-General of Intelligence and Security remained robust and comprehensive.

Earlier this year, after extensive internal and external consultation, I released ASIO's *Corporate Plan 2007–2011*. A new feature, and one which gives greater emphasis to our strategic direction, is the outline of where ASIO sees itself in 2012. I commend the document to you.

With the increased funding from Government comes, appropriately, increased expectations, both internal and external. The men and women of ASIO take their responsibilities very seriously. We all appreciate there is no place for complacency and there can be no guarantees of immunity from terrorism. The threat is real and deadly. But there is no doubt ASIO is better placed to identify and counter such threats than it was 12 months ago. And we will be stronger still in 12 months time.

Finally, I would like to take this opportunity to acknowledge the good work undertaken by the staff of ASIO in the past year, as well as the valuable assistance provided by partner agencies – both Australian and international – and the public. We must all continue to work together on safeguarding Australia and its interests.

Paul O'Sullivan

Director-General of Security

ASIO AND ITS ANNUAL REPORT

WHAT ASIO DOES

The Australian Security Intelligence Organisation (ASIO) was established in 1949 as Australia's national security service. ASIO operates under the control of the Director-General of Security who is responsible to the Attorney-General.

ASIO's role is to identify and investigate threats to security, both in Australia and overseas, and to provide advice to protect Australia, its people and its interests. ASIO's functions are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

Security is defined in the ASIO Act as:

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

It also includes the carrying out of Australia's responsibilities to any foreign country in relation to threats to security.

ASIO collects information using intelligence methods (such as human sources, special powers authorised by warrant, and through its liaison relationships) as well as from published sources.

ASIO is the only Australian intelligence agency which both collects and assesses security intelligence.

The ASIO Act does not limit the rights of persons to engage in lawful advocacy, protest or dissent. ASIO does not carry out criminal investigations nor have powers of arrest, but does cooperate with Australian law enforcement agencies to assist with criminal investigations that have a national security dimension.

Further information about ASIO can be found on our website at www.asio.gov.au, including this annual *Report to Parliament* and statements made by the Director-General.

ASIO's corporate vision, mission and values are contained in its *Corporate Plan 2007–2011* which is available at www.asio.gov.au.

THIS REPORT

Section 94 of the ASIO Act requires the Director-General, as soon as practicable after 30 June, to furnish the Minister with a report on the activities of the Organisation. The Minister is required to table an unclassified 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 Prime Minister, the Attorney-General, other members of the National Security Committee of Cabinet 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.

ASIO is the only Australian intelligence agency to produce an unclassified *Report to Parliament*.

PART 1: OVERVIEW

YEAR IN REVIEW

On the first day of the review period, Saturday 1 July 2006, a seventeen minute audio statement attributed to Usama bin Laden was released.

- Bin Laden did not mention Australia by name, and did not point to specific attacks, but he did praise the 'heroic operations' of the Mujahideen in attacking the American forces and their allies in Iraq, which includes Australia.
- Bin Laden also stated that al-Qa'ida reserves 'the right to punish them on their own land and in any available place at any time or in any way which is convenient for us'.

Such statements underline the ongoing and dangerous terrorist threat to Australia and its interests worldwide.

Action by authorities in Australia and around the world in recent years has had an impact on the capabilities of al-Qa'ida and others, but has not eradicated the threat. Extremists have shown themselves to be patient, persistent and innovative, and continue to attract new followers. They represent a threat that will confront us and many other countries for a long time. Any hiatus between attacks, including those directed against Australians, cannot be considered to signal the end of the threat.

The flow of threat-related intelligence to ASIO continued to increase in 2006–07 and resulted in the Organisation issuing 1 982 Threat Assessments.

The volatile security environment in many places around the world means that more Australians are likely to feel the impact of terrorism, either directly or indirectly.

This presents some significant challenges for ASIO. In October 2005, in recognition of this situation, the Government committed additional resources that will see ASIO grow in a planned and systematic way to around 1 860 staff by 2010–11. It was during 2006–07 that this growth in capability and size started to gather momentum.

COUNTER-TERRORISM

Countering the threat of terrorism directed against Australians and Australian interests, both in Australia and abroad, continued to be the major focus for ASIO.

The national counter-terrorism alert level remained unchanged at medium, which means that a terrorist attack could occur. The alert level was raised to medium following the terrorist attacks in the United States in 2001, and is likely to be at least at medium for some time.

For much of 2006–07, ASIO was involved in contributing to the preparations for the Asia-Pacific Economic Cooperation (APEC) forum aimed at delivering a safe and successful event.

ASIO had a role in supporting the litigation process in connection with individuals who were facing terrorism-related charges through the provision of information, witnesses and other support. In 2006–07, ASIO had the greatest litigation-related workload it has ever experienced, comprising security-related criminal proceedings (including terrorism prosecutions), judicial and administrative reviews of security assessments and other civil proceedings.

In recognition of this upward trend in the litigation workload – one that is likely to continue for some time – ASIO now has a new Legal Division and a Terrorism Litigation Advice Branch within the Investigative Analysis and Advice Division. ASIO has enhanced its legal capabilities but demands on this area remain high; the recruitment of further resources will be required.

The National Security Hotline has been a useful source of leads with over 1 990 new leads generated this financial year; some months required over 300 leads to be considered. In addition, ASIO was

referred leads from other agencies. As with previous years, ASIO, working with police, must quickly assess which leads require priority investigation.

Counter-terrorism checking continued to be an important element in preventing harm in Australia, and ASIO completed 134 981 checks, with none resulting in an adverse assessment.

ASIO also completed some 20 856 assessments for access to national security information, again with none resulting in the denial of access.

VIOLENT PROTEST

Politically motivated violence in the form of violent protest activity occurred in November 2006 in connection with the G20 Finance Ministers' Meeting in Melbourne.

COUNTER-PROLIFERATION

As part of the 2005–06 Budget, ASIO received funding to boost resources devoted to countering the proliferation of weapons of mass destruction. In the current reporting period, ASIO continued to work with other Australian and international agencies on this important work.

COUNTER-ESPIONAGE AND FOREIGN INTERFERENCE

In 2006–07, ASIO continued to enhance its capabilities directed at countering the threats of espionage and foreign interference in Australia. The creation of a separate division with responsibility for this aspect of ASIO's work has provided a framework for boosting this capability.

INTERNATIONAL FOCUS AND CAPABILITIES

In a world where a range of security threats can originate onshore and offshore, and which inevitably transcend national borders, ASIO's focus and reach must be global.

INTERNATIONAL LIAISON

ASIO has close and long-standing liaison relationships with many security, intelligence and law enforcement agencies overseas. In 2006–07, that liaison network grew to encompass 306 agencies in 120 countries. While some of this reflected organisational change in a number of countries, it also was driven by the need to engage in areas where ASIO has not previously needed to focus. In a dynamic global security environment, it is likely that ASIO will need to extend its international liaison network further.

In 2006–07, ASIO's network of liaison officers increased.

ASIO continued to enhance its electronic communication links.

We strengthened relationships with visits by the Director-General to international partners, visits by members of the senior management team, and by working-level visits spanning analytical exchange and training and technical activities.

ASIO also hosted visits to Australia by foreign services.

Such visits, at all levels, serve to give prominence to Australian interests in the minds of our partners, enhance capabilities of all agencies, and nurture the personal links between agencies that are so important in times of crisis.

While much of ASIO's intelligence work requires quite specific and tailored training, we continued to identify and leverage off the capabilities of Australian agencies and some of our international partners. In addition, ASIO continued to work with key regional and international partners for mutual benefit, including

through the Counter-Terrorism Intelligence Training Program.

BORDER SECURITY

ASIO's global focus and reach means it has a key role to play in Australia's border security arrangements. The prevention of harm to Australian interests relies, in part, on preventing entry to Australia by people assessed to be a threat to security.

ASIO has been building its capability to contribute to Australia's border security effort. In late 2005, ASIO implemented a 24x7 border security unit which continued to grow over the reporting period. In addition, ASIO has worked closely with the other Australian border security agencies, particularly the Department of Immigration and Citizenship and the Australian Customs Service, to improve visa security assessment processing times and to ensure that people of security interest are not able to enter Australia. That task continues to increase in complexity as people of security interest become more adept at concealing their identities, activities or intentions.

The volume of this important work continued to increase steadily from previous years.

In 2006–07, ASIO completed 53 387 visa security assessments and issued adverse assessments in relation to seven individuals seeking entry to Australia. This advice was based on rigorous assessments of the potential threat to Australia's security of allowing these individuals entry.

The other side of the security equation is the denial of the opportunity for Australian citizens to travel to other countries with a view to engaging in activities that would be inimical to the security of Australia or to any other country. In the last year, ASIO issued security assessments on a very small number of Australians that resulted in action by the Department of Foreign Affairs and Trade to cancel or deny them issue of a new or replacement Australian passport.

CAPABILITY ENHANCEMENTS

ASIO's growth during 2006–07 continued in a planned and strategic manner. Capabilities were boosted across all of the Organisation's functions.

ASIO's budget increased to $234.8m in 2006–07, up from $181.1m in 2005–06, and is expected to grow to $423.9m by 2010–11.

STRENGTHENING ENGAGEMENT

Over the course of the year, ASIO introduced a range of new analytical products tailored to the needs of particular clients.

Previous client surveys clearly indicate that our customers value the perspective ASIO provides, and the product that flows from our international liaison network. With growth, ASIO has been better placed to meet client demand.

ASIO refined and strengthened its engagement with key Australian partners. One of the aims of this engagement is to build the level of knowledge and understanding by key partners about ASIO's business and the unique security intelligence aspects of our work within the Australian Intelligence Community.

ASIO also continued to build and enhance its engagement with the private sector, including with the owners and operators of critical infrastructure. In 2006–07, ASIO released 33 Threat Assessments on vital infrastructure. The Business Liaison Unit website grew and now has over 200 subscribers. The Director-General also addressed four leading business fora, further underpinning ASIO's commitment to this developing aspect of our work.

TECHNOLOGY AND SUPPORT TO OPERATIONS

In recognition of the important role of technology and technical capabilities, refinements to the organisational structure

boosted the senior management arrangements in the Technical Capabilities Division and created a new Information Division.

ASIO continued to perform its 'lead-house' role in telecommunications interception to ensure that ASIO's capabilities, and those of other Australian agencies, remain effective.

ASIO's other technical capabilities continued to be directed at enhancing technologies for the collection of intelligence through special powers operations or surveillance, as well as the processing of increasing volumes of intelligence.

LEADERSHIP AND MANAGEMENT

ASIO continued to refine its organisational structure to provide a framework for the Organisation's growth out to 2010–11. In addition, ASIO strengthened its corporate governance arrangements including its corporate committee structure, membership and reporting framework.

Developing a strong and effective leadership cadre remained a priority in 2006–07. In addition to requiring all Senior Officers to undertake formal leadership and management training, ASIO conducted four Senior Executive Service (SES) retreats to consider strategic issues and two combined SES and Senior Officer seminars. The need for active management and leadership at all levels was a recurrent theme.

PEOPLE

ASIO bolstered its recruitment area, streamlined processes and adopted a range of innovative advertising methods to attract high calibre applicants across the range of organisational job families and functions. This approach generally has resulted in strong fields of applicants although for some job categories, it remains challenging to meet recruitment targets.

Over the reporting period, ASIO recruited 349 people, which after losses from resignation and retirement resulted in a net growth from 1 110 to 1 356. In a tight employment market this represents an outstanding achievement given that standards have not been compromised.

One unavoidable consequence of taking on so many new people is that average experience levels fall in the short term. Recognising this, ASIO continued to invest heavily in training and induction programs for new starters, a comprehensive program of training across intelligence and enabling functions, and regularly reinforced the need for managers and leaders at all levels to develop our people quickly and appropriately.

ACCOMMODATION

The increase in the number of ASIO officers has continued to put pressure on the Organisation's accommodation. Work continued to reconfigure ASIO's Central Office to accommodate staff increases in ASIO and the Office of National Assessments (ONA).

In the 2007–08 Budget, the Government provided additional funding to the Department of Finance and Administration, ASIO and ONA for the construction of a new building in the Russell precinct to house ASIO's Central Office and ONA. The total project budget is $460m.

ACCOUNTABILITY AND OVERSIGHT

National security remained an issue of public interest throughout the reporting period. ASIO continued to operate under a rigorous oversight regime and remained accountable to the Government and the Parliament.

The Director-General appeared before two Senate Committees on three occasions in relation to the Human Services (Enhanced Service Delivery) Bill 2007 and Senate Estimates hearings.

The Director-General also appeared before the Parliamentary Joint Committee on Intelligence and Security in connection with its *Review of Administration and Expenditure No. 5* and the re-listing of terrorist organisations under the *Criminal Code Act 1995* (Cth). The Deputy Director-General also appeared before the Committee on the Director-General's behalf on two occasions. ASIO sought to enhance its engagement with the Committee and provided a detailed classified submission as well as an unclassified version as part of its *Review of Administration and Expenditure No. 5*. The unclassified submission is available on both the Committee and ASIO websites and adds another dimension to ASIO's accountability and transparency mechanisms.

The program of inspections by the Inspector-General of Intelligence and Security included visits to ASIO's State and Territory offices and some of ASIO's overseas liaison posts. In 2006–07, the Inspector-General reported that ASIO had been committed to acting legally and with propriety and respect for human rights and, apart from a small number of genuine errors, had complied with all of its obligations.

In addition, the Director-General addressed business fora, government agencies, conferences, international partners, institutions and ASIO staff – 18 of these addresses are available on ASIO's website.

THE CHALLENGE AHEAD

ASIO's focus must remain firmly fixed on the prevention of harm to Australians and Australian interests, wherever threats emerge, while effectively managing the continued growth of the Organisation to meet current and future challenges.

The security of APEC, the forthcoming Federal Election, and next year's World Youth Day and Beijing Olympics, will require attention from ASIO over the next reporting period.

Achieving these goals in a volatile and demanding security environment will not be easy. In its *Corporate Plan 2007–2011,* ASIO has identified critical success factors that recognise the importance of managing growth, building and enhancing the Organisation's capability and developing strategic partnerships.

Figure 1: ASIO's work spans many sectors

ORGANISATIONAL STRUCTURE

In July 2006, ASIO moved to a new nine division structure reflecting the first phase of implementation of a five-year plan to grow ASIO to around 1 860 staff by 2010–11 (see Figure 2 on pg.9).

In March 2007, further adjustments were made to the structure to implement strengthened strategic management oversight of critical work areas.

An expanded organisational structure was created to take effect from 1 July 2007 (see Figure 3 on pp.10–11). It consists of 12 divisions, supported by 36 Managers, up from 28.

Features of the new divisional structure include:

- a Support to Operations Division to provide strengthened focus and management support for critical aspects of ASIO's Collection and Technical work;
- splitting the Executive and Legal Division into two separate divisions. This acknowledges the continued upward trend in the litigation and legal matters being managed by the Organisation, and the heavy strategic corporate coordination and reporting workload;
  - The new Legal Division will comprise two Litigation Branches and a Legal Advice Branch.
  - The new Executive Division will comprise a Government Relations Branch and an Executive Coordination Branch.
- an SES Band 2 located within the Security Division structure responsible for security projects; and
- a new Property Division with additional branches – a Building Development Branch and Building Governance and Logistics Branch – to provide enhanced focus on the new Central Office building project.

Changes within the divisions include:

- the creation of a Training Branch in Corporate Management Division. This is designed to ensure appropriate focus on the strategic priority of enhancing the capability of ASIO's people in a period of rapid expansion;
- a Leads Branch within Investigative Analysis and Advice Division to provide more effective and comprehensive evaluation, investigation and development of the large volume of leads managed by ASIO; and
- a new Counter-Terrorism Investigations Branch to provide a close focus on particular operational units engaged in counter-terrorism operations in NSW.

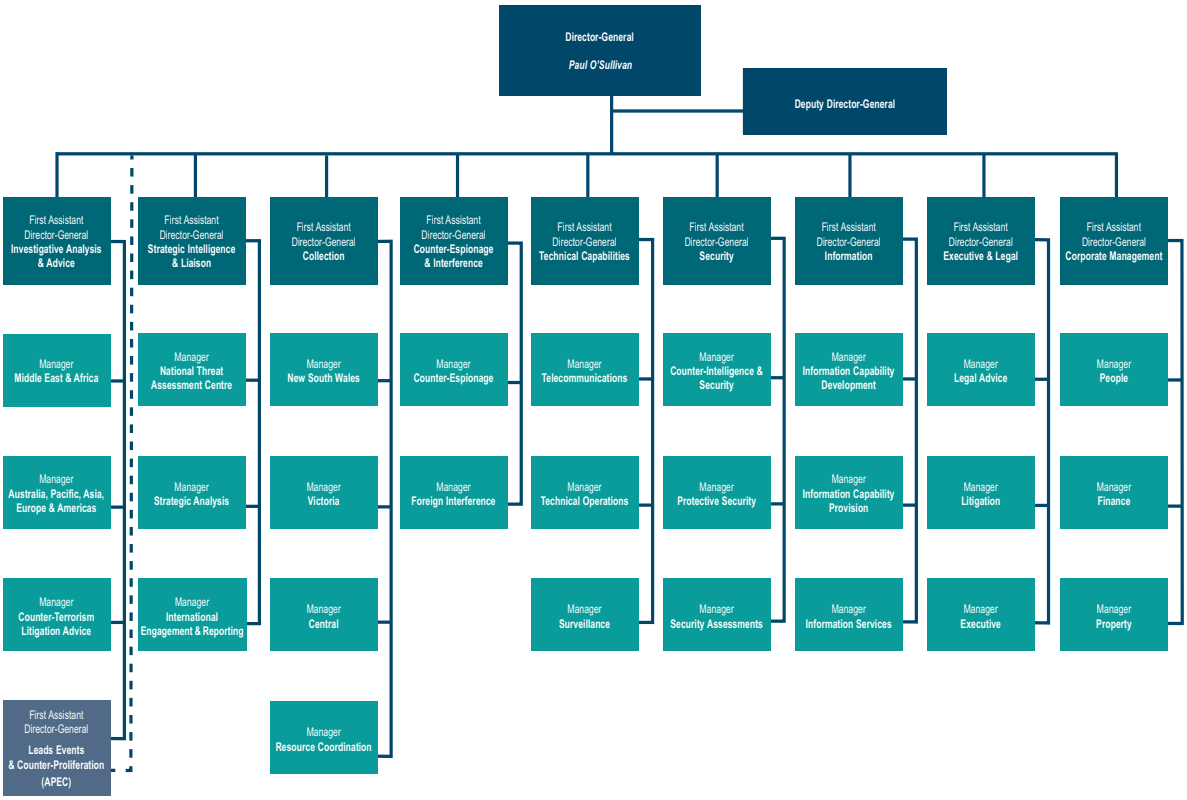


Figure 2: ASIO's organisational structure at 1 July 2006

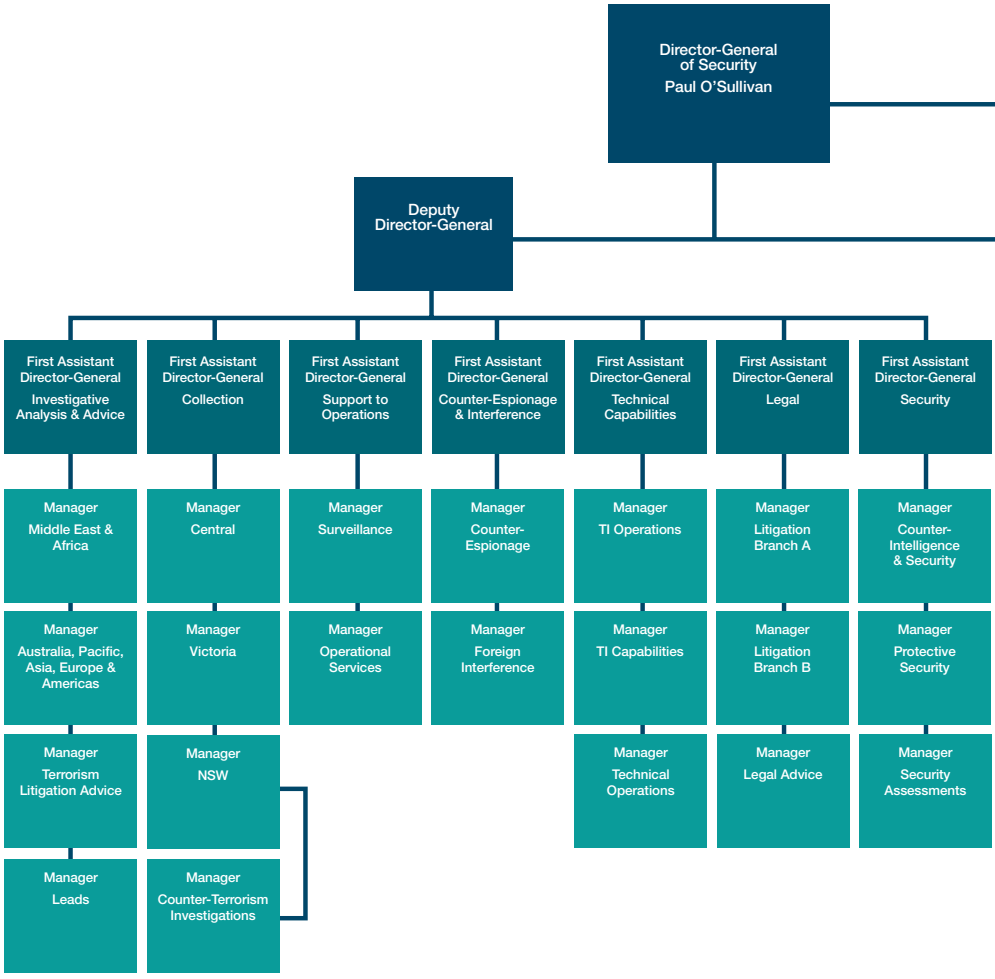
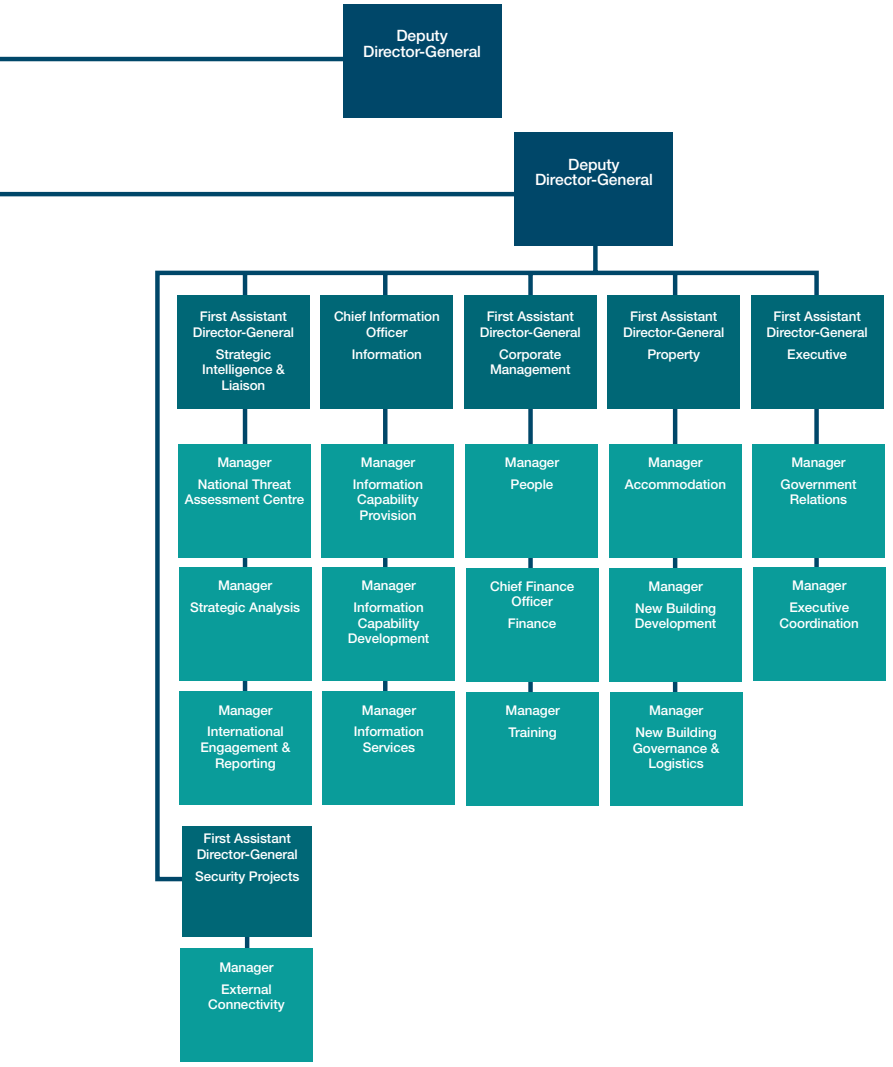


