

# ASIO

---

REPORT TO PARLIAMENT 2007–08

ISSN 0815-4562

© Commonwealth of Australia [2008]

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>



Australian Government

Australian Security  
Intelligence Organisation

Director-General of Security

13 October 2008

eA: 1108549

The Hon Robert McClelland MP  
Attorney-General  
Parliament House  
Canberra ACT 2601

*Dear Minister,*

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 2008. The distribution of that classified Annual Report is limited.

Under the 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 need and that comply with the Guidelines applying in 2007-08.

*James Spittally*  
*Paul O'Sullivan*

Paul O'Sullivan  
Director-General

**ASIO**

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

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



# Contents

Message from the Director-General .....	VII
Key Statistics.....	VIII
Year in Review.....	IX
ASIO’s Role and Functions .....	XII
ASIO’s Funding and Client Satisfaction .....	XIV
Organisational Structure.....	XV
Part 1: Threats to Australia in 2007–08.....	1
Part 2: Output Performance.....	9
Output 1: Security Intelligence Analysis and Advice .....	11
Output 2: Protective Security Advice .....	25
Output 3: Security Intelligence Investigations and Capabilities .....	31
Output 4: Foreign Intelligence Collection .....	41
Part 3: Corporate Management and Accountability – Enabling Functions.....	43
People Development and Management .....	46
Human Resource Policy and Practice.....	49
Financial Services .....	50
Information Services .....	51
Property Management .....	55
Corporate Governance.....	56
Accountability .....	58
Reviews and Inquiries .....	63
Legislative Change .....	64
Security of ASIO .....	65
Part 4: Financial Statements .....	69
Part 5: Appendices .....	119
Compliance Index .....	127
Glossary .....	129
General Index.....	131



The Hon Robert McClelland MP  
Attorney-General



Mr Paul O'Sullivan  
Director-General of Security

## Message from the Director-General

If there has been one defining feature of the security environment in recent years, it has been its increasing complexity. This past year has been no exception.

While terrorism-related threat levels to Australia and its interests – both here and abroad – have remained at elevated levels since 2001, the groups and individuals that impact on the security environment, and the global political and economic landscape in which they operate, have continued to evolve.

ASIO's role, and that of its Australian and international partners, is to make sense of this dynamic and fast-paced environment in order to provide informed, relevant and timely advice to decision-makers and other operational agencies. Our focus must be preventative and forward-looking. We must ensure our collection capability is multi-faceted and agile; that our analytical approach is rigorous and fact-based; and that our advice reaches the right people, when they need it. Our performance in this regard in 2007–08 was strong.

But there can be no let-up.

If not for the action of ASIO and its partners in recent years I believe there would have been a terrorist attack or attacks in Australia. This is a sobering thought. But it underlines – in very clear terms – the seriousness of the threats we face, the importance of the work we do and the criticality of our partnerships.

Much of the capability investment in ASIO in recent years, and in 2007–08 in particular, has bolstered our ability to manage effectively the volume and fragmentary nature of the information we obtain; to keep pace with rapid technological developments; to expand our national and international reach; to enhance the skills of our people; and to ensure we are joined up effectively with partners.

In 2007–08 we improved cooperation and connectivity with Australian partners, including, importantly, with law enforcement on terrorism prosecutions, and with agencies involved in the critical task of border security. We introduced a range of new initiatives in this area, including enhanced briefing and exchange programs. We worked hand-in-hand with the Australian Federal Police (AFP) and the Commonwealth Director of Public Prosecutions to progress the recommendations of the *Street Review of the Interoperability between the AFP and its National Security Partners*. And we worked closely with the Department of Immigration and Citizenship to progress significantly the Next Generation Border Security initiative. These cooperative initiatives are well advanced and have delivered tangible improvements.

While counter-terrorism remains, appropriately, a major priority, it is important to remember that ASIO is not a single issue organisation. In 2007–08 we made a valuable and growing contribution to countering espionage and foreign interference. This trend will continue – both in the demand for reporting and advice, and the increasing sophistication of those involved in such activity. We will continue to build capability to meet growing demands in this area. Countering electronic espionage – a new dimension of an age-old threat – will be resource intensive.

The challenges of the security environment necessitate, and the Government and public expect rightly, that the women and men of ASIO are flexible, responsive, resolute, and forward-looking. In 2007–08 we continued to invest strongly in our staff. And we strengthened further our organisational culture to ensure continued alignment with ASIO's values of excellence, integrity, cooperation and accountability.

And, critically, in 2007–08 we continued to receive the support and assistance of the public, communities and organisations, and industry. Addressing effectively the challenges of our complex security environment requires a sustained and collegiate approach.

This past year has been one of significant progress – as reflected in the Year in Review that follows. We have maintained this momentum into 2008–09.