Figure 3: ASIO's organisational structure at 1 July 2007


Deputy Director-General
Deputy Director-General
First Assistant Director-General Strategic Intelligence & Liaison
Chief Information Officer Information
First Assistant Director-General Corporate Management
First Assistant Director-General Property
First Assistant Director-General Executive
Manager National Threat Assessment Centre
Manager Information Capability Provision
Manager People
Manager Accommodation
Manager Government Relations
Manager Strategic Analysis
Manager Information Capability Development
Chief Finance Officer Finance
Manager New Building Development
Manager Executive Coordination
Manager International Engagement & Reporting
Manager Information Services
Manager Training
Manager New Building Governance & Logistics
First Assistant Director-General Security Projects
Manager External Connectivity

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, government business and national infrastructure, and special events of national and international significance'.

To achieve this outcome ASIO delivers and reports to Government against identified outputs.

OUTPUT 1 – SECURITY INTELLIGENCE ANALYSIS AND ADVICE

Strategic, investigative and complex analysis

Threat assessments

Border security

Critical infrastructure protection

Policy contribution

Support to prosecutions

OUTPUT 2 – PROTECTIVE SECURITY ADVICE

Counter-terrorism checking

Personnel security

Physical security

Policy contribution

OUTPUT 3 – SECURITY INTELLIGENCE INVESTIGATION AND CAPABILITIES

Maintenance and enhancement of all-source security intelligence collection

Complex tactical and technical analysis

Technical research and development

Counter-terrorism response

National and international liaison

Policy contribution

OUTPUT 4 – FOREIGN INTELLIGENCE COLLECTION

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

Incidentally through security intelligence investigations and liaison with overseas partners

ENABLING FUNCTIONS

Maintenance of effective people development and management, financial services, information infrastructure and services, and property management.

Maintenance of effective executive services to provide corporate governance, accountability, strategic coordination, and legal and policy advice.

Excellence in security practice – internal personnel, physical, information and counter-intelligence security.

ASIO'S FUNDING AND PERFORMANCE

Funding to ASIO in 2006–07 expressed in terms of total price of Outputs was $234.764m compared to $181.099m in 2005–06.

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

Output	Actual 2005–06 $m	Estimated 2006–07 $m	Actual 2006–07 $m	Actual 2006–07 % of total
Output Group 1: Security Intelligence	181.099	233.847	234.764	100.00

Table 1: Price of ASIO's Output

ASIO's revenue from Government increased by almost 30% to $227m in 2006–07 from $175m in 2005–06. The current Forward Estimates show ASIO's budget continuing to grow to $418m by 2010–11 (see Figure 4 on pg.15), predominantly reflecting the planned increase in staff numbers and the depreciation associated with future equity injections.

The series of significant equity injections, commencing with $113m in 2006–07, will enable ASIO to:

- replace and upgrade aging equipment to support technical operations and surveillance capabilities;
- undertake essential enhancements to the underlying information technology infrastructure; and
- make consequential adjustments to accommodation to support the planned growth in ASIO's State and Territory offices.

Balanced against this growth in technical capability is the continuing development of human intelligence collection skills, the expansion of liaison relationships, and improvement in corporate training and development strategies.

ASIO is well placed to manage this growth; it has refined its project management, budgeting and reporting methodologies over the past few years as a result of smaller, specific funding increases and equity injections. The successful planning and delivery of $113m of capital projects during 2006–07, whilst achieving a small surplus of $3m, is evidence of the Organisation's ability to focus on implementing a challenging growth and capability enhancement program.

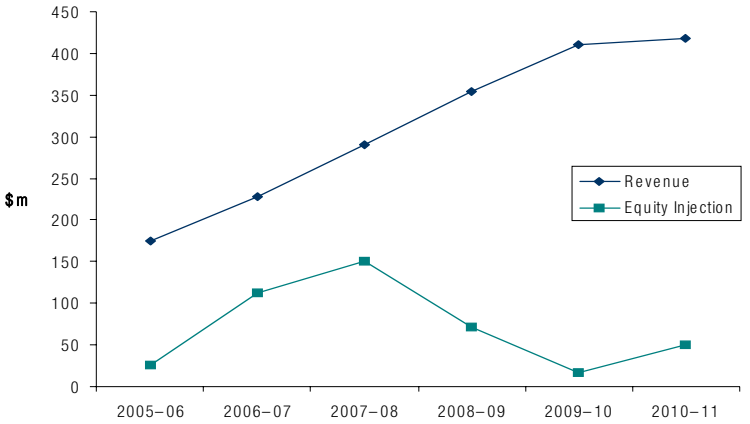


Figure 4: ASIO's revenue from Government 2005–11

CLIENT SATISFACTION

For some years ASIO has conducted annual surveys of key Commonwealth, State and Territory partners. In 2007, the range of respondents was extended to include the private sector, and the focus of the survey broadened to obtain more qualitative feedback on our clients' overall engagement with the Organisation.

Feedback on the quality of ASIO product continued to be sought, as well as the extent to which it met clients' needs. The survey also looked to identify how client relationships with ASIO could be developed, and engagement expanded.

Commonwealth clients mostly viewed their relationships with ASIO in very positive terms, a significant number noting continuing improvement in, and maturing of, their engagement over the last few years. Concerns expressed in earlier years over ASIO's responsiveness largely appear to have been addressed.

Nonetheless, ASIO is continuing to solicit feedback on every report it sends to clients to actively manage our relationships. Clients have welcomed ASIO's efforts to enhance more direct interagency engagement. ASIO will continue to build on this, and will also look to take forward a number of useful suggestions from clients over the coming year.

State and Territory law enforcement clients similarly were very satisfied with their relationships and engagement with the Organisation although, along with the Australian Federal Police, a number thought more could be done at the middle management level. ASIO product continues to contribute significantly to police understanding of the security environment, particularly as it relates to counter-terrorism.

Private sector respondents acknowledged both they and ASIO were still learning how to deal with each other. They were impressed with ASIO's responsiveness to their requests, but saw a need for greater and more comprehensive engagement to ensure there was a more complete understanding of each others' business.

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 through:

- strategic and investigative analysis
- threat assessments
- border security
- critical infrastructure protection
- policy contribution
- support to prosecutions.

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.

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

STRATEGIC AND INVESTIGATIVE ANALYSIS

THREATS TO AUSTRALIAN INTERESTS

Overwhelmingly, ASIO's priority is to counter the persistent terrorist threat from extremists.

The main terrorist threat to Australia and its interests for the foreseeable future comes from extremists inspired or directed by al-Qa'ida and like-minded groups. These extremists have the intent and capability to attack Australian interests globally.

In addition to attacks on Australian Defence Force and Australian security personnel in Iraq and Afghanistan, significant terrorist attacks or incidents involving Australians occurred in 2006–07:

- on 22 May 2007 an Australian photographer was injured in a bomb explosion in Yala province, Thailand; and
- on 10 September 2006 the Governor of Paktia Province in Afghanistan, a dual Afghan-Australian national, was killed in a suicide bombing, along with two others.

Public statements by al-Qa'ida leaders and others have singled out Australia and encouraged attacks against Australian interests since 2001. These statements continue to promote violent ideology and praise the terrorist acts conducted by others. In 2006–07, statements by the al-Qa'ida leadership did not specifically mention Australia but continued to threaten attacks on allies of the United States.

Statements by other extremist elements, including those associated with al-Qa'ida, continue to specifically name Australia.

- In March 2007, the 'Islamic State of Iraq' – a collection of extremist groups dominated by al-Qa'ida in Iraq – issued an opportunistic claim of responsibility for launching an attack in Iraq on an aircraft carrying the Prime Minister, the Hon John Howard MP, and forcing it to land. The aircraft, in fact, made an emergency landing when minutes after take off smoke and fumes were noticed in the cabin.
- Iraqi Shi'a cleric Muqtada al-Sadr described the United States, Israel, the United Kingdom and Australia as 'colonialist and exploitative states' during an interview on Hizballah's Al-Manar television.

Statements by al-Qa'ida and affiliated groups continue to resonate with extremists and provide them with ongoing motivation.

Outside the counter-terrorism arena, the focus of our investigations includes threats to Australian interests from those who:

- engage in espionage;
- are involved in acts of foreign interference;
- seek to acquire material or expertise for use in weapons of mass destruction;
- seek to use, or incite, violence during legitimate protest (the very small minority who advocate and conduct violent protest fall within the politically motivated violence provisions of the ASIO Act); or
- seek to use, or incite, violence against parts of Australia's community because of their national extremist or racist extremist agenda.

Public statements by al-Qa'ida leaders and others have singled out Australia and encouraged attacks against Australian interests since 2001.

THE TERRORIST THREAT

The main global terrorist threat over the past decade has been driven by an extreme Islamic 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.

The global jihadi movement has embraced the Internet as a propaganda and recruitment tool; its reach has extended to an audience far beyond traditional constituencies.

Islamic extremists believe 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 enmity to the West is deep-seated and their cause absolutist, one with which there can be no negotiation.

Al-Qa'ida has been the vanguard of the global jihadist movement. 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.

Since the attacks of 11 September 2001, the core of al-Qa'ida has suffered significant setbacks due to disruption activities undertaken by governments around the world. Despite these setbacks, it appears to have been slowly rebuilding its organisational structures and operational capabilities from bases in the tribal regions on the borders of Pakistan and Afghanistan.

Al-Qa'ida continues to encourage groups involved in localised insurgencies based on nationalist or ethnic issues, to view their struggles in al-Qa'ida's own strategic terms. During the past year, al-Qa'ida has maintained its influence over jihadist militants in Iraq. It has entered into a formal alliance with the Algerian terrorist organisation – the Salafist Group for Call and Combat – to form 'al-Qa'ida in the Islamic Maghreb'. The willingness of jihadist groups to identify themselves as part of al-Qa'ida is likely to extend, which will strengthen the reach of al-Qa'ida.

The trans-Atlantic airliner bomb plot disrupted in August 2006 by United Kingdom authorities, shows that the resolve of global jihadists to sponsor or carry out mass casualty attacks against civilians is undiminished. It illustrates the resilience of al-Qa'ida's organisational model and highlights its potentially lethal reach. In particular it reinforces our concerns over the ability of terrorists to adapt their methods in order to overcome enhanced security measures, and points to the attraction of the jihadist mission to extremists.

There have been further efforts by al-Qa'ida to win support through the use of traditional and new media. The global jihadi movement has embraced the Internet as a propaganda and recruitment tool; its reach has extended to an audience far beyond traditional constituencies. Its media strategy seeks to magnify and exploit grievances and disaffections held by some, and to manipulate them for its own ideological and militant purposes. In 2006–07, al-Qa'ida's media arm released at least 48 video statements, believed to be the most ever released in one year.

Australia is not immune from the efforts of the radicalisation processes of individuals and their embrace of an extremist mindset. The grievances, ideology and strategic vision of al-Qa'ida's leaders – and similarly those held by other leading jihadists not closely linked to al-Qa'ida – have a resonance with a small proportion of extremists, including in Australia. For some, engagement in jihad is at a more emotional and physical level while others have signed up to an extremist ideology at an intellectual level. The beliefs in this latter group include a number of strands, the most important of which are:

- the assertion that militant jihad against the United States and its allies is the individual duty of every Muslim in any country in which it is possible to do so;
- the 'historical narrative' that places the contemporary 'anti-Muslim' nature of Western governments in a

continuous tradition stretching back to the Crusades;

- an extreme Salafist or Takfiri interpretation of Islam that claims to be based on the beliefs and practices of the Prophet Muhammad and his earliest followers, and condemns as apostates those Muslims who do not ascribe to the same interpretation; and
- a political doctrine that holds that the Western values of secularism, democracy and the constitutional separation of religion and state are incompatible with Islam (the desired alternative is an idealised theocratic state, a Caliphate, underpinned by Islamic law).

The adoption of this doctrine is one of the drivers for the development of 'home-grown' terrorist networks and groups. Others who are involved in extremist activity, however, do not have a firm grasp of the ideology or strategic vision. They are drawn to extremism by personal motivations and grievances, including anger over perceived attacks on Islam.

Regardless of what is driving them, individuals in Australia who are drawn to extremism pose a 'home-grown' threat, which has also been seen in the United Kingdom, Canada, Europe and the United States. This threat poses particular challenges for security agencies. The speed and intensity with which some individuals become radicalised makes detection by security agencies more difficult, and this will continue to represent a significant challenge for governments and the broader community in the coming years.

Aside from the threat posed by the global jihadist movement, there are a number of other groups around the world that engage in terrorism to achieve their goals, including nationalist and separatist groups and those supported by nation states.

COUNTER-TERRORISM

As part of our wider restructure on 1 July 2006, ASIO established the Investigative Analysis and Advice Division to provide a sharper focus for ASIO's counter-terrorism investigations. While the majority of our investigative resources are devoted to substantive counter-terrorism leads (the 'knowns'), we also devote resources towards identifying the 'unknowns'. This is becoming an increasingly important facet of our work given the unstructured nature of extremist groups and the growing ability of extremists to conduct their activities in ways that are intended to be hidden from view.

While the majority of our investigative resources are devoted to substantive counter-terrorism leads (the 'knowns'), we also devote resources towards identifying the 'unknowns'.

This year we refined the processes by which decisions regarding investigative priorities occur and how these priorities are translated into specific information collection requirements. We also refined the way outcomes from collection activity are reviewed and the processes by which investigations are suspended or closed. These refinements have increased our flexibility in deploying resources against priority investigations.

While these refinements have resulted in more efficient processes, and despite the growth of the Organisation, strict prioritisation of effort is necessary. Hence not all leads of potential security concern can be pursued to the same extent.

Our current investigative strategy in respect of Islamic extremists leads ASIO to focus on those organisations and individuals we assess as most likely to threaten Australia or Australia's interests. These entities can be broadly defined as:

- 'Home-grown' Islamic extremists who gain their inspiration from al-Qa'ida and like-minded terrorist organisations but are not directed by them;
- Australia-based Islamic extremists working with, or having significant links to, extremists overseas; and
- Foreign-based Islamic extremists who we assess might threaten Australia or Australian interests – either locally or

abroad – without the direct involvement of Australians or Australia-based individuals.

It is important to note that there are no clear cut divides among those who make up these broad categories. Connections between extremists ebb and flow, often driven by their current activities and plans and on the changing nature of personal relationships and allegiances between individuals.

…there was a developing trend towards Iraq-based insurgents' use of toxic industrial chemicals in conjunction with improvised explosive devices…

Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) terrorism

There remain indications of terrorist interest in chemical, biological and radiological (CBR) agents, including attempts by al-Qa'ida and others to acquire CBR-related materials, technical expertise or relevant information.

Over 2006–07, there was a developing trend towards Iraq-based insurgents' use of toxic industrial chemicals in conjunction with improvised explosive devices, using home-made and commercial grade explosives. The majority of casualties from these attacks, however, resulted from the explosive rather than toxic effects. The use of improvised explosive devices remained the most common terrorist weapon.

ASIO continued to provide advice to Government to support policy development and national preparedness on the CBRNE threat, including through key input into the Council of Australian Governments' Review of Hazardous Chemicals. As a member of the National CBR Working Group, coordinated by Emergency Management Australia, ASIO also provided threat briefs to first responders.

Closer collaboration by ASIO with Australian Government CBRNE partners continued to develop, including with the Australian Federal Police (AFP) Australian Bomb Data Centre and its Chemical, Biological, Radiological and Nuclear Data Centre. These government agencies, members of the Australian Intelligence Community (AIC) and the Defence Science and Technology Organisation met regularly through the Special Weaponry Analysis Group to discuss intelligence relating to global CBRNE activity by terrorists, and to identify emerging and developing threats and trends.

On the international level, ASIO worked closely with liaison partners in assessing the CBR threat.

Proscription

The process for proscription of a terrorist group in Australia under subsection 102.1(2) of the *Criminal Code Act 1995* (Cth) 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 a 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).

ASIO has provided security advice regarding the listing of terrorist organisations to the Attorney-General since the introduction of the listing provisions in 2002. ASIO uses a range of criteria to evaluate organisations for possible proscription and provides advice in the form of a 'statement of reasons'. The statement of reasons for each organisation addresses the legislative requirements for proscription set out in subsection 102.1(2) of the *Criminal Code Act 1995* (Cth). The statement of reasons is unclassified and is based on publicly releasable details about the organisation; these are corroborated by classified reporting.

At the end of the reporting period, there were 19 organisations that had been proscribed under the Criminal Code as terrorist organisations. In 2006–07, the

Government re-listed 15 groups as terrorist organisations. In each case, ASIO provided a statement of reasons for the Attorney-General's consideration.

VIOLENT PROTEST

In Australia, the great majority of protest activity is peaceful and lawful. Such lawful protest activity is not the focus of ASIO's investigations. Section 17A of the ASIO Act states:

> 'This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.'.

However, a small number of individuals see the promotion and use of violent tactics at protest activity as a justifiable means to achieve their aims.

In 2006–07, there were violent incidents in connection with the G20 Finance Ministers' Meeting in Melbourne in November. ASIO has worked closely with government agencies, in particular the New South Wales Police Force and the AFP, in planning for the security of the APEC forum Leaders' Week. Other APEC meetings during 2007 passed without incidents of violent protest.

COUNTER-PROLIFERATION

The importance of counter-proliferation efforts was highlighted in 2006–07 by key developments in two major countries of proliferation concern. The Democratic People's Republic of Korea conducted a nuclear test in defiance of United Nations Security Council Resolutions and the Non-Proliferation Treaty, and Iran refused to suspend its uranium enrichment activities as part of its 'peaceful' nuclear program. Their activities resulted in both countries being placed under United Nations sanctions.

ASIO continued to contribute to the acquisition of intelligence on the efforts of nation states attempting to acquire chemical, biological, radiological and nuclear weapons and delivery systems.

State-sponsored programs

A major focus for ASIO during 2006–07 continued to be the investigation of efforts of countries to exploit Australian industrial, technological, and educational and research facilities in order to develop Weapons of Mass Destruction programs and capabilities.

Additional resourcing in 2006–07 enabled ASIO to increase both its analytical and its investigative effort. However, rigorous prioritisation of leads and investigations was essential in a proliferation environment that remained both demanding and complex.

ASIO continued to contribute to the acquisition of intelligence on the efforts of nation states attempting to acquire chemical, biological, radiological and nuclear weapons and delivery systems.

COUNTER-ESPIONAGE

ASIO's work in countering espionage is carried out in a separate division from other security intelligence investigations, in recognition of the particular requirements of these investigations.

Espionage is not defined in the ASIO Act but criminal offences relating to espionage are set out in Division 91 of the *Criminal Code Act 1995* (Cth) and the *Crimes Act 1914* (Cth).

In broad terms, ASIO's counter-espionage investigations are carried out using the same range of capabilities, techniques and approaches used in ASIO's other security intelligence investigations (with the exception of questioning and detention powers, which are applicable only to the investigation of terrorism offences).

Counter-espionage investigations are inherently sensitive:

- they go to activities in Australia of a range of foreign governments and foreign powers and to activities that they direct against Australian interests outside Australia.

FOREIGN INTERFERENCE

There is a significant history of foreign governments gathering information on communities and individuals in Australia they perceive to be hostile.

Those collecting this information in Australia include foreign intelligence officers, diplomats undertaking intelligence tasking and individuals in the community co-opted by foreign intelligence services. It is not uncommon for threats to be made against individuals' relatives and associates in their home country should they not cooperate with a foreign police or intelligence service; some individuals have also been detained, threatened or coerced when they have travelled to their country of origin.

…ASIO has developed significant structural, policy, process and personnel strengths in meeting its security commitments for special events.

PROMOTION OF COMMUNAL VIOLENCE

As noted in ASIO's *2005–06 Report to Parliament*, the ongoing cycle of violence in Iraq has had an effect on the Iraqi Shi'a community in Australia. In late 2005 and early 2006, some violence, including some serious assaults, occurred in Sydney at the time of the Iraqi elections. While there was some possibility this would escalate into more serious violence, tensions reduced during 2006–07 with no substantial communal violence being recorded.

LEADS DEVELOPMENT

ASIO is responsible for the triage, evaluation and investigation of counter-terrorism-related lead information.

We strengthened our relationship with the Australian Customs Service (ACS), which has started to provide all counter-terrorism reports to ASIO electronically.

Other initiatives in 2006–07 included the further development of data analysis and critical thinking methodologies applicable to the investigation of lead intelligence.

During the past year, ASIO held information exchanges with liaison partners on technical capability-building methodologies and training programs focused on lead analysis.

National Security Hotline

Since it was established in December 2002, the Protective Security Coordination Centre's (PSCC) National Security Hotline (NSH) has referred approximately 48 500 calls to ASIO. Of these referrals, approximately 14 490 have been assessed as requiring further investigation.

In 2006–07, ASIO provided input to the Attorney-General's Department in the development of the next advertising campaign for the NSH.

While not all NSH calls provided useful information, those that do can be significant.

SPECIAL EVENTS

With the benefit of the 2000 Sydney Olympic Games, the 2002 Commonwealth Heads of Government Meeting (CHOGM), and the 2006 Melbourne Commonwealth Games experience, ASIO has developed significant structural, policy, process and personnel strengths in meeting its security commitments for special events.

The security of major events – including the G20 Finance Ministers' Meeting in Melbourne and the 2007 APEC forum – was a focus for ASIO in 2006–07, including the production of Threat Assessment advice.

APEC

APEC, culminating in the APEC Leaders' Meeting to be held in Sydney between 2–9 September 2007, is the most significant series of international meetings ever hosted by Australia. ASIO worked closely with government agencies, in particular the New South Wales Police Force, the AFP and the APEC 2007

Taskforce, in planning for the security of APEC events.

While primarily responsible for the provision of security intelligence advice, ASIO also provided technical equipment, protective security advice and risk management training to relevant jurisdictional authorities, and conducted security checking for accreditation and border security purposes for APEC events held during 2006–07. This work will continue until APEC concludes in September 2007.

In addition, ASIO actively engaged international partners to manage any potential threats to the APEC events originating offshore.

ASIO conducted security checking for accreditation purposes on individuals who required access to security controlled areas associated with all APEC meetings in 2007. It is anticipated that ASIO will have checked in excess of 10 000 individuals for the Leaders' Meeting alone. Together with police checks, the accreditation process provided a level of confidence that those with approved access to security-controlled areas did not pose a security threat.

ASIO's national program of engagement with leading members of ethnic communities included communities from APEC member economies.

G20 Finance Ministers' Meeting

ASIO was responsible for the collection, analysis and dissemination of security intelligence advice for the G20 Finance Ministers' Meeting in November 2006, which attracted violent protest activity.

World Youth Day 2008

ASIO will provide security intelligence advice for the security of World Youth Day 2008 – to be held in Sydney in July 2008 – including a number of smaller events held around Australia. His Holiness Pope Benedict XVI will be in Sydney over a period of five days to host a number of events. ASIO is working closely with Federal, State and Territory agencies and the New South Wales Government World Youth Day 2008 Coordination Authority to ensure security for the event.

Beijing Olympics 2008

ASIO is a member of the Security and Intelligence Specialists for the 2008 Beijing Olympics Games, established by the Chinese Government. This group is the official body through which security and intelligence liaison will occur. Security specialists from a variety of nations participate to share expertise with the Chinese authorities.

Other Special Events

Commemorations for the 92nd ANZAC Day, including at Gallipoli, proceeded without security incident, as did the 2007 Cricket World Cup.

A number of Threat Assessments were produced and ASIO participated in the planning of events with other government agencies.

THREAT ASSESSMENTS

Australian government agencies work together in the National Threat Assessment Centre (NTAC) to monitor, collate and analyse threat intelligence available to the Australian Government.

The NTAC provides the Government with a 24x7 threat analysis capability. NTAC product is available immediately to members of the AIC. Agencies represented in the NTAC include the AFP, Australian Secret Intelligence Service (ASIS), Defence Intelligence Organisation (DIO), Defence Signals Directorate (DSD), Department of Foreign Affairs and Trade (DFAT), the Department of Transport and Regional Services and the Office of National assessment (ONA).

ASIO will provide security intelligence advice for the security of World Youth Day 2008 – to be held in Sydney in July 2008 – including a number of smaller events held around Australia.

Officers in the NTAC have on-line access to communications systems and databases of their parent agencies. This allows for connectivity and coordination between agencies, and provides assurance that all relevant information available to government agencies is reflected in Threat Assessment advice.

ASIO'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;
- 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 Ashes Cricket Series, APEC 2007 and the Federal Election; and
- significant events overseas such as the Bali Commemoration Services, 2007 Cricket World Cup, East Asia Summit, CHOGM 2007 and the annual ANZAC Day commemoration at Gallipoli.

Threat Assessments remain the NTAC's vehicle for setting or changing threat levels.

PERFORMANCE

Threat Assessments remain the NTAC's vehicle for setting or changing threat levels. Table 2 shows the number of Threat Assessments issued by category and year. Feedback from clients confirms that the NTAC provides authoritative and coordinated advice on threat intelligence.

The NTAC's product is seen as valuable and is highly respected within the Australian Government.

Category of assessment	2003–04	2004–05	2005–06	2006–07
Australian interests (in Australia and overseas)	559	427	503	502
Australian dignitaries	624	676	755	403
Diplomatic premises in Australia	36	24	22	29
Visiting dignitaries	480	228	162	423
Special events	–	37	58	81
Protective security	35	49	48	46
Vital Infrastructure	–	29	20	33
Demonstration notifications	38	56	32	20
Liaison threat advice	–	347	492	183
Threat Analysis Papers	–	–	6	80
Country Reports	–	–	–	22
Fortnightly Threat Review	–	–	–	24
Other Threat Assessments	245	130	118	148
Total	2 017	2 003	2 216	1 994

Table 2: Threat Assessments issued by category and year

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 grew in 2006–07. ASIO is a key source of advice for the Department of Immigration and Citizenship (DIAC) on border security matters, including providing security assessments on selected visa applicants and unauthorised arrivals.

INITIATIVES

ASIO and DIAC worked closely at the operational, policy and management levels to identify initiatives that improve the processes for managing increasing caseloads and service standards, and to develop policies and procedures to meet new requirements (e.g. citizenship checking).

During 2006–07, ASIO and DIAC completed an evaluation of immigration-related security checking arrangements. The review proposed a number of recommendations across policy, process, resourcing and DIAC areas designed to provide a more effective and efficient security-checking regime.

MOVEMENT ALERT LIST (MAL)

ASIO makes extensive use of MAL, which is maintained by DIAC and draws attention to visa applicants or travellers who may be of security interest; all applicants for Australian visas are checked against MAL.

VISA SECURITY CHECKING ASSESSMENTS

In addition to checks against MAL conducted on visa applicants, DIAC refers individuals to ASIO for security checking under Public Interest Criterion 4002 of the *Migration Regulations*.

ASIO makes an assessment of whether the entry or continued stay of non-citizens would pose a direct or indirect threat to security. Visa security checking processes generally are managed in order of referral from DIAC, taking into account any agreed priority caseloads.

The current security environment, and the increasing volume of intelligence (which is often incomplete), complicates the assessment process and can make it more 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 DIAC.

Both 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 process also may include an ASIO interview of the applicant to

ASIO is a key source of advice for the Department of Immigration and Citizenship (DIAC) on border security matters, including providing security assessments on selected visa applicants and unauthorised arrivals.

Type of entry	2003–04	2004–05	2005–06	2006–07	% increase
Temporary	30 841	39 015	39 973	44 197	10.6%
Permanent	13 881	13 402	13 174	9190	-30.2%
Total	44 722	52 417	53 147	53 387	0.5%

Table 3: Visa security assessments 2003–04 to 2006–07

Note: From 2004–05 onwards figures include unauthorised arrivals.

provide the applicant with an opportunity to resolve issues of concern.

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

In 2006–07, ASIO completed 53 387 visa security assessments (see Table 3 on pg.29). There was a significant reduction in the number of permanent visa assessments due to the increase in temporary visa applications referred to ASIO, and the priority given to their resolution over permanent visa assessments.

…the Next Generation Border Control System announced by the Prime Minister on 8 July 2007, will provide a smarter, more flexible system that will enable ASIO to respond quickly to changes in the security environment.

Security Checking Profile

In 2006–07, ASIO and DIAC jointly delivered training programs for onshore and offshore visa processing officers and overseas airport liaison officers, aimed at enhancing their effectiveness.

This year saw a moderate increase in the number of assessments conducted by ASIO on individuals seeking temporary visas to enter Australia. This continues a trend evident since 2003–04.

The introduction of the Next Generation Border Control System announced by the Prime Minister on 8 July 2007, will provide a smarter, more flexible system that will enable ASIO to respond quickly to changes in the security environment.

Protection visas

In 2006–07, ASIO completed 1 153 assessments on protection visa applicants.

Amendments to section 65A of the *Migration Act 1958* require the Minister for Immigration and Citizenship to make a decision on protection visa applicants within 90 days of their application. ASIO continued to devote specialised resources to assist in meeting these timeframes. Fifty-two percent of protection visa applications referred to ASIO for assessment were completed within the 90 day timeframe. However, the complexity and volume of protection visa applications resulted in a mean processing time of 11.5 weeks.

Adverse and qualified security assessments

In 2006–07, ASIO issued adverse security assessments in respect of seven[1] individuals seeking entry to Australia. These applicants were assessed by ASIO to pose a direct or indirect risk to security based on links to politically motivated violence, terrorist organisations, or foreign intelligence services.

In January 2007, ASIO issued DIAC with a non-prejudicial security assessment in respect of Mr Mohammad Faisal al Delimi who previously had received an adverse security assessment. The non-prejudicial assessment was based on new information and changed circumstances.

In 2006–07, Mr Mohammad Sagar, who was the subject of an adverse security assessment issued in June 2005 was transferred from immigration detention on Nauru and resettled in a third country by the United Nations High Commission for Refugees.

Civil proceedings

Three individuals, Mr Scott Parkin, Mr Mohammad Faisal al Delimi, and Mr Mohammad Sagar, were engaged in proceedings in the Federal Court for judicial review of adverse visa security assessments issued in respect of them at the end of the reporting period.

During the reporting period, ASIO successfully defended an application for judicial review of an adverse security assessment issued in 2004 in relation to Mr Mansour Leghaei. The Full Federal Court unanimously upheld the validity of the assessment and dismissed

[1] Includes one person who was the subject of a security assessment in 2005–06.

Mr Leghaei's appeal with costs. Mr Leghaei has sought to challenge this Full Court decision before the High Court of Australia.

CITIZENSHIP SECURITY CHECKING

Following the introduction of the *Australian Citizenship Act 2007*, ASIO continued to work with DIAC to develop an appropriate process for the security checking of applicants for Australian citizenship based on a phased implementation from 1 July 2007.

CRITICAL INFRASTRUCTURE PROTECTION

Within the Australian Government's framework for protection of Australia's critical infrastructure from terrorism and other threats, ASIO:

- is responsible for maintenance of a national database of critical infrastructure assets on behalf of the National Counter-Terrorism Committee (NCTC);
- provides assessments on the threat from terrorism to Australia's 11 critical infrastructure sectors (see Appendix B); and
- provides briefings on threats to critical infrastructure to government and private sector stakeholders.

NATIONAL CRITICAL INFRASTRUCTURE DATABASE

ASIO is mandated by Government to maintain a database of Australia's critical infrastructure. This is done in collaboration with State and Territory agencies. There are 2 050 asset entries in the database, each of which is ranked for criticality (vital, major, significant or low – see Appendix B). The database is updated frequently, and in May 2007 ASIO began a comprehensive review of the database and its content.

ASSESSING THE THREAT TO CRITICAL INFRASTRUCTURE

Threat Assessments of nationally vital assets and economic sectors are key elements in Australia's coordinated protective security arrangements. They underpin critical infrastructure protection activities undertaken by the Federal, State and Territory Governments, and assist in the formulation of risk context analyses by Australian government regulatory agencies, State and Territory jurisdictions and the private sector. This in turn helps shape business continuity planning. Critical infrastructure data is provided to ASIO by all jurisdictions and Australian government departments and agencies to assist in the formulation of Threat Assessments.

ASIO's critical infrastructure Threat Assessment research, and the dissemination of threat-related information, involves close consultation with owners and operators of critical infrastructure, regulatory agencies and States and Territories.

ASIO released nine sectoral Threat Assessments during 2006–07. An annual review of threats to vital assets is carried out in accordance with NCTC recommendations to the Council of Australian Governments.

INFORMATION SHARING AND ENGAGEMENT WITH INDUSTRY STAKEHOLDERS

In accordance with NCTC arrangements, briefings are provided for owners and operators of critical infrastructure on the completion of sectoral and vital asset Threat Assessments. Briefings are undertaken in conjunction with relevant government departments and State and Territory agencies, representative of the whole-of-government approach to counter-terrorism.

ASIO is a member of the Critical Infrastructure Advisory Council, a collaborative body comprising

ASIO's critical infrastructure Threat Assessment research, and the dissemination of threat-related information, involves close consultation with owners and operators of critical infrastructure, regulatory agencies and States and Territories.

representatives of the Federal, State and Territory Governments, and the critical infrastructure sectors. ASIO worked with Government and industry to support established key initiatives including the Trusted Information Sharing Network, which is coordinated by the Attorney-General's Department.

Figure 5: ASIO's Business Liaison Unit website

Business Liaison Unit

The ASIO Business Liaison Unit (BLU) provides a direct interface between the private sector and the AIC.

The BLU launched a website at the Business-Government Advisory Group meeting on 24 July 2006 (see Figure 5). The website is password-secured (obtained through subscription) and is the principal means by which the BLU disseminates information to the private sector.

As at 30 June 2007, there were 247 subscribers to ASIO's BLU website.

The BLU produces unclassified *Business Security Reports* – national security-related information comprising industry surveys, security awareness briefings and major event and incident reporting. The reports are designed to raise awareness and assist business risk management planning. As at June 2007, the BLU had posted more than 55 reports for the benefit of business security personnel through the BLU website.

The BLU also liaises directly with the private sector through presentations at industry conferences and briefings to major Australian companies. Part of this work includes arranging executive meetings between the Director-General and CEOs, board members and other executive management.

Major conference presentations to business leaders have included fora arranged by the Business Council of Australia, the American Chamber of Commerce, Australian Business Limited, the Australian Institute of Company Directors and the Sydney Institute.

Other activity commenced during 2006–07 includes a joint project with the NTAC, which involves the development of a database of Australian commercial interests overseas. The information – to be finalised during the second half of 2007 – will increase ASIO's capability to respond to threats abroad and will inform BLU reporting and liaison activity targeted at the many Australian companies who have personnel and assets based internationally.

MONITORING EMERGING THREATS TO NATIONAL INFORMATION INFRASTRUCTURE

The National Information Infrastructure (NII) comprises electronic systems that underpin critical services such as telecommunications, banking and finance, transport and distribution, energy and utilities.

ASIO, DSD, and the AFP have formal arrangements for identifying, assessing and responding to threats to the NII.

SUPPORT TO PROSECUTIONS

ASIO's involvement in security-related litigation continued to grow. During the reporting period, ASIO was involved in litigation matters comprising security-related criminal proceedings (including terrorism prosecutions), judicial and administrative reviews of security assessments and other civil proceedings.

Paramount to ASIO's involvement in these proceedings was the protection of capabilities, modus operandi and sources of information.

During 2006–07, ASIO was involved in counter-terrorism prosecutions. In response to requests for evidence, ASIO provided information to the Commonwealth Director of Public Prosecutions and the AFP for evidentiary use in terrorism prosecutions. This included the prosecution of 22 individuals

in Sydney and Melbourne (the Sydney and Melbourne Pendennis proceedings). In all terrorism prosecutions, ASIO has worked closely with Commonwealth prosecuting agencies and State law enforcement agencies.

Additionally, ASIO was involved in civil and criminal proceedings and applications for merits review before the AAT. During 2006–07, ASIO officers supported these legal proceedings by providing statements, and in many cases, giving evidence.

Timely and regular briefings have been provided to the Attorney-General on significant litigation matters.

R v Lodhi

During the reporting period, Faheem Lodhi was convicted by a jury of three terrorism offences and sentenced to 20 years imprisonment. Mr Lodhi has sought to challenge the conviction and sentence before the Court of Criminal Appeal.

R v Seivers and O'Ryan

The leak of classified ASIO documents relating to the 'Senate Foreign Affairs, Defence and Trade References Committee Inquiry into the Assessment of Threats to the Security of Australians in South East Asia' culminated in the committal for trial of two individuals for unauthorised disclosure of Commonwealth information. One of the two individuals, Mr Seivers, is a former ASIO officer.

CAPABILITY BUILDING

ASIO continues to build capability to manage the increasing demand placed upon legal resources, both in terms of the in-house counsel role and litigation.

During the reporting period, ASIO was able to contribute to the prosecution of individuals without prejudicing ongoing investigations.

RELEASE OF ASIO'S RECORDS

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

Access to archival records

Members of the public can apply to the National Archives of Australia (NAA) for access to ASIO records that are at least 30 years old (described as the 'open access period'). When the NAA does not hold records on a subject, it passes the application to ASIO. ASIO locates and assesses any relevant records and provides advice to the NAA about whether the records contain information that should be exempt from public release under section 33 of the Archives Act.

ASIO only claims an exemption where disclosure of the information could reasonably damage security. ASIO balances the commitment to release information into the public domain with the need to protect security.

In rare cases, the NAA will inform ASIO of the identity of the applicant to facilitate ASIO's contact with them in an attempt to identify relevant records or agree on priorities.

Trends

We received 582 applications for access to separate items or subjects in 2006–07. This compared with 338 in 2005–06.

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. There were 143 family requests completed in 2006–07 compared to 132 in 2005–06. Ninety eight percent of these were completed within the benchmark period of 90 days compared with 100% for 2005–06.

During the reporting period, ASIO was able to contribute to the prosecution of individuals without prejudicing ongoing investigations.

The total number of folios (pages) examined during 2006–07 was 52 234 compared to 45 454 in 2005–06.[2]

The percentage of folios exempted from release, or with part of the text exempted, varies (see Table 4). For example, policy files typically have a much greater percentage of documents released without exemption than files relating to ASIO's sensitive operations.

The total number of folios (pages) examined during 2006–07 was 52 234 compared to 45 454 in 2005–06.

Appeals

Applicants dissatisfied with exemptions claimed by ASIO can request an internal reconsideration of the decision; this process is undertaken in conjunction with the NAA.

	2002–03	2003–04	2004–05	2005–06	2006–07
Folios released without exemption	33%	35%	48%	45%	53.6%
Folios released with part of text claimed as exempt	56%	58%	46%	53%	43.8%
Folios claimed as totally exempt	11%	7%	6%	2%	2.6%
Total	100%	100%	100%	100%	100%

Table 4: Release of records - Distribution of exemption claims across assessed folios

[2] In the 2005–06 *Annual Report* the number of folios examined was incorrectly reported as 43 222.

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 through:

- counter-terrorism checking
- personnel security
- physical security
- policy contribution.

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

COUNTER-TERRORISM CHECKING AND PERSONNEL SECURITY

ASIO security assessments, including for counter-terrorism purposes or access to national security classified information or areas, are governed by the ASIO Act. These assessments determine whether anything in the candidate's background or activities gives cause for security concern.

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 potential security concern, ASIO may conduct interviews or make other inquiries.

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 recommends against the proposed access.
- A qualified assessment provides information that ASIO considers may be relevant to the agency's decision to help minimise the identified potential risk.

COUNTER-TERRORISM CHECKING

Counter-terrorism security checking comprises checks in relation to:

- aviation security – including Aviation Security Identity Cards (ASICs);
- maritime security – Maritime Security Identity Cards (MSICs);
- ammonium nitrate licensing;
- staff and visitors to the Australian Nuclear Science and Technology Organisation's (ANSTO) Lucas Heights facility; and
- special events such as the Asia-Pacific Economic Cooperation (APEC) forum.

A total of 134 981 counter-terrorism checks were completed this year.

A total of 134 981 counter-terrorism checks were completed this year (see Table 5).

Counter-terrorism checks are limited to inquiring whether an individual has any known links to terrorism. They are completed more quickly than assessments for access to classified information, which are more detailed and processed manually.

ASIO completed 97% of counter-terrorism checks in five days and 99% in ten days.

Type of check	2003–04	2004–05	2005–06	2006–07
Aviation	58 147	38 466	62 285	36 338
Maritime Security Identity Cards	–	–	9 448	81 780
Ammonium Nitrate	–	1 634	7 428	6 419
ANSTO	–	–	–	1 027
Commonwealth Games	–	–	56 149	–
G20 Finance Ministers' Meeting	–	–	–	1 580
APEC	–	–	–	7 837
Total	58 147	40 100	135 310	134 981

Table 5: Counter-terrorism assessments by type and year

Security checking of 1 580 staff and officials was undertaken for the G20 Finance Ministers' Meeting held in Melbourne in September 2006.

Aviation Security Identity Cards

Checks for ASICs, including pilots and trainee pilots, continued for people requiring access to security-controlled areas at Australian airports.

Maritime Security Identity Cards

The maritime industry completed its implementation of the MSIC scheme in January 2007. The final number requiring checks by the implementation date was less than the estimated 93 000, so the implementation process had a lesser impact on our resources than anticipated.