## Key statistics, 2007–08

- ASIO's workforce grew from 1,356 to 1,492 and its budget was \$304m.
- ASIO provided regular intelligence reporting to at least 75 Commonwealth and State and Territory government customers, compared with around 45 ten years ago. ASIO produced 3,224 intelligence assessment reports, 17% more than 2006–07. This included 2,075 Threat Assessments and other specialised threat product.
- In 2007–08 some 140 security reports were provided to around 400 private-sector subscribers to ASIO's Business Liaison Unit website – a 55% increase on 2006–07.
- For the Asia Pacific Economic Cooperation (APEC) forum series of meetings, ASIO conducted 16,573 individual security checks.
- ASIO provided 72,688 visa security assessments, 36% more than 2006–07. The number of counter-terrorism assessments completed decreased 34% to 82,290. But personnel security assessments increased slightly to 21,386.
- ASIO was involved in more than 60 civil and criminal proceedings – including terrorism prosecutions.
- ASIO certified 57 new Top Secret sites and conducted technical surveillance countermeasures tests to protect government sites from unauthorised monitoring.
- ASIO expanded its program of attached staff. It hosted representatives from 12 Australian departments or agencies and out-posted officers to six of these.
- In response to 530 applications for public access to ASIO records, 63,932 folios (pages) were examined for release, an increase from 52,234 in 2006–07.

Key statistics provide only an indication of the extent and breadth of ASIO's work throughout 2007–08. Many other aspects of ASIO's work during the year are canvassed in detail in other sections of the Annual Report, including the Year in Review section.



## Year in Review, 2007–08

### The security environment

Terrorism – particularly by violent jihadists – has posed the most significant security threat to Australia for at least the last seven years. It will continue to do so for the foreseeable future.

- Tactically the threat is manifest in attacks against civilians as well as governments, while strategically it aims to influence and degrade institutions and principles that are fundamental to Australia's social, economic and security interests.
- Australia and Australians have been specific targets of actual and planned terrorist attacks.

The terrorist threat evolved further in 2007–08. It was linked in large part to the Middle East and South Asia. While core al-Qa'ida retained the capability and intent to target Western interests, its alliances and ideological reach generated new challenges.

- Jihadist groups in places such as the Gulf, the Middle East, and Africa forged alliances with al-Qa'ida.
- And the ideology of violent jihad – often disseminated via the Internet – continued to resonate with a small but potentially dangerous group, some of whom were not known to be connected to al-Qa'ida but who were nonetheless inspired to plan and conduct terrorist acts.

The counter-terrorism outlook for South-East Asia is generally improved, but remains serious. South-East Asia's most wanted terrorist, Noordin Mohammad Top, remains at large.

- Indonesian authorities disrupted a terrorist cell in June 2008 and recovered a number of explosive devices that were reportedly to be used to attack Western targets in Indonesia.

Within Australia, a small but significant minority of the community hold or have held extremist views. An even smaller minority is prepared to act in support of it – including by advocating violence, providing logistical or propaganda support to extremists, or travelling abroad to train with terrorist groups or participate in violent jihad activities. During 2007–08 legal proceedings commenced against a number of individuals charged with related offences.

But there are other threats to Australia's security beyond terrorism. Australia's economic strength, technological development, and strong global partnerships make it a continuing target for espionage and foreign interference. In 2007–08 ASIO continued, therefore, to enhance its counter-espionage and counter-foreign interference efforts.

### Meeting the challenges

This year marked the mid-point of a program – implemented as a result of the 2005 review by Mr Allan Taylor AM of ASIO resourcing – to build capability across ASIO's functions. ASIO's ability to respond to the challenging security environment relies on high quality staff, robust information systems, and an expert assessment base built on ASIO's long experience with security intelligence issues.

ASIO continued to build the capability of its workforce through the recruitment of new staff and ongoing development of existing staff.

- By 30 June 2008 ASIO's workforce had grown to 1,492. Although this was short of target growth for the year, it was ahead of the overall growth target. ASIO remains confident it will achieve its target of 1,860 by 2010–11.
- Innovative, targeted recruitment campaigns attracted high quality applicants who brought a diversity of relevant experience to ASIO.
- ASIO invested \$6.4m in training through its *Learning and Development Strategy* to ensure that staff received high quality – and often specialised – training that enhanced whole-of-Organisation capability.

Development of ASIO's technical collection and analysis capabilities also continued in 2007–08, a particular challenge in an environment of rapid technological change.

- To supplement in-house research and development, ASIO used its partnerships to share the burden of expensive technological development.
- The appointment of the first full-time Science Adviser in 2007–08 was an important milestone for ASIO in its ongoing research and development programs.
- ASIO expanded its complex and advanced analytical capabilities, allowing complex data sorting and exploitation, and providing higher quality information for ASIO's intelligence operations and analysis.