Ammonium nitrate

Security checking as part of State and Territory licensing regimes for security-sensitive ammonium nitrate continued – six jurisdictions currently undertake security checking for access to ammonium nitrate.

Australian Nuclear Science and Technology Organisation

The checking of staff and visitors to ANSTO's Lucas Heights facility has been brought within the counter-terrorism checking regime. The security checking relates to staff who do not have a national security clearance and visitors who have access to restricted areas for scientific purposes.

Special events

Security checking of 1 580 staff and officials was undertaken for the G20 Finance Ministers' Meeting held in Melbourne in September 2006. ASIO worked with the Victoria Police, which was responsible for G20 security, and with the sponsoring department, the Department of Treasury, to ensure that all checking was completed within agreed timeframes.

ASIO was also engaged in security checking arrangements for the APEC meetings.

Interaction with other agencies

In carrying out its counter-terrorism security checking responsibilities, ASIO maintains excellent working relationships with the regulatory authorities involved, including the Australian Federal Police (AFP) and the Department of Transport and Regional Services (DOTARS).

The commencement of AusCheck in 2007–08, a new division within the Attorney-General's Department, will enhance counter-terrorism checking with a more robust and purpose-designed system. AusCheck will be responsible for the coordination and assessment of background checks on persons seeking ASICs and MSICs and will maintain a database of cardholders. ASIO is working closely with AusCheck to assist in the transition of this work from DOTARS, including in developing processes and establishing electronic connectivity.

Adverse and qualified assessments

No adverse or qualified security assessments were issued in relation to counter-terrorism security checking during 2006–07, although 50 detailed investigations were initiated.

PERSONNEL SECURITY CHECKING

ASIO provides agencies with personnel security assessments for people who require access to national security classified information and secure areas (see Table 6 on pg.39).

Workload trend

In 2006–07, there was a 16.5% increase in access assessments, however, no single reason for this increase is apparent.

The completion times for access assessments were slowed towards the end of the reporting period due to an influx of requests from the Department of Defence.

Adverse and qualified assessments

One qualified assessment was issued during the year. This assessment provided information to assist the Department in managing a potential risk (see Table 7).

Appeals

A person who is the subject of an adverse or qualified personnel security assessment is notified and has a right of appeal to the Administrative Appeals Tribunal.

There were no appeals lodged or outstanding in 2006–07.

PHYSICAL SECURITY

PROTECTIVE SECURITY AND RISK MANAGEMENT

ASIO provides protective security advice to Australian government clients on a cost-recovery basis. Advice to State and Territory Governments and private sector clients is provided on the same basis after approval from the Attorney-General.

ASIO's advice to the private sector primarily relates to critical infrastructure.

This work, in addition to other activity, saw ASIO recover $950 818 in costs for the year. Advice provided within ASIO was notionally valued at $780 900.

Certification of TOP SECRET sites

ASIO is responsible for the inspection and certification of all sites holding or handling TOP SECRET national security material. Re-certification is required every five years.

ASIO accredited 24 new sites in 2006–07, and an additional 20 sites were inspected and will be considered for certification after completion of physical security improvements.

Accreditation and training of physical security practitioners

ASIO continued to provide accreditation to security practitioners on behalf of the inter-departmental Security Construction and Equipment Committee in addition to the provision of protective security and risk management training.

- ASIO accredits private sector physical security practitioners to enable them to provide advice to government agencies. During the reporting period, a significantly enhanced course, incorporating latest standards, was provided to 19 physical security consultants.
- ASIO's locksmith accreditation package was also enhanced and 53 locksmiths were accredited during the reporting period.

Figure 6: Force-testing of a padlock as part of ASIO's security equipment evaluation (see pg. 40).

Level of access	2002–03	2003–04	2004–05	2005–06	2006–07
Confidential	1 542	1 611	1 951	2 310	3 073
Secret	7 618	9 577	9 372	10 255	11 469
Top Secret	5 112	5 018	5 694	5 343	6 314
Total	14 272	16 206	17 017	17 908	20 856

Table 6: Personnel security assessments – number by level of access sought

	2002–03	2003–04	2004–05	2005–06	2006–07
Qualified	3	2	1	0	1
Adverse	2	0	0	0	0
Total	5	2	1	0	1

Table 7: Personnel security assessments – number of qualified and adverse assessments

Figure 7: Attack testing of a mortice lock as part of ASIO's security equipment evaluation.

ASIO also contributed to 13 other security training courses facilitated by the Protective Security Coordination Centre (PSCC) in 2006–07.

SECURITY EQUIPMENT STANDARDS

ASIO released a new edition of the Australian Government's *Security Equipment Catalogue* in August 2006.

This catalogue lists approved security products for government use that have been evaluated by ASIO on behalf of the inter-departmental Security Construction and Equipment Committee.

A further 85 products have since been evaluated for possible inclusion in the 2008 Catalogue (see Figures 6 and 7).

Enhancement of ASIO's testing facility continued, providing an increased capability for security equipment evaluation and security training.

ELECTRONIC AND AUDIO SURVEILLANCE COUNTER-MEASURES

ASIO conducts electronic and audio surveillance counter-measures testing to assist in the protection of classified and sensitive discussions.

This testing includes electronic surveys, monitoring of government premises for possible hostile electronic activity, and physical security inspections.

Demand for testing remained high in 2006–07.

POLICY CONTRIBUTION

INTER-AGENCY SECURITY FORUM

ASIO continued to provide leadership and secretariat support to the Inter-Agency Security Forum (IASF). The IASF maintains best practice in security within the Australian Intelligence Community (AIC) and related policy departments, through its working groups on personnel, information management and physical security.

IASF members include representatives from all agencies that are represented on the Secretaries' Committee on National Security (SCNS) and the National Security Committee of Cabinet (NSC), as well as the Department of Immigration and Citizenship and the PSCC.

This year, the IASF focused on producing unclassified product for release to the broader government and enhancing the formal links and reporting between related cross-portfolio committees.

Annual reporting on the security of IASF agencies

Drawing on agency reports, ASIO provided SCNS and the NSC with an annual overview report of the status of security in IASF agencies. The report was endorsed by SCNS and noted by the NSC.

For detail on ASIO's Annual Security Status Report please see pg.76.

CONTACT REPORTING SCHEME

Through the Australian Government Contact Reporting Scheme, ASIO seeks to identify potential threats to security by exposing unauthorised attempts to gain sensitive information. The Australian Government *Protective Security Manual* requires Australian government employees to report suspicious, unusual, or persistent contact with foreign nationals.

Trends and analysis

ASIO delivered 89 presentations on the Scheme to Commonwealth, State and Territory agencies.

ASIO will continue to encourage agencies to submit Contact Reports so that appropriate action can be taken to reduce risks to national security.

OUTPUT 3
SECURITY INTELLIGENCE INVESTIGATIONS AND CAPABILITIES

To meet its responsibilities under legislation, ASIO must continue to 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. Activities include:

- maintenance and enhancement of all-source security intelligence collection
- complex tactical and technical analysis
- technical research and development
- counter-terrorism response
- national and international liaison
- policy contribution.

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

SECURITY INTELLIGENCE COLLECTION

INTELLIGENCE COLLECTION

ASIO's collection effort is directed at obtaining information about threats to security as defined by the ASIO Act. The diverse array of threats facing Australia translates into a complex, fast-paced and demanding operational environment.

- The challenge of balancing the urgency, complexity and volume of information is resource intensive.
- Individuals who are the subject of investigation are adept at concealing their activities and intentions, which presents intelligence collection challenges.
- The need to maintain flexiblility in responding to new lead information while maintaining existing ongoing priority investigations provides a further challenge for ASIO due to the need to prioritise resources in assessing potentially serious threats.

ASIO investigations are confined in their scope by law; they are conducted with as little intrusion into privacy as possible, consistent with requirements of security. The use by ASIO of intrusive investigative methods is determined by the seriousness 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.

Management arrangements

During 2006–07 ASIO's Collection Division structure comprised three geographically defined branches managed by Senior Executive Service officers in Sydney, Melbourne and Canberra.

A fourth branch – Collection Resource Coordination – was established in July 2006 to deliver flexible national coordination of:

- specialised resources (such as ASIO's linguists and front-line staff at airports and seaports);
- support to terrorism prosecutions; and
- operational response to special events, such as the Asia-Pacific Economic Cooperation (APEC) forum series of meetings.

The continued evolution of a national approach to coordination of such operational support capabilities is reflected in the creation of a Support to Operations Division in July 2007 and will be reported on in 2007–08.

Covert collection of intelligence and security of ASIO operations requires anonymity. As a result, ASIO's State and Territory offices are not publicly identified and ASIO officers' identities are protected. The largest State and Territory offices are located in the major population centres.

Capability enhancement

Additional resourcing has increased operational flexibility and given ASIO the ability to temporarily re-deploy intelligence collection officers to meet operational needs. During 2006–07, temporary deployments for APEC and in support of intelligence operations enhanced ASIO's intelligence collection efforts.

Growth has placed some strain on line management arrangements. We have increased the number of Senior Officers to allow for a closer focus by senior staff on complex operational and organisational matters. Not all positions are yet filled and the filling of vacant positions is prioritised according to risk management principles and broader Organisational priorities. These positions will be filled by 2010–11.

The requirement to house an expanding workforce has brought forward a program of works to relocate and/or upgrade the facilities in all State offices.

- Secure areas have been designed to match ASIO's business needs and ensure new and enhanced technical

We have increased the number of Senior Officers to allow for a closer focus by senior staff on complex operational and organisational matters.

capabilities can be used to their full extent.

ASIO continued to work towards increasing its capability across a range of languages that are relevant to our investigations.

Support to prosecutions

The work in support of prosecutions has continued to impact on Collection Division. Key legal proceedings relating to the prosecution of 22 individuals in Melbourne and Sydney, stemming from a joint Australian Federal Police (AFP) and New South Wales and Victoria Police investigation, have required ongoing support.

Ongoing matters within the Administrative Appeals Tribunal and various Federal and State Courts have also required support.

Further information on ASIO's support to prosecutions is reported against Output 1 (see pg.32).

ASIO continues to increase its contact with leaders and members of the community.

Impact of legislative change

The changing security environment since 2001 has seen an increase in ASIO's legislated powers. Many of the new powers are designed specifically for the gathering of intelligence. The changes in the legislation reflect not only an increased threat from terrorism, but an environment where subjects of investigation actively seek to modify their behaviours to avoid ASIO scrutiny.

The different investigative tools at ASIO's disposal also enable ASIO to gather enough information to make timely and accurate assessments.

Developing our engagement with the Australian community

ASIO continues to increase its contact with leaders and members of the community. This contact provides context to our investigations.

Operational accountability

ASIO regularly develops and reviews policies and procedures for officers involved in collection operations. Strict accountability mechanisms are employed to ensure the degree of intrusion is approved by an appropriate senior officer.

These policies provide guidance to ASIO officers in the execution of operations, including use of warrant powers.

SPECIAL POWERS – WARRANT OPERATIONS

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

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

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

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

Warrant requests

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

All warrant requests put to the Attorney-General in 2006–07 were approved.

Emergency warrants

The Director-General may issue warrants for up to 48 hours in emergency situations. The Attorney-General is to be advised of any such warrants and the IGIS must receive a copy of the warrant within three working days.

Questioning and detention

ASIO has used its questioning warrant powers prudently since their inception. In 2006, Parliament enacted legislation to allow the warrant regime to continue until 2016. In addition, the Parliamentary Joint Committee on Intelligence and Security is required to review the regime by 22 January 2016, and to report its comments and recommendations to Parliament and the Attorney-General.

Questioning and detention warrants can only be sought as a last resort for the purpose of investigating a terrorism offence where other means of investigation would be ineffective.

Questioning is conducted in the presence of a prescribed authority (a former Federal or serving State senior Judge or the President or Deputy President of the Administrative Appeals Tribunal). The IGIS may attend all questioning. All interviews are video-recorded and a person has the right to access a lawyer at all times.

ASIO is able to question people for a maximum of 24 hours in eight-hour blocks. Where an interpreter is required, a person can be questioned for a maximum of 48 hours, subject to review by the prescribed authority.

ASIO does not have the authority to detain a person. Any detention under an ASIO questioning and detention warrant is managed by police.

These powers do not apply to people under the age of 16. Those who are at least 16, but under 18, can be questioned in the presence of a parent, guardian or appropriate other person.

Under a questioning warrant persons are obliged to answer questions and can be charged for providing misleading answers.

In 2006–07, no questioning or questioning and detention warrants were issued (see Appendix E).

TELECOMMUNICATIONS INTERCEPTION CAPABILITIES

Interception capabilities and delivery systems

ASIO continued to work with the telecommunications industry to ensure comprehensive interception capabilities were in place. 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 carriers and carriage service providers (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.

SURVEILLANCE

ASIO provides leading-edge surveillance capabilities to support the collection of intelligence. Surveillance officers operate in support of two different intelligence objectives: counter-terrorism and counter-espionage. The information collected by surveillance officers supports the collection, analysis and assessment processes within the Organisation.

During 2006–07, business processes were improved in relation to financial controls and accountability.

Investments in technical capability were made to enhance productivity and

Questioning and detention warrants can only be sought as a last resort for the purpose of investigating a terrorism offence where other means of investigation would be ineffective.

operational effectiveness, and enhancements were made to officer safety processes.

MONITORING AND ALERTING

The Research and Monitoring Unit (RMU) is ASIO's conduit for time-critical reporting of security-related information. The RMU has two principal functions:

The Research and Monitoring Unit (RMU) is ASIO's conduit for time-critical reporting of security-related information.

- 'around-the-clock' monitoring and reporting of information available through both classified and unclassified sources about the global and domestic security environment to alert ASIO and Government to significant security events; and
- the provision of information in the public domain and material purchased from commercial providers, including electronic databases to support intelligence analysis, operational activity and administrative functions.

In addition, the RMU is responsible for:

- ASIO's 'after hours' receipt of National Security Hotline calls referred by the Protective Security Coordination Centre; and
- responding to 'out of hours' public line calls.

COMPLEX TACTICAL AND TECHNICAL ANALYSIS

The range and quantity of information requiring analysis by ASIO continued to increase.

Dealing with this increased quantity and range of data has required ASIO to acquire and develop new capabilities and techniques to:

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

These new approaches do not replace traditional methods. They augment them, allowing ASIO to deal with the increased range and quantity of information, and provide new avenues for progressing investigations.

Complex analytical work involves a number of work units within ASIO.

TECHNICAL RESEARCH AND DEVELOPMENT

The ASIO engineering and development group provides technical capabilities to support ASIO's technical intelligence collection capability.

COUNTER-TERRORISM RESPONSE

COUNTER-TERRORISM EXERCISES

ASIO contributed to National Counter-Terrorism Committee (NCTC) training courses and exercises to improve counter-terrorism response capability across Government.

To ensure it remains ready to respond to a terrorist incident, ASIO participates in the NCTC training and exercise program. A comprehensive schedule of exercises brings together Federal, State and Territory security, law enforcement, intelligence and emergency management agencies to test and improve working relationships and capabilities across and between jurisdictions and organisations.

During the reporting period, ASIO participated in the planning and execution of an extensive series of counter-terrorism exercises. They were designed to test security preparations for APEC meetings held in 2007, and to practise national counter-terrorism arrangements.

These exercises were held in New South Wales, Tasmania, Queensland, South Australia and the Northern Territory.

Technical Support Unit

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

NATIONAL AND INTERNATIONAL LIAISON

NATIONAL LIAISON PARTNERS

ASIO continued to develop its strong relationships with a range of Australian partners.

Law enforcement partners

ASIO has well-developed and long-standing relationships with the AFP and State and Territory police services. These relationships have evolved with changes in the security environment and Australia's counter-terrorism legislative framework. ASIO is committed to working with law enforcement partners to prevent terrorism and support terrorism prosecutions.

Technical cooperation

ASIO has well-developed relationships on technical matters with a range of Australian agencies.

Other Australian partners

ASIO has increased the level and frequency of its liaison with other Australian agencies to assist the Organisation carry out its functions. The Australian Customs Service (ACS) and the Department of Immigration and Citizenship (DIAC) are major and long-standing partners.

Information obtained from the ACS and the Australian Transaction Reports and Analysis Centre (AUSTRAC) generated important leads and enabled ASIO to progress its security intelligence investigations.

INTERNATIONAL LIAISON 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.

Section 19(1)(c) of the ASIO Act provides that ASIO may cooperate with authorities of other countries that the Attorney-General approves as being capable of assisting in the performance of ASIO's functions. As at 30 June 2007, ASIO had 306 approved liaison relationships with authorities in 120 countries.

ASIO Liaison Offices

Liaison relationships with international partners are managed by overseas-based ASIO officers and through foreign representatives who are based in, or who visit, Australia. ASIO officers overseas often have responsibility for representing the Organisation in neighbouring countries. They travel regularly to exchange information.

Foreign intelligence service visits

In 2006–07, the Director-General visited the heads of a number of international liaison partners.

COUNTER-TERRORISM INTELLIGENCE TRAINING PROGRAM

The Counter-Terrorism Intelligence Training Program (CTITP) was established in 2005. Its purpose is to deliver counter-

ASIO's Technical Support Unit (TSU) can be called upon to assist the State, Territory and Federal police manage a terrorist incident.

terrorism training and capacity building to enhance security intelligence cooperation with, and between, partner agencies of countries in Australia's region.

The CTITP brings together Australian resources, people and counter-terrorism expertise to assist other countries where requested. It also provides opportunities where the experience and talent of foreign intelligence partners can be shared to improve understanding of the complex task of countering terrorism.

In the first two years of operation, the CTITP has gained wide acceptance and support. It has contributed to the increase of counter-terrorism capacity of partner agencies in the region and facilitated effective regional cooperation.

ASIO has continued to engage …on a range of policy issues expected to impact on interception in the longer term.

POLICY CONTRIBUTION

TELECOMMUNICATIONS INTERCEPTION

Regulatory framework

Part III of the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) provides for ASIO to intercept telecommunications and access stored communications under warrant issued by the Attorney-General.

The *Telecommunications Act 1997* (Cth) requires all C/CSPs, including Internet service providers, to give ASIO and law enforcement agencies such help as is reasonably necessary for the purposes of safeguarding national security, enforcing the criminal law and protecting the public revenue. That help extends to the provision of interception services, including services for executing an interception warrant under the TIA Act.

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

ASIO has continued to engage with the Attorney-General's Department, the Department of Communications, Information Technology and the Arts, the Australian Communications and Media Authority, the telecommunications industry and law enforcement agencies on a range of policy issues expected to impact on interception in the longer term.

Significant policy issues addressed included:

- implementation of the August 2005 *Report of the Regulation of Access to Communications* (the Blunn Review).

In relation to the Blunn Review implementation, ASIO worked closely with the Attorney-General's Department regarding the development of the Telecommunications (Interception and Access) Amendment Bill 2007.

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

Telecommunications Industry obligations and compliance

Since 1 July 1997, the Australian Communications and Media Authority has issued licences to 227 carriers. Approximately 167 of these carriers are now actively providing telecommunications services in the Australian market. There are also 1 718 CSPs registered with the Telecommunications Industry Ombudsman. Of these approximately 932 are listed as Internet service providers.

SUPPORT TO GOVERNMENT COUNTER-TERRORISM ARRANGEMENTS

In 2006–07, ASIO continued to contribute to whole-of-government counter-terrorism policy coordination and national counter-terrorism arrangements. This work focused on the four key phases of prevention, preparation, response and recovery, developed under the auspices of the National Counter-Terrorism Committee (NCTC) and set out in Australia's National Counter-Terrorism Plan (NCTP). The NCTP can be found at www.nationalsecurity.gov.au.

ASIO contributes to each of the four phases of the NCTP. Strategic national-level policy spanning all four phases is developed through a series of high level committees and working groups. ASIO actively investigates potential threats to national security, contributing to the prevention of acts of terrorism. ASIO is involved in national response and recovery arrangements, and participates in training and exercises across Australia and internationally to improve our response capability.

Support to the National Counter-Terrorism Committee (NCTC) and related bodies

The NCTC is Australia's peak body for counter-terrorism policy development. It was established under the 2002 *Inter-Governmental Agreement on Australia's National Counter-Terrorism Arrangements*, to contribute to the security of the Australian community through the coordination of a nation-wide cooperative framework to counter terrorism and its consequences.

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

- contributing to strategic policy advice;
- contributing to the development of an effective nation-wide counter-terrorism capability; and
- sharing relevant security intelligence between agencies and jurisdictions.

There are a number of other bodies nationally that work to support the NCTC, including inter-departmental committees and subject-specific working groups. ASIO is a member of several of those committees that collectively ensure coordination of counter-terrorism policy arrangements.

- The Australian Government Counter-Terrorism Policy Committee is chaired by the Department of the Prime Minister and Cabinet. ASIO provides regular security environment briefings to this key interagency body, which has responsibility for coordination of strategic policy on counter-terrorism issues.
- The Australian Government Counter-Terrorism Committee is chaired by the Protective Security Coordination Centre. This committee regularly reviews the national counter-terrorism alert level to advise Ministers on whether changes to the alert level should be considered.

During 2006–07, ASIO participated in working groups covering a broad range of topics including information sharing, critical infrastructure protection, border security, transport security, and science and technology.

Support to Government Counter-Terrorism Arrangements

While 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 ready to respond to any terrorist incident that may occur.

Under the NCTP, ASIO has responsibility for the National Intelligence Group (NIG),

…ASIO continued to contribute to whole-of-government counter-terrorism policy coordination and national counter-terrorism arrangements.

an operations centre located in ASIO Central Office in Canberra. In the event of a terrorist incident the NIG draws on members of other relevant agencies to coordinate and disseminate intelligence to inform and support senior government decision-makers and operational commanders.

ASIO can activate the NIG for either a major terrorist incident in Australia, or in support of the Inter-departmental Emergency Task Force arrangements. These arrangements are designed to plan appropriate responses to any terrorist incident overseas involving Australians or Australian interests. ASIO supports the Taskforce arrangements by hosting the NIG and maintaining a capability to deploy intelligence support overseas.

For a terrorist incident in any Australian State or Territory, ASIO can also provide direct support to police operational commanders …

For a terrorist incident in any Australian State or Territory, ASIO can also provide direct support to police operational commanders through deployment of intelligence officers and supporting staff to the Joint Intelligence Group and Police Forward Command Post, located at or near the scene of a terrorist incident.

CHANGES TO LEGISLATIVE FRAMEWORK IN 2006–07

Telecommunications (Interception) Amendment Act 2006

The *Telecommunications (Interception) Amendment Act 2006* (Cth) (the Amendment Act) received Royal Assent on 3 May 2006 and amended the *Telecommunications (Interception) Act 1979* (Cth).

The Amendment Act implemented certain recommendations of the Blunn Review. The Amendment Act clarified and enhanced ASIO's telecommunications interception capability.

In particular, the Amendment Act assisted ASIO in countering evasive techniques employed by persons of interest by including the following powers:

- an ability to issue a telecommunications service warrant in respect of the communications of a person known to communicate with a person of interest (known as a 'B Party' warrant);
- an authority to access stored communications alongside traditional telecommunications interception; and
- an ability to issue a named person telecommunications interception warrant based on the identifier of either the telecommunications service or the telecommunications device used by a person of interest.

It is not sufficient to establish that a person is known to communicate with a person of interest for a 'B Party' warrant to be authorised. Such warrants may only be authorised where ASIO has exhausted all other practicable means of identifying the service being used by the person of interest, or it would not otherwise be possible to intercept the service.

A named person warrant, based on a telecommunications device identifier, may not be authorised unless it can be demonstrated that there are no practicable methods available to identify the telecommunications services used by the person of interest, or that interception based on a telecommunications service used by that person (or likely to be) would not otherwise be practicable.

Telecommunications (Interception and Access) Amendment Bill 2007

ASIO provided comments on the Telecommunications (Interception and Access) Amendment Bill 2007 that was introduced into Parliament on 14 June 2007. This Bill seeks to implement further recommendations of the Blunn Review.

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML CTF Act) received Royal Assent on

12 December 2006. It formed part of a legislative package that implemented the first tranche of reforms to Australia's anti-money laundering and counter-terrorism financing regulatory regime.

In particular, the AML CTF Act enables ASIO to access information held by AUSTRAC, Australia's anti-money laundering regulator and specialist financial intelligence unit.

The AML CTF Act limits ASIO officers' ability to disclose AUSTRAC information to the following individuals:

- an IGIS official for the purposes of, or in connection with, the performance of the official's duties in relation to ASIO;
- the ASIO Minister if the disclosure is for the purposes of, or in connection with the performance of the ASIO Minister's functions under the ASIO Act or 'security' within the meaning of the Act;
- the Minister responsible for the administration of the *Telecommunications (Interception and Access) Act 1979* (Cth) in accordance with the Minister's functions under that Act; or
- the Minister who is empowered to issue an authorisation in relation to ASIS under the *Intelligence Services Act 2001* (Cth), provided that disclosure is for the purposes of, or in connection with the exercise of that power.

…the AML CTF Act enables ASIO to access information held by AUSTRAC, Australia's anti-money laundering regulator and specialist financial intelligence unit.

OUTPUT 4
FOREIGN INTELLIGENCE COLLECTION

Output 4 contributes to the Government Outcome of 'a secure Australia in a secure region' by:

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

ENABLING FUNCTIONS

To deliver its outputs ASIO develops and maintains – within legislative and accountability frameworks – enabling functions including:

- people development and management, financial services, information infrastructure and services, and property management
- executive services to provide corporate governance, accountability, strategic coordination, and legal and policy advice
- security of ASIO.

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

PEOPLE DEVELOPMENT AND MANAGEMENT

Decisions taken by the Government in 2005 mean that the number of ASIO staff will grow to 1 860[3] by 30 June 2011. Accordingly, it remains critical that the Organisation attracts, integrates, develops and retains high calibre people.

…a total of 349 new staff joined ASIO…the most staff ever recruited into the Organisation during a financial year…

RECRUITMENT

This year saw the continuation of ASIO's high level of recruitment activity to meet its growth targets. This effort will continue throughout 2007–08 as we seek to fill a broad range of roles with high quality staff.

Recruitment progressed well again in 2006–07; a total of 349 new staff joined ASIO compared to 247 in 2005–06. This was a noteworthy effort as it is the most staff ever recruited into the Organisation during a financial year, and well in excess of the annual net growth target of 170 endorsed by Government. We have bolstered our recruitment area further and have continued to enhance and streamline our processes and recruitment systems.

Notwithstanding these achievements, challenges remain in meeting targets for some specific job families in a tight and competitive employment market.

Recruitment strategies

Further development of a range of strategies ensured recruitment targets were met without compromising standards.

- Prioritised 'job family' campaigns were extended to most ASIO vacancies in 2006–07. This approach minimised the number of separate recruitment processes and facilitated coordinated selection processes. It also enabled better forward planning to ensure effective deployment of resources.
- ASIO continued to use recruitment agencies to assist in sourcing applicants for some roles, coordinate assessment centres, and conduct on-line testing.
- Vetting agencies were employed to support some stages of the vetting processes.

Figure 8: ASIO recruitment promotional material

Figure 9: Intelligence Officer campaign – October 2006

[3] This figure will be slightly above 1 860 (1 879 Full Time Equivalent) flowing from approved additional New Policy Proposals.

- Development of an ASIO recruitment Internet tool progressed in 2006–07, with a view to implementation in late 2007. When deployed, it will improve efficiency in receiving and processing applications, and allow applicants to receive timely and regular updates.
- ASIO enhanced its presence on the Internet and presentations at major universities, and also increased its participation at Australian Intelligence Community (AIC) Roadshows, University Careers Fairs and Defence Resettlement seminars (where we distributed a range of promotional material).
- ASIO undertook further research and development of an organisational 'brand' to position ASIO as a unique and dynamic organisation offering 'careers with meaning' in a wide range of disciplines.

Recruitment advertising

ASIO continued to engage recruitment and advertising agencies to enhance our attraction strategies and ensure we remain a competitive employer. We ran a series of innovative recruitment advertising campaigns in 2006–07 aimed at attracting quality applicants from diverse backgrounds to fill a range of vacancies (see Figures 8 and 9 on pg.58).

These new initiatives drew on results from commissioned market research and highlighted ASIO's ability to offer a 'career with meaning', a valuable point of difference from many other potential employers. The advertisements also built upon previous work aimed at shifting public perceptions of the Organisation, highlighting ASIO as a modern and dynamic workplace. We also successfully re-branded our generic ASIO recruitment advertisements to reinforce the 'meaningful career' message.

Other advertising initiatives included targeted campaigns in relevant industry publications (e.g. legal and engineering magazines) and Internet advertising (e.g. career websites and Google). ASIO's overall recruitment advertising costs for 2006–07 were $2.126m compared to $2.044m in 2005–06.

…new initiatives drew on results from commissioned market research and highlighted ASIO's ability to offer a 'career with meaning', a valuable point of difference from many other potential employers.

STAFFING PROFILE

As at 30 June 2007, staffing levels had increased to 1 356 – an increase of 246 from the previous year (see Figure 10).

The percentage of staff engaged as non-ongoing employees decreased to 10%, which is a substantial decrease from previous years (see Figure 11 and Appendix C).

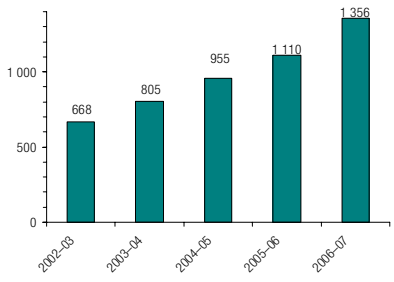
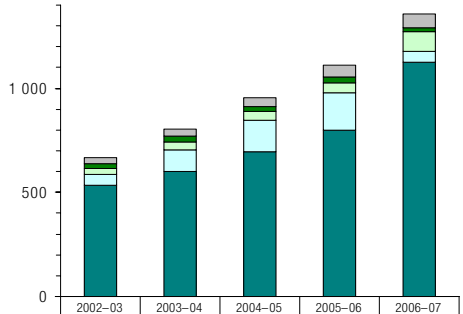


Figure 10: Staffing numbers 2002–03 to 2006–07



	2002–03	2003–04	2004–05	2005–06	2006–07
Non-ongoing Casual	30	33	42	55	64
Non-ongoing Part time	23	28	22	27	18
Ongoing Part time	28	38	43	50	94
Non-ongoing Full time	51	103	155	178	55
Ongoing Full time	536	603	693	800	1 125

Figure 11: Employment status of workforce 2002–03 to 2006–07

This follows a deliberate decision to offer ongoing employment status to many non-ongoing staff as a means of providing the Organisation with a more stable working environment.

Additional data on the staffing profile is contained in Appendix C.

Staff retention

During 2006–07, ASIO engaged an external consultant to undertake an evaluation of its training and development strategies to ensure they remain appropriate and will be effective throughout the period of growth.

ASIO's separation rate for 2006–07 decreased to 5.5% from 6% in 2005–06.[4] In the context of voluntary separation interviews conducted over the past year, staff cited increased remuneration, promotion or career opportunities, work/life balance and greater job satisfaction as major reasons for their departure.

Age of staff

The median age at 30 June 2007 was 38 years with the largest percentage being in the 25-34 years age group. The average age of ASIO's workforce has decreased slightly over the last four years by two years. ASIO's substantial workforce growth in recent years has not significantly altered its age profile.

STAFF DEVELOPMENT

ASIO remained committed to increasing its capability to deal effectively with the security intelligence needs of Australia through continued learning and development of staff. To achieve this ASIO continued to invest in the development of intelligence, technical, leadership, management and administrative capabilities.

In 2006–07, ASIO invested $4.9m (about 2% of our budget) in training and development, an increase of $1.3m since last year. This reflects the additional resources required for the training and development of a growing workforce, and our commitment to ensuring staff are adequately trained to meet the security intelligence needs of the Organisation.

Evaluation of training and development strategies

During 2006–07, ASIO engaged an external consultant to undertake an evaluation of its training and development strategies to ensure they remain appropriate and will be effective throughout the period of growth.

The evaluation included consultation with a range of staff and other AIC agencies, and was benchmarked against Australian Public Service standards.

The evaluation concluded that there is a strong and genuine commitment to learning and development in ASIO, and our learning and development strategies could be enhanced through adopting a number of recommended initiatives. These included:

- more proactive engagement with stakeholders to ensure courses and programs align closely with business needs;
- the establishment of a Training Branch to ensure more focused management oversight, control and consistency across all training and development functions;
- the use of technologies to improve staff awareness of, and access to, information about training and development courses and programs;
- improving ASIO's performance management system to link more closely with training and development; and
- building the basis to more thoroughly measure the effectiveness and efficiency of training and development.

A number of these recommendations align with, and enhance, existing initiatives, and the implementation of recommendations

[4] The separation rate measures the number of staff who left during 2006–07 as a percentage of the total number of staff employed at the end of the period.

had commenced by the end of the period – Training Branch was established on 1 July 2007.

Leadership and management skills

ASIO places a strong emphasis on developing the leadership and management skills of all its Senior Officers. ASIO's *Learning and Development Strategy for Leadership* continues to align our leadership and management capabilities with nationally benchmarked public sector standards. It also provides guidance to individuals when planning their professional development.

All aspects of leadership and management are addressed by a range of learning activities (for example see Table 8).

Leadership and management learning and development also involved:

- four Senior Executive Service (SES) time-outs (one residential), which focused on managing organisational growth and restructuring, workforce and corporate planning, and corporate governance. These programs were addressed by leading academics and practitioners in a range of leadership and management fields; and
- two combined SES and Senior Officer time-outs, which considered a range of organisational issues such as the development of the Corporate Plan, Organisational priorities and direction, preparations for the Asia-Pacific Economic Cooperation (APEC) forum, and legislative developments.

Corporate training

All officers below the SES level are provided learning opportunities under the (classified) *ASIO Officer Capability Strategy*. This strategy ensures that appropriate training and career development occurs across the Organisation.

Corporate training activities include:

- administrative training – contract management, project management, staff selection skills, presentation skills, trainer training, interviewing, effective reading and writing, finance and budgeting;
- IT training – basic and advanced training in the use of ASIO's computer systems;
-

ASIO places a strong emphasis on developing the leadership and management skills of all its Senior Officers.

Activity	Description	Number of attendees
Management to Leadership	A five-day course designed to help managers achieve high quality outcomes through effective leadership of their teams.	49
Diploma of Business (Frontline Management)	Provides essential skills and knowledge to effectively manage staff, resources and projects.	34
Career Development Assessment Centres	Designed to assess a Senior Officer's skills and knowledge against the SES capabilities.	5
Senior Officer Orientation Workshop	An ASIO-specific course designed to provide Senior Officers with an understanding of their management responsibilities and accountabilities.	69

Table 8: Leadership and Management – learning activities

ethics and accountability – all members of staff are required to attend at least once every three years;

- the Studies Assistance Program – supporting tertiary study, including language study, by members of staff; and
- the Director-General's Study Bursaries – supporting members of staff who achieve outstanding results in their studies while maintaining high levels of work performance.

In addition, the ASIO induction program has been reviewed to ensure it continues to be effective. The updated program will be introduced in 2007–08.

ASIO also conducts an internal Seminar Series that consists of monthly presentations on topics of general professional interest to staff. It seeks to foster a sense of teamwork and a shared culture, through broadening knowledge of work areas across the Organisation.

Seminars this year included:

- exposure to new technologies in intelligence analysis;
- ASIO's response to APEC;
- understanding warrant processes;
- the importance of effective security assessments; and
- roles and responsibilities of managers.

To mark International Women's Day, Ms Pru Goward presented on her experiences and observations as the former Sex Discrimination Commissioner and Commissioner Responsible for Age Discrimination.

There was a steady increase in the demand for training for Intelligence Officers and Intelligence Analysts in 2006–07.

Intelligence Training

There was a steady increase in the demand for training for Intelligence Officers and Intelligence Analysts in 2006–07.

Demands for intelligence training will continue to increase in 2007–08.

Australian Intelligence Community Training

ASIO supports the continued efforts to broaden the understanding of the whole-of-government approach to intelligence needs and partnerships. This includes by providing presenters and participants to the AIC-wide induction and Senior Officer development programs.

Language training

ASIO continued to invest in the development of language skills.

- The full-time training program in languages relevant to ASIO's investigative work for selected officers continued. This training included formal classroom instruction in Australia and overseas.
- ASIO Liaison Officers who require language training undertake full-time language courses with the Department of Foreign Affairs and Trade, including one-on-one tutorials, small group learning and 'in-country' training.
- ASIO's Linguists are provided with training to refine and enhance their skills.

Secondments

ASIO has a well-developed secondment program which embeds staff from the following agencies within the Organisation:

- Australian Transaction Reports and Analysis Centre (AUSTRAC);
- Australian Federal Police (AFP);
- Australian Secret Intelligence Service (ASIS);
- Defence Imagery and Geospatial Organisation;
- Defence Intelligence Organisation;
- Defence Science and Technology Organisation;
- Defence Signals Directorate;

- Department of Defence;
- Department of Finance and Administration;
- Department of Foreign Affairs and Trade;
- Department of Transport and Regional Services; and
- Office of National Assessments (ONA).

Complementing this cooperation and engagement, in 2006–07 ASIO seconded officers to the AFP, ASIS, the Department of the Prime Minister and Cabinet (PM&C) and ONA.

Special achievement and meritorious performance awards

ASIO recognises and rewards the meritorious performance and special achievements of both individuals and teams through an awards program. The awards are conferred in two ceremonies; the first is on Australia Day, 26 January; the other on Foundation Day, 16 March, the anniversary of ASIO's establishment.

Foundation Day 2007 was the first time a Governor-General of Australia had visited ASIO's Central Office in Canberra. His Excellency Major General Michael Jeffery AC CVO MC delivered a speech to ASIO staff reflecting on the changes that have taken place in the global security environment since ASIO was established in 1949. His Excellency concluded the Foundation Day ceremony by presenting awards for special achievement and meritorious performance.

HUMAN RESOURCE POLICY AND PRACTICE

Workplace relations and reforms

The following initiatives were implemented during 2006–07:

- a pay increase through a staff Workplace Agreement, with additional increases scheduled over the next two years;
- changes to the employment framework for non-ongoing staff to enable them to apply for a broader range of positions;
- a formal job-sharing arrangement to provide greater work/life balance opportunities; and
- conditions of service proactively promulgated to increase staff awareness.

The ASIO Consultative Council – which comprises management and staff representatives – maintains an oversight of workplace relations, including those relating to the implementation of initiatives contained in the current Workplace Agreement. The Council met monthly throughout the year (see also pg.71).

WORKPLACE DIVERSITY

Active management of the (classified) *Workplace Diversity Program 2005–09* continued. The program encourages the recognition and appreciation of individuals and their contribution to the corporate mission and objectives. Workforce diversity is monitored through the collection and reporting of relevant statistics to the Senior Management team.

Harassment contact officers

Following the restructure in July 2006, elections for new Harassment Contact Officers were held to ensure effective representation across the Organisation. This assisted in raising awareness of support mechanisms available to staff should they experience harassment.

Diversity statistics

At 30 June 2007, the representation of women in ASIO's workforce was 45.5%. Women comprised 25.7% of the SES (an increase from 21.4% in 2005–06) and 32.8% of Executive Level staff (compared to 32.6% in 2005–06) (see Figure 13 on pg.64). The representation of ethnically diverse staff has decreased slightly in

Figure 12: His Excellency Major General Michael Jeffery AC CVO MC, Governor-General of the Commonwealth of Australia, addresses ASIO staff on Foundation Day

2006–07. Additional data on workforce diversity is contained in Appendix C.

Staff survey

In March/April 2007, a staff survey was conducted to measure perceptions, attitudes, concerns and areas of satisfaction across a range of key cultural, security and people management performance dimensions. The response rate of 79% exceeded the 2005 survey response rate of 76%. Key findings of the 2007 survey included:

- staff enjoy the team environment, the interesting, rewarding and challenging nature of their work, and the ability to contribute positively to the Australian community;
- staff believe the Organisation has a clear set of values which is relevant to their work;
- staff are satisfied with opportunities for promotion, job rotation, transfer, remuneration and recognition; and
- responses indicated improvement across all key survey areas compared to 2005 survey results.

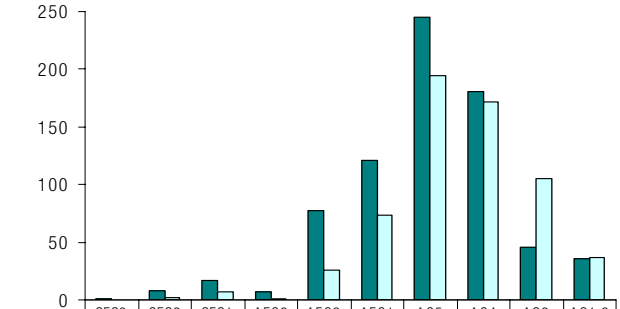
Overall, the survey indicated staff are very committed to the Organisation and strongly support its mission, goals and objectives.

Overall, the survey indicated staff are very committed to the Organisation and strongly support its mission, goals and objectives.

A small percentage of staff identified areas, such as the management of underperformance, that require improvement. These were the subject of further consideration by the Senior Management team, with the aim of developing and implementing appropriate strategies to address the issues.

Disability Strategy

ASIO continues to manage the issue of disability through the *Disability Action Plan 2005–09*. The Plan ensures people with disabilities are treated in accordance with the principles of equity, inclusion, participation, access, and accountability. These principles are incorporated into ongoing planning and service delivery.



	SES3	SES2	SES1	AE03	AE02	AE01	A05	A04	A03	A01-2
Males	1	8	17	7	77	121	245	181	46	36
Females	0	2	7	1	26	73	194	172	105	37

Figure 13: Workplace diversity - gender representation by classification

Notes:

1. Classifications include equivalent staff in the Engineer and Information Technology classifications
2. ASIO Officer 5 translates to APS Level 6 classification level
3. ASIO Officer 4 translates to APS Level 5 classification level

Occupational Health and Safety

ASIO seeks to achieve the highest Occupational Health and Safety (OH&S) standards for its staff, and implement the systems required to sustain and promote healthy and safe work environments. During the year, ASIO focused on initiatives to effectively manage health and safety for a rapidly growing workforce.

Injury Prevention

With a strategic focus on preventing workplace injuries, ASIO:

- established a system for the timely provision of ergonomic workstation assessments;
- revised the Designated Work Group structure to reflect organisational growth;
- enhanced consultative arrangements, ensuring the growing workforce is well-represented on OH&S matters;
- completed a number of risk assessments and implemented the recommended control strategies; and
- established health and safety training programs.

Injury Management

To manage injuries sustained by staff and mitigate the direct and indirect costs ASIO:

- established an early intervention framework to ensure staff members are maintained at work or have a plan in place to facilitate timely and durable return to work;
- educated supervisors on managing absenteeism, recognising trends, and notifying the OH&S Section as soon as a staff member reports symptoms or an injury; and
- educated staff on the need to communicate any health and safety concerns, injuries or symptoms impacting on their ability to work.

Auditing and Compliance

The data collection phase of the SafetyMAP audit reported in 2005–06 has been completed. Data analysis was underway at the end of the reporting period and preliminary findings are expected to be circulated to relevant stakeholders in 2007–08.

Health Promotion

ASIO continued to implement its health and wellbeing strategy, focusing on a range of seminars as well as on-site health appraisals, an influenza vaccination program, and the encouragement of staff to participate in a range of physical and social activities.

During the year, ASIO focused on initiatives to effectively manage health and safety for a rapidly growing workforce.

Workplace Incidents

One incident was notified to Comcare under section 68 of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*.

Workers' Compensation Claims

Twenty workers' compensation claims were submitted in 2006–07. Liability was accepted for 16 claims and determination of liability is pending for three claims. Liability was denied for two claims (one claim was submitted in the previous financial year).