ASIO developed further its domestic liaison partnerships during 2007–08.

- ASIO expanded its officer attachment arrangements with Australian agencies. These attachments enhance agency understanding, cooperation, and information sharing.
- In cooperation with other Australian agencies, ASIO advanced several initiatives to improve service delivery related to border security. These included the first two phases of the Next Generation Border Security initiative.
- ASIO began implementing the recommendations of the *Review of Interoperability between the AFP and its National Security Partners* (the Street Review).

Because most of the security threats facing Australia have significant overseas links, ASIO also bolstered its international partnerships.

- ASIO expanded its network of overseas liaison relationships to 311 agencies in 120 countries.

ASIO's customer base has increased significantly over the past decade and now includes private sector companies and a greater range of international liaison partners. Within Australia, ASIO's intelligence product is distributed to some 75 government customers, including Ministers and other senior decision-makers, and law enforcement, policy, and intelligence agencies at the Commonwealth and State and Territory levels.

During 2007–08 ASIO continued to refine its reporting to meet its customers' needs.

- Reflecting ongoing high demand for threat-related intelligence, the National Threat Assessment Centre published 2,075 reports. It diversified its product range to include monthly snapshots of the threat environment and trend analyses.
- ASIO produced a range of strategic assessments on both specific and thematic issues to assist policy and capability development.
- ASIO continued to enhance its engagement with, and reporting to, business and industry through its Business Liaison Unit and Critical Infrastructure Protection programs. These units continued to provide valuable assistance to businesses, particularly for their risk planning.

Along with other security and law enforcement agencies ASIO helped ensure there were no major incidents during the 2007 Asia-Pacific Economic Cooperation (APEC) meetings, 2007 Federal Election, 2008 Anzac Day Commemorations or 2008 Beijing Olympic Torch Relay.

- ASIO's support to APEC in particular was substantial. It involved most areas of the Organisation.

ASIO's involvement in criminal and civil litigation continued to increase. During 2007–08, ASIO was involved in a range of legal matters including terrorism prosecutions, civil litigation, and review of administrative decisions.

- ASIO created a Legal Division on 1 July 2007, and continued to expand its legal team.

ASIO cooperated closely with several reviews and inquiries in 2007–08, including the *Homeland and Border Security Review* (the Smith Review), the Street Review, and the *Clarke Inquiry into the Case of Dr Mohamed Haneef*. Implementation of Street Review recommendations is already underway and will continue into the next reporting period.

ASIO continued to operate under rigorous internal and external accountability and oversight arrangements. The principle of proportionality was strictly applied to intelligence collection – meaning that capabilities were applied in a measured and graduated manner commensurate with the level of threat.

- ASIO updated its operational policies to ensure they remained relevant and continued to provide clear guidance to officers.
- The Attorney-General gave the Director-General of Security updated written guidelines to be observed by ASIO in the performance of its functions.

## ASIO's Role and Functions

The Australian Security Intelligence Organisation (ASIO) is Australia's security service. It is a critical component of Australia's national security community and deals with threats to Australia's security.

ASIO's roles and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). ASIO's primary function is to collect, analyse and disseminate security intelligence. The ASIO Act defines 'security' as the protection of Australia, its people and interests against:

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

The ASIO Act extends ASIO's responsibility for security intelligence beyond Australia's borders. The ASIO Act also includes, in the definition of security, Australia's security obligations to other countries.

In fulfilling its obligations to protect Australia, its people and its interests, ASIO:

- collects intelligence through a wide range of means, including human sources and technical operations, using the least intrusive means possible in accordance with guidelines issued by ASIO's Minister, the Attorney-General;
- assesses intelligence and provides advice to Government on security matters;
- investigates and responds to threats to security;
- maintains a national counter-terrorist capability; and
- provides security assessments, including visa entry checks and for access to classified material and designated security controlled areas.

Under the ASIO Act and other legislation, ASIO can be authorised to use special powers under warrant, including powers to intercept telecommunications, enter and search premises, and compel persons to appear before a prescribed authority to answer questions relating to terrorism matters. ASIO also has specialist capabilities that can be deployed to assist in intelligence operations and incident response.

The ASIO Act also gives ASIO a function of more generally providing protective security advice to Government.

ASIO is responsible for collecting foreign intelligence under warrant within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence, and in collaboration with the Australian Secret Intelligence Service (ASIS) or the Defence Signals Directorate (DSD).

As ASIO is the only agency in the Australian Intelligence Community (AIC) authorised in the course of its normal duties to undertake investigations into, and collect intelligence on, the activities of Australian citizens; it operates within a particularly stringent oversight and accountability framework. The foundation of this framework is the ASIO Act, which has been crafted to ensure there is an appropriate balance between individual rights and the public's collective right to security. The Inspector-General of Intelligence and Security (IGIS) – an independent statutory authority – also plays an important role in ASIO's oversight.