Notice and Investigations

An investigation was conducted under section 41 of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*. This resulted in a section 46 Improvement Notice being issued in July 2006, relating to potential safety issues associated with working on the roof area of ASIO's Central Office building in Russell, ACT. Remedial action was taken to address the concerns, and Comcare provided written advice confirming that ASIO had adequately addressed the requirements set out in the Improvement Notice.

Performance pay

In recognition of their performance during 2005–06, 27 substantive and two temporarily acting members of the SES received bonus payments in 2006–07, with individual amounts ranging from $1 934 to $15 475. The average payment was approximately $6 420 and the total amount paid was $186 178.

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.

FINANCIAL SERVICES

PURCHASING

All purchasing activity in ASIO is conducted in accordance with the *Chief Executive's Instructions*, which require officers to have regard for 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 ASIO's Intranet. The Instructions give direction on purchasing goods and services and entering into, and managing, contracts, agreements and other procurement arrangements. Staff are provided with guidance on procurement policy and practice, along with document templates.

In 2006–07, ASIO's annual investment program continued. Purchasing objectives focused on equipment to support growth in key business areas including technical capabilities. Additionally, procurement was conducted in relation to information infrastructure and accommodation to support staffing growth.

COMMONWEALTH PROCUREMENT GUIDELINES AND EXEMPT CONTRACTS

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 on request.

CONSULTANTS

During 2006–07, ASIO let 16 consultancy contracts, an increase from eight in 2005–06. The total expenditure during the year on consultancy contracts valued at $10 000 or more (including contracts let during the previous year) totalled $0.864m, up from $0.369m in 2005–06.

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 13 Restricted Requests for Tender during 2006–07. In each case the Request for Tender was not advertised publicly for security reasons. Instead, a restricted set of suppliers was invited to tender.

INFORMATION INFRASTRUCTURE AND SERVICES

INTELLIGENCE ANALYSIS CAPABILITY DEVELOPMENT PROGRAM

During 2006–07, ASIO deployed a new document ingestion system that enables robust search and alerting capability against large volumes of incoming intelligence reports and open source information.

CONNECTIVITY IMPROVEMENTS

ASIO continues to enhance business outcomes, with advances in its information and communication technology platforms and improved connectivity with key Australian and international partners.

These initiatives enable our business areas to be more responsive, robust and effective.

EXPANDING INFRASTRUCTURE PROGRAM

ASIO developed its information and communications technology infrastructure during 2006–07 to meet the demands of an expanding organisation.

- Initial deployment of a mobile communications solution, the purchase of large-scale data storage arrays and expanded software licensing agreements contributed to the growing infrastructure program.

Project governance

Improvements to the governance of projects were made during the year:

- Program Boards, with representation at a senior level from across the Organisation, were established to oversee IT capability development projects and ensure they deliver the required organisational capabilities; and
- working groups were established to manage other ongoing infrastructure programs, including:
  - redesign of analytical systems;
  - refurbishment of ASIO's Central Office; and
  - increased bandwidth for ASIO's networks.

BUSINESS CONTINUITY

ASIO continued the development of its classified *Business Continuity Plan*, and responsibilities for all aspects of the Plan have been assigned to teams of staff drawn from across the Organisation. Locations for remote contingency sites have been selected.

A project team has coordinated the documentation of recovery procedures and conducted desktop exercises. Ongoing testing of the Plan and the equipment that supports it will be required.

RECORDS MANAGEMENT

A review of ASIO's information management processes commenced to ensure the Organisation is well-positioned to continue the management of information as an asset and strategic resource. Improvements to ASIO's records management processes continued throughout 2006–07.

Processing Backlogs

The rate and volume of information flowing to and from ASIO, including new streams of intelligence, continued to increase. ASIO processed all priority material quickly but the backlog of routine papers awaiting filing remained steady.

During 2006–07, ASIO deployed a new document ingestion system that enables robust search and alerting capability against large volumes of incoming intelligence reports and open source information.

PROPERTY MANAGEMENT

The growth in staff numbers, flowing from the Government's decision in 2005 to increase the size of ASIO, has put pressure on ASIO's accommodation nationally. A new Central Office building is required in Canberra to accommodate the expansion of ASIO, to be co-located with an expanded ONA. ASIO's offices in each State capital also will grow. The Central Office building in Russell, Canberra, is the only building that is declared publicly.

A new Central Office building is required in Canberra to accommodate the expansion of ASIO, to be co-located with an expanded ONA.

NEW OFFICES AND RENOVATIONS

Central Office, Canberra

On 12 April 2006, the Government agreed that ASIO and ONA needed more space and a new Central Office building in Canberra was appropriate.

On 16 August 2006, the Attorney-General and the Minister for Finance and Administration announced that ASIO and ONA would move to a purpose-built building within Canberra's defence and security precinct.

The new building will be constructed in partnership between ASIO, ONA and the Department of Finance and Administration (DoFA). It will be located on Commonwealth land between Constitution Avenue and Parkes Way, next to Anzac Park East.

The site is known as Section 49, Parkes, located within the Parliamentary Triangle, and in close proximity to the Russell Precinct and other partner agencies (see Figure 14).

The new building will be purpose-designed to operate 24 hours a day with a level of security commensurate with the functions of the Organisation. A project architect and managing contractor were engaged early in 2007–08 to commence design and development of the new building.

The Government provided additional funding to DoFA, ASIO and ONA in the 2007–08 Budget. The total project budget is $460m.

State and Territory offices

The Organisation's growth has put pressure on accommodation in our State and Territory offices. Funding was provided in the 2005–06 Additional Estimates, and in both the 2006–07 and 2007–08 Budgets, for the expansion of

Figure 14: Location of new ASIO building

these offices. Significant progress has been made to deliver new and refurbished accommodation nationally.

The new and refurbished offices provide:

- flexible, multi-functional environments that can be rapidly converted to accommodate operational task force units in response to emerging issues; and
- contemporary fit-out solutions while maintaining the rigorous security standards that are a necessary requirement of the Organisation.

The locations of ASIO's State and Territory offices are not publicly declared.

ENVIRONMENTAL PERFORMANCE

All ASIO contracts include clauses that ensure best use is made of recycled materials and fixtures, and fittings are recycled wherever possible.

All new or refurbished office fit-outs utilise energy efficient T5 lighting and variable volume air handling units. They also employ water-saving and recycling measures to all wet areas in an endeavour to achieve an Australian Greenhouse Building Rating of at least 4 stars – one of our offices has achieved 4.5 stars.

The Building Management System installed in the Central Office was expanded to monitor and control more elements of building plant and equipment. This allows us to optimise the operation of these units to deliver maximum efficiency.

The Organisation's demand for energy continues to climb as ASIO enhances its capabilities in line with advances in technology. While the Organisation's computer systems are designed with energy efficiency in mind, increases in staff numbers, and further expansion of ASIO's 24x7 operations, has driven total energy demands upward.

ASIO recycles cardboard waste and has engaged a service provider to recycle computer packaging, including polystyrene components. The Organisation is moving to recycle its end-of-life unclassified IT equipment including computers, monitors, printers, faxes, scanners and photocopiers. The recycling process will result in the re-use of up to 95% of the component material. Requirements for the protection of national security material prevent ASIO from recycling classified IT equipment.

BUILDING MANAGEMENT

ASIO worked closely during the year with DoFA – via the Department's contracted property manager United Group Services – to upgrade major plant and equipment in ASIO's Central Office:

- a third electricity supply was introduced to the building; and
- the uninterruptible power supply (UPS) system was replaced with a Dual Redundant UPS System, providing greater capacity in line with the increased power demands of both ASIO and ONA.

In 2007–08, ASIO intends to replace the main chiller units, which will provide the building with more efficient air-cooling capacity, and upgrade the passenger lifts to meet the current building code and standards.

EXECUTIVE SERVICES

STRENGTHENING PARTNERSHIPS

ASIO continued to develop the strength and breadth of its engagement with government agencies to provide a better understanding of ASIO and security intelligence, and to identify and maximise opportunities for further engagement.

In 2006–07, ASIO continued to strengthen its relationships with government agencies through various high-level meetings and committees.

ASIO continued to develop the strength and breadth of its engagement with government agencies to provide a better understanding of ASIO and security intelligence, and to identify and maximise opportunities for further engagement.

CORPORATE GOVERNANCE

Corporate governance in ASIO is exercised through two high level corporate committees: the Director-General's Meeting and the Corporate Executive.

ASIO's corporate governance arrangements support the regular critical measurement and evaluation of performance across the range of Organisational functions, as well as providing for transparency and accountability.

In 2006–07, ASIO's corporate governance arrangements were strengthened and streamlined, including enhancements to corporate committee reporting frameworks.

Corporate governance in ASIO is exercised through two high level corporate committees: the Director-General's Meeting and the Corporate Executive.

- The Director-General's Meeting is held twice weekly and comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. It manages the day-to-day business of ASIO, including areas of ongoing corporate priority and urgent or emerging issues requiring consideration by the Executive.
- The Corporate Executive meets twice monthly and comprises the Director-General, Deputy Directors-General, First Assistant Directors-General and two managers on rotation, with the Staff Association President attending as an observer. It sets ASIO's strategic direction and

Figure 15: ASIO's corporate governance arrangements

oversees resource management, providing 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 ASIO's *Annual Report*.

The Director-General's Meeting and Corporate Executive manage a number of corporate committees that formally report to them (see Figure 15 on pg.70). In 2006–07, these committees grew from six to eight, reflecting the Organisation's focus on effectively managing growth and capability enhancement.

- The Intelligence Coordination Committee, chaired by a Deputy Director-General, includes senior managers involved in the intelligence process. The committee sets security intelligence investigative priorities and allocates broad resources to these on a risk management basis. It also performs quarterly reviews against strategic objectives and approves arrangements for ensuring the legality and propriety of ASIO's intelligence collection, analysis and advice.
- The Audit and Evaluation Committee, chaired by a Deputy Director-General, includes a senior executive from the Australian National Audit Office. The committee facilitates the internal audit of ASIO in accordance with the Internal Audit Charter, by setting priorities for audit, fraud control and evaluation planning. It also considers the findings of the internal audits and evaluations and ensures management-endorsed recommendations are implemented.
- The Organisational Development Committee, chaired by the head of Corporate Management Division, includes the Staff Association President. This new committee provides strategic guidance on ASIO's growth with particular regard to growing the capabilities of ASIO's staff, shaping an appropriate culture and managing change.
- The Staff Placements Committee is comprised of two of the Deputy Directors-General, who make strategic decisions on staff commencements and placements.
- The Security Committee, chaired by the head of Security Division, includes the Staff Association President. It reviews and addresses key issues relevant to the security of ASIO people, property and performance. The committee also provides a consultative forum to develop security policies and practices.
- The Research and Development Committee, chaired by the head of Technical Capabilities Division, includes a representative from the Defence Science and Technology Organisation. This new committee provides strategic oversight and direction to technical collection and analysis capability.
- The Information Management Committee, chaired by the head of Information Division, provides strategic oversight and direction to ASIO's information and communication technology work program.
- The ASIO Consultative Council, co-chaired by the head of the Corporate Management Division and the Staff Association President, comprises representatives from management and the Staff Association. The committee makes recommendations to the Director-General on personnel policies and practices. It is an advisory and deliberative body, enabling management and staff discussion and resolution of issues of mutual interest and concern.

In 2006–07…committees grew from six to eight, reflecting the Organisation's focus on effectively managing growth and capability enhancement.

ACCOUNTABILITY

ASIO operates under an extensive oversight and accountability framework, which includes the Government, the Parliament, and the Inspector-General of Intelligence and Security (IGIS). This provides assurance that ASIO's work is transparent and part of a coordinated response to protecting Australian interests and its people.

Figure 16: Attorney-General the Hon Philip Ruddock MP addresses ASIO staff

National Security Committee of Cabinet

The National Security Committee of Cabinet (NSC), chaired by the Prime Minister, determines the strategic direction for Australia's intelligence agencies. It considers the major long-term issues relevant to Australia's national security interests. As the Government's peak body on national security, the NSC sets the budgets for intelligence agencies (including ASIO) and considers performance throughout the year, which includes reviewing ASIO's classified *Annual Report*.

The Director-General is a member of the NSC, ensuring it has timely and relevant information in considering security matters.

Attorney-General

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

ASIO briefs the Attorney-General on all matters concerning national security, including its investigations and operations. In 2006–07, ASIO provided 358 briefings and submissions to the Attorney-General, compared to 304 in 2005–06. The rise reflects the growth of the Organisation and the continued increase in briefings on legal issues in which ASIO has involvement.

The Attorney-General also receives reports from the IGIS on any inquiries or complaints relating to ASIO.

Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (the Committee) plays a significant role in the oversight and accountability framework of ASIO. The Committee has a number of functions in its mandate, which includes to:

- review the administration and expenditure of ASIO (and the other intelligence agencies);
- review the listing of an organisation as a terrorist organisation under the *Criminal Code Act 1995* (Cth) (see also pg.24 on Proscription);
- review questioning and detention powers; and
- inquire into other matters referred to it by the Government or Parliament.

The Committee's comments and recommendations are reported to each House of the Parliament and to the responsible Minister.

The Committee's membership is included as Appendix A.

Review of administration and expenditure

The Committee selects different areas for review each year. In 2006–07, the focus of the Committee's *Review of Administration and Expenditure No.5* included:

- the impact of legislative changes on administration;
- human resource management;
- organisational structure and staff distribution;
- security issues;
- public relations and reporting;
- strategic planning and management of growth; and
- performance management and evaluation.

On 28 February 2007, ASIO submitted a classified submission to the Committee and an unclassified version suitable for

release to the public – the unclassified version is available on ASIO's website www.asio.gov.au. On 23 March 2007, the Director-General appeared (in camera) before the Committee in relation to the Review.

The Committee's report on its *Review of Administration and Expenditure No.5* will be tabled early in 2007–08.

Proscription of terrorist organisations

As part of the Committee's process of reviewing the listing of terrorist organisations, the Director-General appeared before the Committee on:

- 18 June 2007 (in camera), in connection with the Review of the re-listing of Hizballah's External Security Organisation as a terrorist organisation; and
- 23 March 2007 (in camera), in connection with the Review of the re-listing of Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn as a terrorist organisation.

The Deputy Director-General also appeared before the Committee on:

- 4 April 2007, at the Inquiry into the Terrorist Organisation Listing Provisions of the *Criminal Code Act 1995* (Cth); and
- 27 November 2006 (in camera), in connection with the Review of the re-listing of Abu Sayyaf Group, Jamiat ul-Ansar, Armed Islamic Group and Salafist Group for Call and Combat as terrorist organisations.

Other Inquiries

There were no ASIO-specific matters referred to the Committee for inquiry by the Government or Parliament in 2006–07.

Other Parliamentary Oversight

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

- 31 October 2006 and 23 May 2007, before the Senate Standing Committee on Legal and Constitutional Affairs as part of the Senate Estimates process; and

On 28 February 2007, ASIO submitted a classified submission to the Committee and an unclassified version suitable for release to the public…

Figure 17: ASIO Annual Reports

- 6 March 2007, before the Senate Finance and Public Administration Committee in relation to the Access Card – Inquiry Into Human Services (Enhanced Service Delivery) Bill 2007.

ASIO also responded to a number of Questions on Notice from Parliamentarians.

…the IGIS was satisfied that there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or human rights.

Inspector-General of Intelligence and Security (IGIS)

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

Monitoring and review

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

- use of special powers under warrant;
- access to and use of AUSTRAC and Australian Taxation Office information;
- compliance with the Archives Act;
- 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 IGIS in 2006–07, the IGIS was satisfied that there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or human rights. Further details can be found in the IGIS's Annual Report at www.igis.gov.au.

Audit, evaluation and fraud control

Internal audits and evaluations

Throughout the year, 11 internal audits and one evaluation in relation to training and development (see pp.60–61) were completed and were the subject of (classified) reporting to ASIO's 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.

Fraud Control in ASIO

During 2006–07, ASIO launched its *Fraud Control Plan 2006–2008* (the Plan) based on current fraud risk assessments.

ASIO also completed the Commonwealth Fraud Control Guidelines Annual Questionnaire and holds data as required under the Guidelines. The AFP has been advised of ASIO's major fraud risks.

One of our main strategies in minimising fraud is an ethics and accountability program that all members of staff must attend at least once every three years. The Office of the IGIS contributes to this program.

In addition, all new staff, Senior Officers and relevant external providers and clients are provided with a user-friendly *Guide to Fraud Prevention, Detection and Reporting Procedures in ASIO*, and the Plan is available on ASIO's Intranet.

There were no suspected or actual incidents of fraud reported in 2006–07.

Assumed identities

All use of assumed identities in ASIO is authorised under Part 1AC of the *Crimes Act 1914* (Cth), commonly referred to as the 'Commonwealth Assumed Identity Scheme' and in accordance with the New South Wales *Law Enforcement and National Security (Assumed Identities) Act 1998*.

The Commonwealth legislation provides a mechanism whereby the Director-General and delegates may authorise the use of

assumed identities and the acquisition of supporting documents from Commonwealth agencies and non-government agencies.

The New South Wales legislation is used by ASIO in addition to the Commonwealth scheme where evidence of assumed identity is sought in New South Wales.

As required under the Commonwealth Assumed Identity Scheme, audits were conducted in July 2006 and January 2007 of records of authorisations with no discrepancies detected. Likewise, in accordance with the New South Wales legislation, the records were audited for the reporting period and there were no breaches of the legislation reported.

In addition, the IGIS regularly audits ASIO's use of assumed identities. There have been no instances identified of improper use of assumed identities. As required by the legislation, a report for 2006–07 on the number of authorisations, the general activity undertaken with the use of assumed identities and on relevant audit results, has been provided to the IGIS.

Identity security regimes

In 2006, ASIO received $1.562m over four years. This was as part of a cross portfolio initiative designed to combat identity crime through the creation of a common proof of identity under the auspices of the Document Verification Service.

Accessibility to the public

ASIO website

ASIO's website (www.asio.gov.au) is its primary channel for providing information that is able to be made available publicly. During 2006–07, the website was redeveloped to make it more accessible and user-friendly. The changes better aligned it with Australian Government Information Management Office standards.

Media policy

The Media Liaison Officer is the central point of contact for inquiries from journalists. ASIO does not comment on sensitive national security matters such as its investigations, operational methods and liaison with overseas agencies. The Media Liaison Officer's telephone number is listed in the telephone directories of all State and Territory capitals.

Public statements

In 2006–07, the Director-General addressed business fora, government agencies, conferences, international partners, institutions and ASIO staff – 18 of these statements are available on ASIO's website.

In 2006–07, the Director-General addressed business fora, government agencies, conferences, international partners, institutions and ASIO staff – 18 of these statements are available on ASIO's website.

Some of the topics highlighted in these addresses included:

- the real and continuing threat of terrorism and other threats to security;
- the challenges and responsibility to provide the highest levels of service to Government and the people of Australia;
- the importance of ASIO's international engagement with intelligence, security and law enforcement agencies in countering the threat of terrorism in Australia;
- the threat of terrorism affecting the business sector and the need for a cooperative, well-informed approach to terrorism across all levels of government, business and the wider community;
- the role and future of security intelligence within the Australian context; and
- national security and the role of the media.

CORPORATE PLAN

In March 2007, ASIO launched its *Corporate Plan 2007–2011* which is available at www.asio.gov.au.

This Plan sets the broad framework for how ASIO does its business, measures its performance and achieves its outcomes. It sets out the critical success factors driving

ASIO, maps out where it needs to be in 2012, and provides a guide to meeting the expectations of the Government, the Parliament and the Australian community.

ASIO's business focus in 2006–07 was to:

- counter threats to security;
- manage growth and change;
- enhance the capability of our people;
- shape an appropriate culture – to achieve a loyal, innovative, flexible and cohesive workforce; and
- increase the capability of our technology and systems.

The strength of ASIO's security culture was reflected in the Staff Survey conducted in early 2007.

SECURITY OF ASIO

EXCELLENCE IN SECURITY PRACTICE

Security in ASIO is a collective responsibility – best security practice is the responsibility of every ASIO member of staff.

The strength of ASIO's security culture was reflected in the Staff Survey conducted in early 2007. The survey results indicated the majority of staff support ASIO's security measures, have a good understanding of specific security arrangements and requirements, and have a high level of comfort in approaching security staff for advice and assistance on security matters.

During 2006–07, we continued to strengthen our security culture through:

- awareness and education;
- increased accountability, including audits;
- personnel security;
- enhanced physical security measures; and
- information technology security.

SECURITY AWARENESS AND EDUCATION

Security awareness briefings and activities include an initial induction, (classified) *House Security Instructions*, formal presentations and circulation of policies to all members of staff, security briefings, articles in the staff newsletter and the revalidation and re-evaluation of security clearances.

Security policies

ASIO's security policies are developed in response to emerging security trends and reflect the current operating environment. All policies are endorsed by ASIO's Security Committee (see also pg.71), are consistent with the Inter-Agency Security Forum (IASF)[5] best practice, and conform to the *Australian Government Protective Security Manual* (PSM) and the *Australian Government Information and Communications Technology Security Manual* (ACSI33). Policies are circulated to staff and available on ASIO's Intranet site.

In 2006–07, an advanced presentation on security classifications and caveats was developed in addition to induction training.

House Security Instructions

ASIO's (classified) *House Security Instructions* place the mandatory security standards set by Government into the ASIO context and incorporate ASIO-specific requirements. Members of staff must read them at least annually. A review of the Instructions has begun and is expected to be completed in 2007–08.

SECURITY ACCOUNTABILITY

This year's review of ASIO's security plan was conducted in accordance with the PSM and resulted in minor amendments.

Annual Security Status Report

Significant findings in ASIO's *Annual Security Status Report* for 2005–06 to the

[5] The IASF maintains best practice in security. See pg.40 for more information on the IASF.

National Security Committee of Cabinet were:

- ASIO regards security as a top priority and has well-established security policies and procedures; and
- the number and percentage of security breaches have declined significantly due to staff attention to a revised security policy which came into effect on 1 July 2005.

Security audits

No major issues were identified in this year's security audits, which were conducted in line with requirements of the PSM and those endorsed by the IASF.

PERSONNEL SECURITY

Security clearance re-evaluations

ASIO continues to conduct re-evaluations of all TOP SECRET vetted staff, contractors and appropriate associates within six years (a requirement of the PSM).

The number of security clearance re-evaluations is growing with the growth of the Organisation. ASIO is seeking to identify efficiencies – resources in this area will grow, but meeting the workload will be challenging.

Personal security

Personal security is monitored through annual supervisor and clearance-holder appraisals, and in more detail at the 30-month revalidation and the five-yearly re-evaluation of security clearances.

ASIO manages issues of staff concern through formal and informal means. Where issues of concern are identified, action is tailored to meet the specific circumstances and an individual's needs.

Suspicious incidents

All members of staff are encouraged to report suspicious incidents involving ASIO premises or staff. During 2006–07, there were a small number of incidents involving staff being threatened by members of the public. These were investigated and managed to ensure the safety of staff.

Employee Assistance Program

ASIO's Employee Assistance Program provides assistance to staff in dealing with personal issues.

PHYSICAL SECURITY

During 2006–07, enhancements were made to ASIO's physical security measures.

Security Working Groups

Security Working Groups oversee the security requirements for all new ASIO office locations.

IT SECURITY

IT security advice and assistance was provided to major IT projects to ensure practical security requirements were incorporated into system design.

Building on efforts undertaken in previous years, the breadth and depth of ASIO's IT security audit capability was expanded during 2006–07.

Next year will see significant security challenges and opportunities arise through major IT and accommodation projects. It is also expected that the number of security threats from the Internet will continue to rise, requiring increased effort over the coming years.

The number of security clearance re-evaluations is growing with the growth of the Organisation. ASIO is seeking to identify efficiencies – resources in this area will grow, but meeting the workload will be challenging.

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

I have audited the accompanying financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2007, which comprise:

- Statement by the Director-General;
- Income Statement, Balance Sheet and Cash Flow Statement;
- Statement of Changes in Equity;
- Schedule of Commitments;
- Schedule of Contingencies; and
- Notes to and forming part of the Financial Statements.

The Responsibility of the Director-General for the Financial Statements

The Director-General is responsible for the preparation and fair presentation of the financial statements in accordance with the Agreement between the Attorney-General and the Finance Minister. This Agreement requires the financial statements to be prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997* and the Australian Accounting Standards (including the Australian Accounting Interpretations), except where disclosure of information in the notes to and forming part of the financial statements would or could reasonably be expected to be operationally sensitive.

The Director-General's responsibility for the financial statements includes establishing and maintaining internal controls relevant to the preparation and fair presentation of the financial statements that are free from material misstatement, whether due to fraud or error; selecting and applying appropriate accounting policies; and making accounting estimates that are reasonable in the circumstances.

Auditor's Responsibility

My responsibility is to express an opinion, based on my audit, as to whether the financial statements are fairly presented in accordance with both the Agreement and the Australian Accounting Standards. My audit has been conducted in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. These Auditing Standards require that I comply with relevant ethical requirements relating to audit engagements and plan and perform the audit to obtain reasonable assurance as to whether the financial statements are free from material misstatement.

GPO Box 707 CANBERRA ACT 2601
19 National Circuit BARTON ACT 2600
Phone (02) 6203 7300 Fax (02) 6203 7777

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the Australian Security Intelligence Organisation's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Australian Security Intelligence Organisation's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by the Australian Security Intelligence Organisation's Director-General, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

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 Agreement between the Attorney-General and the Finance Minister, which invokes the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, and the Australian Accounting Standards (including the Australian Accounting Interpretations); and

(b) give a true and fair view of the matters required by the Agreement between the Attorney-General and the Finance Minister, including the Australian Security Intelligence Organisation's financial position as at 30 June 2007 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
18 September 2007

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2007 are based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.

Paul O'Sullivan
Director-General of Security

19 September 2007

INCOME STATEMENT – FOR THE PERIOD ENDED 30 JUNE 2007

	Notes	2007 $'000	2006 $'000
INCOME			
Revenue			
Revenue from Government	3A	**227,617**	174,845
Sale of goods and rendering of services	3B	**4,040**	3,224
Total Revenue		**231,657**	178,069
Gains			
Reversals of previous asset write-downs	3C	**281**	–
Other gains	3D	**2,826**	3,030
Total Gains		**3,107**	3,030
Total Income		**234,764**	181,099
EXPENSES			
Employee benefits	4A	**112,828**	91,430
Suppliers	4B	**79,970**	62,965
Depreciation and amortisation	4C	**36,029**	14,370
Finance costs	4D	**96**	6
Write-down and impairment of assets	4E	**2,437**	424
Net losses from sale of assets	4F	**49**	70
Total Expenses		**231,409**	169,265
Surplus (Deficit)		**3,355**	11,834

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

BALANCE SHEET – AS AT 30 JUNE 2007

	Notes	2007 $'000	2006 $'000
ASSETS			
Financial Assets			
Cash and cash equivalents	5A	**16,314**	12,742
Trade and other receivables	5B	**85,904**	40,738
Other financial assets	5C	**1,801**	165
Total financial assets		**104,019**	53,645
Non-Financial Assets			
Land and buildings	6A,C	**48,457**	24,643
Infrastructure, plant and equipment	6B,C	**90,000**	46,099
Intangibles	6D,E	**15,157**	8,708
Other non-financial assets	6F	**10,560**	1,336
Total non-financial assets		**164,174**	80,786
Total Assets		**268,193**	134,431
LIABILITIES			
Payables			
Suppliers	7A	**15,994**	6,000
Other payables	7B	**2,578**	3,481
Total payables		**18,572**	9,481
Interest Bearing Liabilities			
Lease incentives	8	**3,164**	1,313
Total interest bearing liabilities		**3,164**	1,313
Provisions			
Employee provisions	9A	**26,028**	21,649
Other provisions	9B	**4,671**	2,518
Total provisions		**30,699**	24,167
Total Liabilities		**52,435**	34,961
Net Assets		**215,758**	99,470
EQUITY			
Contributed equity		**195,309**	82,323
Reserves		**8,894**	8,947
Retained surplus or (accumulated deficit)		**11,555**	8,200
Total Equity		**215,758**	99,470
Current assets		**114,579**	54,981
Non-current assets		**153,614**	79,450
Current liabilities		**40,311**	27,814
Non-current liabilities		**12,124**	7,147

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

STATEMENT OF CHANGES IN EQUITY – AS AT 30 JUNE 2007

	Retained Earnings		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2007 $'000	2006 $'000	**2007 $'000**	2006 $'000	**2007 $'000**	2006 $'000	**2007 $'000**	2006 $'000
Opening Balance	**8,200**	(3,635)	**8,947**	9,436	**82,323**	56,714	**99,470**	62,515
Surplus (Deficit) for the period	**3,355**	11,834	**–**	–	–	–	**3,355**	11,834
Net revaluation increments/(decrements)	**–**	–	**(53)**	(489)	–	–	**(53)**	(489)
Transactions with Owners								
Contributions by Owners								
Appropriation (equity injection)	–	–	–	–	**112,986**	25,609	**112,986**	25,609
Closing Balance at 30 June	**11,555**	8,200	**8,894**	8,947	**195,309**	82,323	**215,758**	99,470

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

CASH FLOW STATEMENT – FOR THE PERIOD ENDED 30 JUNE 2007

	Notes	2007 $'000	2006 $'000
OPERATING ACTIVITIES			
Cash received			
Goods and services		**5,141**	2,631
Appropriations		**195,933**	151,913
Other gains		**2,523**	2,232
Net GST received		**12,169**	7,237
Total cash received		**215,766**	164,013
Cash used			
Employees		**108,449**	87,055
Suppliers		**94,364**	65,235
Total cash used		**202,813**	152,290
Net cash from or (used by) operating activities	10	**12,953**	11,723
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		**419**	611
Total cash received		**419**	611
Cash used			
Purchase of property, plant and equipment		**100,289**	29,054
Purchase of intangibles		**12,578**	1,399
Total cash used		**112,867**	30,453
Net cash from or (used by) investing activities		**(112,448)**	(29,842)
FINANCING ACTIVITIES			
Cash received			
Appropriations–contributed equity		**103,067**	12,562
Total cash received		**103,067**	12,562
Net cash from or (used by) financing activities		**103,067**	12,562
Net increase or (decrease) in cash held		**3,572**	(5,557)
Cash at the beginning of the reporting period		**12,742**	18,299
Cash at the end of the reporting period	5A	**16,314**	12,742

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

SCHEDULE OF COMMITMENTS – AS AT 30 JUNE 2007

	Notes	2007 $'000	2006 $'000
BY TYPE			
Capital commitments			
Infrastructure, plant and equipment	A	**4,316**	9,291
Total capital commitments		**4,316**	9,291
Other commitments			
Operating leases	B	**155,406**	85,603
Other commitments		**23,783**	14,044
Total other commitments		**179,189**	99,647
Commitments receivable		**18,150**	12,738
Net commitments by type		**165,355**	96,200
BY MATURITY			
Capital commitments			
One year or less		**4,316**	9,291
Total capital commitments		**4,316**	9,291
Operating lease commitments			
One year or less		**15,584**	10,071
From one to five years		**66,628**	50,834
Over five years		**73,194**	24,698
Total operating lease commitments		**155,406**	85,603
Other commitments			
One year or less		**23,783**	14,044
Total other commitments		**23,783**	14,044
Commitments Receivable		**18,150**	12,738
Net commitments by maturity		**165,355**	96,200

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; and - 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 2007

Contingent assets	Claims for damages or costs		Total	
	2007	2006	**2007**	2006
	$ '000	$ '000	**$ '000**	$ '000
Balance from previous period	**–**	–	**–**	–
Re-measurement	**–**	–	**–**	–
Total Contingent Assets	**–**	–	**–**	–
Contingent liabilities	**Claims for damages or costs**		**Total**	
	2007	2006	**2007**	2006
	$ '000	$ '000	**$ '000**	$ '000
Balance from previous period	**100**	200	**100**	200
Re-measurement	**(100)**	(100)	**(100)**	(100)
Total Contingent Liabilities	**–**	100	**–**	100
Net Contingent Liabilities	**–**	100	**–**	100

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 11: 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 2007

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 and notes are required by section 49 of Schedule 1 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 *Finance Minister's Orders (FMOs) for reporting periods ending on or after 1 July 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 (FMOs) for reporting periods ending on or after 1 July 2006; and
- Australian Accounting Standards and Interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial report has been prepared on an accrual basis and is 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 otherwise specified.

Unless an alternative treatment is specifically required by an accounting standard or the FMOs, assets and liabilities are recognised in the Balance Sheet when, and only when, it is probable that future economic benefits will flow to ASIO 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 11).

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

Australian Accounting Standards require a statement of compliance with International Financial Reporting Standards (IFRSs) to be made where the financial report complies with these standards. Some Australian equivalents to IFRSs and other Australian Accounting Standards contain requirements specific to not-for-profit entities that are inconsistent with IFRS requirements. ASIO is a not-for-profit entity and has applied these requirements, so while this financial report complies with Australian Accounting Standards including Australian Equivalents to International Financial Reporting Standards (AEIFRSs) it cannot make this statement.

Adoption of new Australian Accounting Standard Requirements

No accounting standard has been adopted earlier than the effective date in the current period.

Other effective requirement changes

The following amendments, revised standards or interpretations have become effective but have had no financial impact or do not apply to the operations of ASIO.

Amendments:

- 2005-1 Amendments to Australian Accounting Standards [AASBs 1, 101, 124]
- 2005-6 Amendments to Australian Accounting Standards [AASB 3]
- 2006-1 Amendments to Australian Accounting Standards [AASB 121]
- 2006-3 Amendments to Australian Accounting Standards [AASB 1045]

Interpretations:

- UIG 4 Determining whether an Arrangement contains a Lease
- UIG 5 Rights to Interests arising from Decommissioning, Restoration and Environmental Rehabilitation Funds
- UIG 7 Applying the Restatement Approach under AASB 129 Financial Reporting in Hyperinflationary Economies
- UIG 8 Scope of AASB 2
- UIG 9 Reassessment of Embedded Derivatives

UIG 4 and UIG 9 might have impacts in future periods, subject to existing contracts being renegotiated.

Future Australian Accounting Standard requirements

The following new standards, amendments to standards or interpretations have been issued by the Australian Accounting Standards Board but are effective for future reporting periods. It is estimated that the impact of adopting these pronouncements when effective will have no material financial impact on future reporting periods.

Financial instrument disclosure

AASB 7 Financial Instruments: Disclosure is effective for reporting periods beginning on or after 1 January 2007 (the 2007-08 financial year) and amends the disclosure requirements for financial instruments. In general AASB 7 requires greater disclosure than that presently. Associated with the introduction of AASB 7 a number of accounting standards were amended to reference the new standard or remove the present disclosure requirements through 2005-10 Amendments to Australian Accounting Standards [AASB 132, AASB 101, AASB 114, AASB 117, AASB 133, AASB 139, AASB 1, AASB 4, AASB 1023 & AASB 1038]. These changes have no financial impact but will effect the disclosure presented in future financial reports.

Other

The following standards and interpretations have been issued but are not applicable to the operations of ASIO.

- AASB 1049 Financial Reporting of General Government Sectors by Governments
- UIG 10 Interim Financial Reporting and Impairment

1.5 Revenue

Revenue 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 types of 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.

1.6 Gains

Resources Received Free of Charge

Resources 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 another government agency as a consequence of a restructuring of administrative arrangements.

Resources received free of charge are recorded as either revenue or gains depending on their nature, ie. whether they have been generated in the course of the ordinary activities of ASIO.

Sale of Assets

Gains 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 formal reductions) are recognised directly in Contributed Equity in that year.

1.8 Employee Benefits

Liabilities for services rendered by employees are recognised at the reporting date to the extent that they have not been settled.

Liabilities for '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 the work of an actuary as at 30 June 2007. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

Separation and Redundancy

Provision is made for separation and redundancy benefit payments. ASIO recognises a provision for termination when it has developed a detailed formal plan for the terminations and has informed those employees affected that it will carry out the terminations.

Superannuation

Staff of ASIO are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS), the PSS accumulation plan (PSSap) or other complying superannuation funds.

The CSS and PSS are defined benefit schemes for the Australian Government. 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 employee superannuation scheme at rates determined by an actuary to be sufficient to meet the cost to the Government of the superannuation entitlements of the Agency's employees. ASIO accounts for the contributions as if they were contributions to defined contribution plans.

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

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.

1.14 Impairment of Financial Assets

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 is measured as the difference between the asset's carrying amount and the present value 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 the Income Statement.

Financial Assets held at Cost

If there is objective evidence that an impairment loss has been incurred on an unquoted equity instrument that is not carried at fair value because it cannot be reliably measured, or a derivative asset that is linked to and must be settled by delivery of such an unquoted equity instrument, the amount of the impairment loss is the difference between the carrying amount of the asset and the present value of the estimated future cash flows discounted at the current market rate for similar assets.

1.15 Supplier and other Payables

Supplier and other payables are recognised at amortised cost. Liabilities are recognised to the extent that the goods or services have been received (and 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 reported 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. Contingent assets are reported when settlement is probable, and contingent liabilities are recognised when settlement is greater than remote.

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

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

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, property, plant and equipment are carried at fair value less accumulated depreciation and accumulated impairment losses. 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. 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 surplus and deficit. Revaluation decrements for a class of assets are recognised directly through the operating result 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:

	2007	2006
Buildings on freehold land	**25-40 years**	25-40 years
Leasehold improvements	**Lease term**	Lease term
Plant and equipment	**2-20 years**	3-15 years

Impairment

All assets were assessed for impairment at 30 June 2007. 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.

1.19 Intangibles

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

Software is amortised on a straight-line basis over its anticipated useful life. The useful lives of ASIO's software is 3 years (2005-06: 3 to 4 years).

All software assets were assessed for indications of impairment as at 30 June 2007.

1.20 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.

NOTE 2: EVENTS AFTER THE BALANCE SHEET DATE

There were no events occurring after reporting date which had an effect on the 2007 financial statements.

	2007 $'000	2006 $'000
Note 3: Income		
Revenue		
Note 3A: Revenue from Government		
Appropriation–Departmental outputs	**227,617**	174,845
Total revenue from Government	**227,617**	174,845
Note 3B: Sale of goods and rendering of services		
Provision of goods–related entities	**25**	6
Provision of goods–external entities	**67**	8
Total sale of goods	**92**	14
Rendering of services to:		
Rendering of services–related entities	**3,704**	2,997
Rendering of services–external entities	**244**	213
Total rendering of services	**3,948**	3,210
Total sale of goods and rendering of services	**4,040**	3,224
Gains		
Note 3C: Reversals of previous asset write-downs		
Assets revaluation increment	**281**	–
Total reversals of previous asset write-downs	**281**	–
Note 3D: Other gains		
Resources received free of charge	**1,459**	1,168
Rent	**867**	1,273
Miscellaneous	**500**	589
Total other gains	**2,826**	3,030

	2007 $'000	2006 $'000
Note 4: Expenses		
Note 4A: Employee benefits		
Wages and salaries	**83,216**	66,459
Superannuation	**16,052**	11,970
Leave and other entitlements	**3,461**	3,676
Separation and redundancies	**89**	739
Other employee benefits	**10,010**	8,586
Total employee benefits	**112,828**	91,430
Note 4B: Suppliers		
Provision of goods–related entities	**364**	1,003
Provision of goods–external entities	**16,326**	6,022
Rendering of services–related entities	**21,722**	15,681
Rendering of services–external entities	**29,794**	30,539
Operating lease rentals:		
Minimum lease payments	**11,201**	9,128
Workers' compensation premiums	**563**	592
Total supplier expenses	**79,970**	62,965
Note 4C: Depreciation and amortisation		
Depreciation		
Infrastructure, plant and equipment	**22,230**	8,098
Buildings	**7,671**	4,508
Total depreciation	**29,901**	12,606
Amortisation		
Intangibles–Computer Software	**6,128**	1,764
Total depreciation and amortisation	**36,029**	14,370

Depreciation expenses are higher as useful lives were reviewed and adjusted down to reflect appropriate asset life cycles.

	2007 $'000	2006 $'000
Note 4D: Finance Costs		
Interest	**1**	–
Unwinding of discount	**95**	6
	96	6
Note 4E: Write down and impairment of assets		
Financial assets		
- Bad and doubtful debts expense	**1**	–
- Foreign exchange variations	**3**	(3)
Non-financial assets		
- Plant and equipment written off at stocktake	**1,577**	–
- Plant and equipment written off	**807**	146
- Plant and equipment –revaluation decrement	–	281
- Intangibles written off	**49**	–
Total write-down and impairment of assets	**2,437**	424
Note 4F: Losses from asset sales		
Infrastructure, plant and equipment		
Proceeds from sale	**(419)**	(611)
Carrying value of assets sold	**468**	681
Total losses from asset sales	**49**	70

Note 5: Financial Assets

Note 5A: Cash and cash equivalents		
Cash on hand or deposit	**16,314**	12,742
Total cash and cash equivalents	**16,314**	12,742

	2007 $'000	2006 $'000
Note 5B: Trade and other receivables		
Goods and services	**1,737**	3,653
Appropriations Receivable:		
- for existing outputs	**77,582**	35,979
GST receivable from the Australian Taxation Office	**6,585**	1,106
Total trade and other receivables (gross)	**85,904**	40,738
Less allowance for doubtful debts:		
Goods and services	**–**	–
Total trade and other receivables (net)	**85,904**	40,738
Receivables are aged as follows:		
Not overdue	**84,689**	39,158
Overdue by:		
Less than 30 days	**461**	1,207
30 to 60 days	**55**	277
61 to 90 days	**32**	18
More than 90 days	**667**	78
Total receivables (gross)	**85,904**	40,738
Receivables are represented by:		
Current	**85,904**	40,738
Non-current	**–**	–
Total trade and other receivables (net)	**85,904**	40,738
Note 5C: Other Financial Assets		
Accrued Revenue	**1,801**	165

Note 6: Non-Financial Assets

Note 6A: Land and buildings		
Freehold land		
-fair value	**1,730**	1,575
Total freehold land	**1,730**	1,575

	2007 $'000	2006 $'000
Buildings on freehold land		
-fair value	**3,212**	1,950
-accumulated depreciation	**–**	–
Total buildings on freehold land	**3,212**	1,950
Leasehold improvements		
-fair value	**45,226**	22,150
-accumulated depreciation	**(1,711)**	(1,032)
Total leasehold improvements	**43,515**	21,118
Total land and buildings (non-current)	**48,457**	24,643
Note 6B: Infrastructure, plant and equipment		
Infrastructure, plant and equipment		
- work in progress	**2,815**	7,825
- fair value	**90,370**	38,274
- accumulated depreciation	**(3,185)**	–
Total Infrastructure, Plant and Equipment (non-current)	**90,000**	46,099
All revaluations are conducted in accordance with the revaluation policy stated in Note 1. In 2006-07, 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 section of the balance sheet:		
Land, buildings and leasehold improvements	**(837)**	(558)
Plant & equipment	**784**	69
	(53)	(489)

Note 6C: Analysis of Property, Plant and Equipment

TABLE A–Reconciliation of the opening and closing balances of property, plant and equipment (2006-07)

	Land	Buildings	Buildings-Leasehold Improvement	Total Land & Buildings	Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000	$'000
As at 1 July 2006						
Gross book value	1,575	1,950	22,150	25,675	46,099	71,774
Accumulated depreciation / amortisation and impairment	–	–	(1,032)	(1,032)	–	(1,032)
Net book value 1 July 2006	1,575	1,950	21,118	24,643	46,099	70,742
Additions:						
by purchase	–	1,295	30,452	31,747	67,933	99,680
Revaluations and impairments through equity	155	60	(370)	(155)	1,065	910
Depreciation / amortisation expense	–	(93)	(7,578)	(7,671)	(22,231)	(29,902)
Disposals:						
Other disposals	–	–	(107)	(107)	(2,866)	(2,973)
Net book value 30 June 2007	**1,730**	**3,212**	**43,515**	**48,457**	**90,000**	**138,457**
Net book value as of 30 June 2007 represented by:						
Gross book value	1,730	3,212	45,226	50,168	93,185	143,353
Accumulated depreciation / amortisation and impairment	–	–	(1,711)	(1,711)	(3,185)	(4,896)
	1,730	**3,212**	**43,515**	**48,457**	**90,000**	**138,457**

TABLE B–Reconciliation of the opening and closing balances of property, plant and equipment (2005-06)

	Land	Buildings	Buildings-Leasehold Improvement	Total Land & Buildings	Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000	$'000
As at 1 July 2005						
Gross book value	1,500	2,019	22,487	26,006	35,317	**61,323**
Accumulated depreciation / amortisation and impairment	–	–	(706)	(706)	(227)	**(933)**
Net book value 1 July 2006	1,500	2,019	21,781	25,300	35,090	**60,390**
Additions:						
by purchase	–	–	4,410	4,410	19,872	**24,282**
Revaluations and impairments through equity	75	9	(642)	(558)	65	**(493)**
Depreciation/ amortisation expense	–	(78)	(4,430)	(4,508)	(8,097)	**(12,605)**
Disposals:						
other disposals	–	–	–	–	(831)	**(831)**
Net book value 30 June 2006	**1,575**	**1,950**	**21,118**	**24,643**	**46,099**	**70,742**
Net book value as of 30 June 2006 represented by:						
Gross book value	1,575	1,950	22,150	25,675	46,099	**71,774**
Accumulated depreciation / amortisation and impairment	–	–	(1,032)	(1,032)	–	**(1,032)**
	1,575	**1,950**	**21,118**	**24,643**	**46,099**	**70,742**

	2007 $'000	2006 $'000
Note 6D: Intangibles		
Computer Software		
Purchased–at cost	**9,779**	10,320
Internally developed–in progress	**2,910**	5,345
Internally developed–in use	**14,170**	–
Total Computer Software	**26,859**	15,665
Accumulated amortisation	**(11,702)**	(6,957)
Total intangibles (non-current)	**15,157**	8,708

No indicators of impairment were found for intangible assets.

Note 6E: Intangibles

TABLE A–Reconciliation of the opening and closing balances of intangibles (2006-07)

	Computer software internally developed	Computer software purchased	Total
	$'000	$'000	$'000
As at 1 July 2006			
Gross book value	5,345	10,320	**15,665**
Accumulated depreciation / amortisation and impairment*	–	(6,957)	**(6,957)**
Net book value 1 July 2006	5,345	3,363	**8,708**
Additions:			
by purchase or internally developed	11,735	890	**12,625**
Amortisation expense	(3,327)	(2,801)	**(6,128)**
Disposals:			
Other disposals	–	(49)	**(49)**
Net book value 30 June 2007	**13,753**	**1,403**	**15,156**
Net book value as of 30 June 2007 represented by:			
Gross book value	17,080	9,779	**26,859**
Accumulated depreciation / amortisation and impairment	(3,327)	(8,375)	**(11,702)**
	13,753	**1,404**	**15,157**

TABLE B–Reconciliation of the opening and closing balances of intangibles (2005-06)

	Computer software internally developed	Computer software purchased	Total
	$'000	$'000	$'000
As at 1 July 2005			
Gross book value	3,004	8,934	**11,938**
Accumulated depreciation / amortisation and impairment	(285)	(5,689)	**(5,974)**
Net book value 1 July 2005	2,719	3,245	**5,964**
Additions:			
by purchase or internally developed	3,109	1,401	**4,510**
Amortisation expense	(483)	(1,281)	**(1,764)**
Disposals:			
other disposals	–	(2)	**(2)**
Net book value 30 June 2006	**5,345**	**3,363**	**8,708**
Net book value as of 30 June 2006 represented by:			
Gross book value	5,345	10,320	**15,665**
Accumulated depreciation / amortisation and impairment	–	(6,957)	**(6,957)**
	5,345	**3,363**	**8,708**

	2007 $'000	2006 $'000
Note 6F: Other non-financial assets		
Prepayments	**10,560**	1,336
All other non-financial assets are current assets.		
No indicators of impairment were found for other non-financial assets.		

Note 7: Payables

Note 7A: Suppliers		
Trade Creditors	**15,994**	6,000
Total supplier payables	**15,994**	6,000
Supplier payables are represented by:		
Current	**15,994**	6,000
Non-Current	**–**	–
Total supplier payables	**15,994**	6,000
Settlement is usually made net 30 days.		
Note 7B: Other Payables		
Accrued expenses	**2,578**	3,481
Total other payables	**2,578**	3,481
All other payables are current liabilities		

Note 8: Interest bearing liabilities

Lease incentives	**3,164**	1,313
Total interest bearing liabilities	**3,164**	1,313
Lease incentives are represented by:		
Current	**676**	657
Non-current	**2,488**	656
Total interest bearing provisions	**3,164**	1,313

	2007 $'000	2006 $'000
Note 9: Provisions		
Note 9A: Employee provisions		
Salaries and wages	**1,209**	995
Leave	**24,404**	20,288
Superannuation	**130**	108
Other	**285**	258
Total employee provisions	**26,028**	21,649
Employee provisions are represented by:		
Current	**21,063**	17,516
Non-current	**4,965**	4,133
Total employee provisions	**26,028**	21,649

The classification of current includes amounts for which there is not an unconditional right to defer settlement by one year, hence in the case of employee provisions the above classification does not represent the amount expected to be settled within one year of reporting date. Employee provisions expected to be settled in twelve months from the reporting date is $16,281,068 (2006: $13,841,013), in excess of one year $9,746,957 (2006: $7,807,304).

Note 9B: Other provisions		
Restoration obligations	**4,671**	2,518
Total other provisions	**4,671**	2,518
Other provisions are represented by:		
Current	**4**	160
Non-current	**4,667**	2,358
Total other provisions	**4,671**	2,518
Carrying amount 1 July 2006	**2,518**	
Additional provisions made	**1,303**	
Lease expiry	**(107)**	
Revaluations	**862**	
Unwinding of discount or change in discount rate	**95**	
Closing balance	**4,671**	

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.

	2007 $'000	2006 $'000
Note 10: Cash flow reconciliation		
Reconciliation of cash and cash equivalents per Balance Sheet to Cash Flow Statement		
Report cash and cash equivalents as per:		
Cash Flow Statement	**16,314**	12,742
Balance Sheet	**16,314**	12,742
Reconciliation of operating result to net cash from operating activities:		
Operating result	**3,355**	11,834
Depreciation/amortisation	**36,029**	14,370
Net write down of non-financial assets	**2,152**	427
Net loss on disposal of assets	**49**	70
Lease make good	**–**	1,390
(Increase)/Decrease in receivables	**(35,247)**	(23,974)
(Increase)/Decrease in accrued revenue	**(1,636)**	(165)
(Increase)/Decrease in prepayments	**(9,223)**	(37)
Increase/(Decrease) in employee provisions	**4,379**	4,375
Increase/(Decrease) in provision for make good	**2,153**	(2)
Increase/(Decrease) in interest bearing liabilities	**1,851**	459
Increase/(Decrease) in supplier payables	**9,994**	2,518
Increase/(Decrease) in accrued expenses	**(903)**	458
Net cash from/(used by) operating activities	**12,953**	11,723

Note 11: Contingent Liabilities and Assets

Unquantifiable contingencies

At 30 June 2007, 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.

	2007 $'000	2006 $'000

Note 12: Executive Remuneration

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

	2007	2006
$130 000 to $144 999	–	2
$145 000 to $159 999	–	4
$160 000 to $174 999	–	1
$175 000 to $189 999	1	6
$190 000 to $204 999	6	2
$205 000 to $219 999	6	5
$220 000 to $234 999	6	4
$235 000 to $249 999	3	1
$250 000 to $264 999	2	1
$265 000 to $279 999	1	3
$280 000 to $294 999	6	–
$295 000 to $309 999	2	1
$310 000 to $324 999	1	–
$325 000 to $339 999	–	1
$340 000 to $354 999	1	–
$355 000 to $369 999	1	–
$385 000 to $399 999	–	1
$400 000 to $414 999	1	–
	37	32

The aggregate amount of total remuneration of executive officers shown above.	**$9,287,036**	$6,869,799
The aggregate amount of separation and redundancy/termination benefit payments during the year to executives shown above.	**$115,204**	nil

Note 13: Remuneration of Auditors

	2007	2006
Financial statement audit services are provided free of charge to ASIO.		
The fair value of audit services provided was:		
Australian National Audit Office (ANAO)	**$86,900**	$69,500

No other services were provided by the Auditor-General.

Note 14: Staffing Levels

	2007	2006
Total Full Time Equivalent staffing levels for ASIO at the end of the year were:	**1246**	1062

Note 15: Financial Instruments

Note 15A: Interest Rate Risk

Financial Instrument	Note	Non-Interest Bearing		Total		Weighted Average Effective Interest Rate	
		2007	2006	**2007**	2006	**2007**	2006
		$'000	$'000	**$'000**	$'000	**%**	%
Financial Assets							
Cash and cash equivalents	5A	**16,314**	12,742	**16,314**	12,742	**–**	–
Receivables for goods and services (gross)	5B	**1,737**	3,653	**1,737**	3,653	**n/a**	n/a
Total		**18,051**	16,395	**18,051**	16,395		
Total Assets				**268,193**	134,431		
Financial Liabilities							
Trade creditors	7A	**15,994**	6,000	**15,994**	6,000	**n/a**	n/a
Total		**15,994**	6,000	**15,994**	6,000		
Total Liabilities				**52,435**	34,961		

Note 15B: Fair Values of Financial Assets and Liabilities

All financial assets and liabilities are carried at fair value.

Note 15C: 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 16: Appropriations

Note 16A: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriation

	2007	2006
Balance carried from previous period	**30,704,793**	13,128,617
Correction in prior year error in disclosure	**–**	822,138
Adjusted balance carried forward	**30,704,793**	13,950,755
Appropriation Act:		
Appropriation Act (No.1)	**227,617,000**	171,727,000
Appropriation Act (No.3)	**–**	3,118,000
FMA Act:		
Refunds credited (FMA s30)	**1,156,061**	370,499
Appropriations to take account of recoverable GST (FMA s30A)	**7,188,124**	5,981,173
Annotations to 'net appropriations' (FMA s31)	**6,928,402**	5,104,696
Total appropriations available for payments	**273,594,380**	200,252,123
Cash payments made during the year (GST inclusive)	**202,663,767**	169,547,330
Balance of Authority to draw cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriations	**70,930,613**	30,704,793
Represented by:		
Cash at bank and on hand	**16,313,613**	7,772,139
Receivables–departmental appropriations	**54,617,000**	22,932,654
Total	**70,930,613**	30,704,793

Note 16B: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriation

	2007	2006
Balance carried from previous year	**18,015,015**	5,171,091
Appropriation Act:		
Appropriation Act (No.2)	**112,986,000**	14,201,000
Appropriation Act (No.4)	**–**	11,408,000
FMA Act:		
Appropriations to take account of recoverable GST (FMA s30A)	**4,980,256**	1,256,242
Total appropriations available for payments	**135,981,271**	32,036,333
Cash payments made during the year (GST inclusive)	**113,016,000**	14,021,318
Balance of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriations	**22,965,271**	18,015,015
Represented by:		
Cash at bank and on hand	**–**	4,968,438
Appropriation Receivable	**22,965,271**	13,046,577
Total	**22,965,271**	18,015,015

Note 17: Special Accounts

ASIO has an Other Trust Monies Special Account and a Services for Other Government & Non-Agency Bodies Account. These accounts were established under section 20 of the *Financial Management and Accountability Act 1997* (FMA Act). For the years ended 30 June 2007 and 30 June 2006, both special accounts had nil balances and there were no transactions debited or credited to them. For the periods 2005-06 and 2006-07 ASIO has not used section 39 of the FMA Act regarding investments in respect of these Special Accounts.

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

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

Note 18: Compensation and Debt Relief

	2007	2006
No payments were made during the reporting period under the 'Defective Administration Scheme'. (2006:Eleven payments made).	Nil	$114,623

Note 19: Reporting of Outcomes

Note 19A: Net Cost of Outcome Delivery

	2007	2006
	$'000	$'000
Expenses		
Departmental	231,409	169,265
Costs recovered from provision of goods and services to the non-government sector		
Departmental	811	810
Other external revenues		
Departmental	4,596	4,276
Net cost / (contribution) of outcome	226,002	164,179

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

PART 5: APPENDICES

APPENDIX A
PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

The Parliamentary Joint Committee on Intelligence and Security 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 Committee during 2006–07 is shown in Table 9.

Member	
The Hon David Jull MP (Chair)	Liberal Party, QLD
Mr Anthony Byrne MP (Deputy Chair)	Australian Labor Party, VIC
Senator the Hon Alan Ferguson	Liberal Party, SA
Senator the Hon Robert Ray	Australian Labor Party, VIC
Senator the Hon John Faulkner	Australian Labor Party, NSW
Senator Fiona Nash	National Party, NSW
Mr Stewart McArthur MP	Liberal Party, VIC
The Hon Duncan Kerr SC MP	Australian Labor Party, TAS
Mr Steven Ciobo MP	Liberal Party, QLD

Table 9: Members of the Parliamentary Joint Committee on Intelligence and Security

APPENDIX B
CRITICAL INFRASTRUCTURE CATEGORIES AND SECTORS

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 10: National Criticality Categories

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

Table 11: 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)	35	9	0	0	0	34
Senior Officers[6]	305	100	33	0	4	283
AO5[7]	388	187	74	2	3	379
AO1–4[8]	538	303	78	1	7	496
ITO1–2[9]	87	18	17	1	1	83
ENG1–2[10]	3	0	0	0	0	3
Total	1 356	617	202	4	15	1 278

Table 12: Representation of designated groups within ASIO at 30 June 2007

[1] Based on staff salary classifications recorded in ASIO's human resource 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 5 translates to APS Level 6.
[8] Translates to span the APS 1 to 5 classification levels.
[9] Information Technology Officers Grades 1 and 2.
[10] Engineers Grades 1 and 2.

Group	June 2003	June 2004	June 2005	June 2006	June 2007
Women[1]	42.00	41.00	43.14	45.86	45.50
Race/Ethnicity[2]	12.00	11.00	14.64	16.16	15.81
ATSI[3]	0.74	0.41	0.45	0.38	0.31
PWD[4]	4.00	2.00	1.59	1.36	1.17
Total	58.74	54.41	59.82	63.76	62.79

Table 13: Percentage representation of designated groups in ASIO 2003 to 2007

[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.
[3] Aboriginal and Torres Strait Islander.
[4] People with a disability.

APPENDIX C CONTINUED
WORKFORCE STATISTICS

	2003–04	2004–05	2005–06	2006–07
Ongoing full-time	603	693	800	1 125
Non-ongoing full-time[1]	103	155	178	55
Ongoing part-time	38	43	50	94
Non-ongoing part-time	28	22	27	18
Non-ongoing casual	33	42	55	64
Total	805	955	1 110	1 356

Table 14: Composition of workforce 2003–04 to 2006–07

[1] Includes secondees and locally engaged staff and contractors/consultants held against positions in the structure.

		2003–04	2004–05	2005–06	2006–07
Band 1	Female	2	4	5	7
	Male	9	10	17	17
Band 2	Female	1	1	1	2
	Male	4	4	4	8
Band 3	Female	0	0	0	0
	Male	1	1	1	1
Total		17	20	28	35

Table 15: SES equivalent staff classification and gender 2003–04 to 2006–07 (does not include the Director-General)

APPENDIX D
ASIO SALARY CLASSIFICATION STRUCTURE AT 30 JUNE 2007

ASIO MANAGERS			
SES Band 3	$177 313		minimum point
SES Band 2	$140 149		minimum point
SES Band 1	$117 546		minimum point
AEO 3	$102 136		
AEO 2	$92 656	to	$102 136
AEO 1	$81 702	to	$88 191

INTELLIGENCE OFFICERS			
IO	$62 386	to	$71 159

ASIO OFFICERS			
ASIO Officer 5	$62 386	to	$71 159
ASIO Officer 4	$51 453	to	$56 166
ASIO Officer 3	$44 869	to	$48 347
ASIO Officer 2	$39 513	to	$43 708
ASIO Officer 1	$35 022	to	$38 607

ASIO ITOs			
SITOA	$102 136		
SITOB	$92 656	to	$102 136
SITOC	$81 702	to	$88 191
ITO2	$62 386	to	$71 159
ITO1	$48 347	to	$56 166

ASIO ENGINEERS			
SIO(E)5	$103 758		
SIO(E)4	$92 656	to	$102 136
SIO(E)3	$81 702	to	$88 191
SIO(E)2	$62 386	to	$71 159
SIO(E)1	$48 347	to	$56 166

Table 16: ASIO salary classification structure at 30 June 2007

APPENDIX E
MANDATORY REPORTING REQUIREMENTS UNDER SECTION 94 OF THE ASIO ACT

94(1A)(a)	the total number of requests made under Division 3 of Part III to issuing authorities during the year for the issue of warrants under that Division	Nil
94(1A)(b)	the total number of warrants issued during the year under that Division	Nil
94(1A)(c)	the total number of warrants issued during the year under section 34E	Nil
94(1A)(d)	the number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year under section 34E and the total of all those hours for all those persons	Nil
94(1A)(e)	the total number of warrants issued during the year under section 34G	Nil
94(A)(f)(i)	the number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year under section 34G	Nil
94(A)(f)(ii)	the number of hours each person spent in detention under such a warrant	Nil
94(A)(f)(iii)	the total of all those hours for all those persons	Nil
94(1A)(g)	the number of times each prescribed authority had persons appear for questioning before him or her under warrants issued during the year	Nil

Table 17: Mandatory reporting requirements under section 94 of the *Australian Security Intelligence Organisation Act 1979*

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACS	Australian Customs Service
AFP	Australian Federal Police
AIC	Australian Intelligence Community
ANSTO	Australian Nuclear Science and Technology Organisation
APEC	Asia-Pacific Economic Cooperation
ASIO	Australian Security Intelligence Organisation
ASIC	Aviation Security Identity Card
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
BLU	Business Liaison Unit
CBR	Chemical Biological and Radiological
CBRNE	Chemical Biological Radiological Nuclear and Explosives
C/CSP	Carrier/Carriage Service Provider
CHOGM	Commonwealth Heads of Government Meeting
CTITP	Counter-Terrorism Intelligence Training Program
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DIO	Defence Intelligence Organisation
DoFA	Department of Finance and Administration
DOTARS	Department of Transport and Regional Services
DSD	Defence Signals Directorate
FADG	First Assistant Director-General
IASF	Inter-Agency Security Forum
IGIS	Inspector-General of Intelligence and Security
MAL	Movement Alert List
MSIC	Maritime Security Identity Card
NAA	National Archives of Australia
NCTC	National Counter-Terrorism Committee
NCTP	National Counter-Terrorism Plan
NII	National Information Infrastructure
NIG	National Intelligence Group
NSC	National Security Committee of Cabinet
NSH	National Security Hotline
NTAC	National Threat Assessment Centre
ONA	Office of National Assessments
PSCC	Protective Security Coordination Centre
PSM	Protective Security Manual
RMU	Research and Monitoring Unit
SCNS	Secretaries' Committee on National Security
SES	Senior Executive Service
TSPV	Top Secret Positive Vetted

COMPLIANCE INDEX

Part of Report	Annual Report requirements	Page
	Letter of transmittal	*iii*
	Table of contents	*v*
	Index	126
	Glossary	123
	Contact officers(s)	Back cover
	Internet home page address and Internet address for report	Back cover
Review by Secretary	Review by departmental secretary (Director-General of Security)	*vii*
Departmental Overview	Organisational structure	9–11
	Role and function	*vii*
	Overview description of department	8
	Outcome and output structure	13
Report on Performance	Review of performance during the year in relation to outputs and contribution to outcomes	17–77
	Performance of purchaser/provider arrangements	N/A
	Narrative discussion and analysis of performance	17–77
	Discussion and analysis of the departments financial performance	14
	Summary resource tables by outcomes	14
	Developments since the end of the financial year that have affected or may significantly affect the department's operations or financial results in future	N/A
Corporate Governance	Statement of the main corporate governance practices in place	70–71
	Agency heads are required to certify that their agency comply with the Commonwealth Fraud Control Guidelines	*iii*
External Scrutiny	Significant developments in external scrutiny	72–74
Management of Human Resources	Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	58–66
	Statistics on staffing	59–60; Appendix C
	Certified agreements and AWAs	N/A
	Performance pay	66

Part of Report	Annual Report requirements	Page
Purchasing	Assessment of purchasing against core policies and principles	66
Consultants	A summary of statements detailing the number of new consultancy services contracts; the total actual expenditure an all new consultancy contracts; the number of ongoing consultancy contracts that were active; and the total actual expenditure on the ongoing consultancy contracts (inclusive of GST).	66
	Statement noting that information on contracts and consultancies is available through the AusTender website.	66
Competitive tendering and Contracting	Absence of provisions in CTC contracts allowing access by the Auditor-General	66
Exempt Contracts	Contracts exempts from the AusTender	66
Commonwealth Disability Strategy	Report on performance in implementing the Commonwealth Disability Strategy	64
Financial Statements	Financial statements	79–114
Other Information	Reporting requirements under section 94 of the ASIO Act	
	Occupational health and safety	65
	Freedom of Information	33
	Advertising and Market Research	58–59
	Ecologically sustainable development and environmental performance	68
	Correction of material errors in previous annual report	34

GENERAL INDEX

A

U

V

W

Y

WRITTEN INQUIRIES

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

GENERAL INQUIRIES

Central Office switchboard

Tel: (02) 6249 6299
1800 020 648 (toll free)

Fax: (02) 6257 4501

MEDIA INQUIRIES

Media Liaison Officer

Tel: (02) 6249 8381

Fax: (02) 6262 9547

STATE AND TERRITORY OFFICE TELEPHONE INQUIRIES

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

WEBSITE

www.asio.gov.au

Visit the ASIO website at: www.asio.gov.au