## The History and Concept of Security Intelligence

The concept of ‘security intelligence’ can be traced back to before the First World War. It was originally understood to mean protection against espionage, sabotage and subversion. Australia experimented with this concept of security between 1915 and 1949, creating several different security organisations.

A dedicated security intelligence service was established in 1949 when Prime Minister Chifley gave the Hon Sir Geoffrey Reed KC PJ the directive that effectively created ASIO. At that time, a requirement was identified for an agency that would be an additional component in the defensive suite available to the Commonwealth, but performing a role distinct from the police and military. The need for such an agency stemmed directly from concerns within and outside Australia about the Australian Government’s ability to protect sensitive information. ASIO was thus charged with “the defence of the Commonwealth and its Territories from external and internal dangers arising from attempts at espionage and sabotage, or from actions of persons and organisations, whether directed from within or without the country, which may be judged to be subversive of the security of Australia”.

In his 1974–77 Royal Commission on Intelligence and Security, the Hon Justice Robert Hope AC CMG QC began his consideration of ASIO from the fundamental position of “whether Australia needs a security service such as ASIO”. He concluded it did, and recommended that the areas of ASIO’s ‘security’ interests be expanded beyond those originally prescribed.

Justice Hope noted that “there are many ways, short of war, in which a foreign power can weaken another, or strengthen itself vis-à-vis that other, by clandestine activities in the latter’s territory. There are likewise many ways in which a country can be weakened and the overthrow of its government planned and organised by clandestine activity of a wholly or substantially domestic origin”. Justice Hope considered it ASIO’s role to protect against these activities, and they were consequently enshrined in the definition of ‘security’ in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), the legal framework within which ASIO continues to operate. Justice Hope specified that ASIO should have responsibilities for counter-terrorism, noting that it was the normal purview of security agencies internationally and that Australia required “an organisation with access to intelligence available in and from other parts of the world about terrorism and identified or possible terrorists”.

The activities defined as ‘threats to security’ in the ASIO Act have in common that they can cause grave harm to Australians, Australian institutions or Australian interests. They will often target or involve Australian citizens or residents and they may be directed by, influenced by or otherwise linked to factors outside Australia, including foreign governments.

These features make protecting Australia against the high-impact consequences of threats to ‘security’ a particular challenge. Special capabilities and measures are often required to identify and respond to security threats, but this also needs to be balanced with concerns about the civil liberties of Australians, strong oversight and accountability, and public confidence that security investigations and operations are not politically influenced. This delicate balance has been achieved through the ASIO Act and other associated legislation.

## ASIO's Funding and Client Satisfaction

Funding to ASIO in 2007–08 expressed in terms of total price of Outputs was \$304.109m compared with \$234.764m in 2006–07.

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

Output	Actual 2006–07 \$m	Estimated 2007–08 \$m	Actual 2007–08 \$m	% of total
Output Group 1: Total	234.764	296.304	304.109	100

Table 1: Price of ASIO's Outputs

ASIO's revenue from Government increased 28% to \$291m in 2007–08, up from \$227m in 2006–07. The current Forward Estimates show ASIO's budget continuing to grow to \$417m by 2011–12, predominantly reflecting the planned increase in staff and depreciation associated with equity injections.

A significant equity injection of \$159m in 2007–08, following on from \$113m in 2006–07, allowed ASIO to continue its major capital investment activities, including:

- replacing and/or upgrading ageing equipment to support technical operations and surveillance capabilities;
- essential enhancements to underlying information technology infrastructure; and
- improved quality and flexibility of accommodation to support the growth of ASIO's State and Territory offices.

### Client Survey 2007–08

ASIO's 2007–08 Client Survey comprised interviews of clients from Commonwealth, State and Territory and private sector partners.

Consistent with the 2006–07 survey, client feedback was sought on the quality and effectiveness of ASIO's engagement with clients, and on ASIO's reporting and product. Clients were also asked for any specific initiatives and/or improvements that could be made to strengthen further and expand their engagement with ASIO.

Commonwealth agencies overall viewed their relationships with ASIO positively, with a number noting the further strengthening of partnerships on 2006–07 levels. State and Territory police were generally very satisfied with the level and quality of engagement with ASIO. ASIO was generally viewed as responsive and client-focused. A range of initiatives introduced by ASIO in 2007–08 were cited by partners as enhancing understanding and visibility of ASIO roles and priorities.

ASIO's reporting was seen generally as responsive, timely, useful and reaching the right people in client agencies. The introduction of new products, such as the *Insight* report, and refinements to Threat Assessments, were seen to have value-added to the current suite of ASIO products. Many clients indicated they would welcome a regular report that provides a summary/overview of all recently published ASIO products – a template is being developed to be introduced in 2008–09.

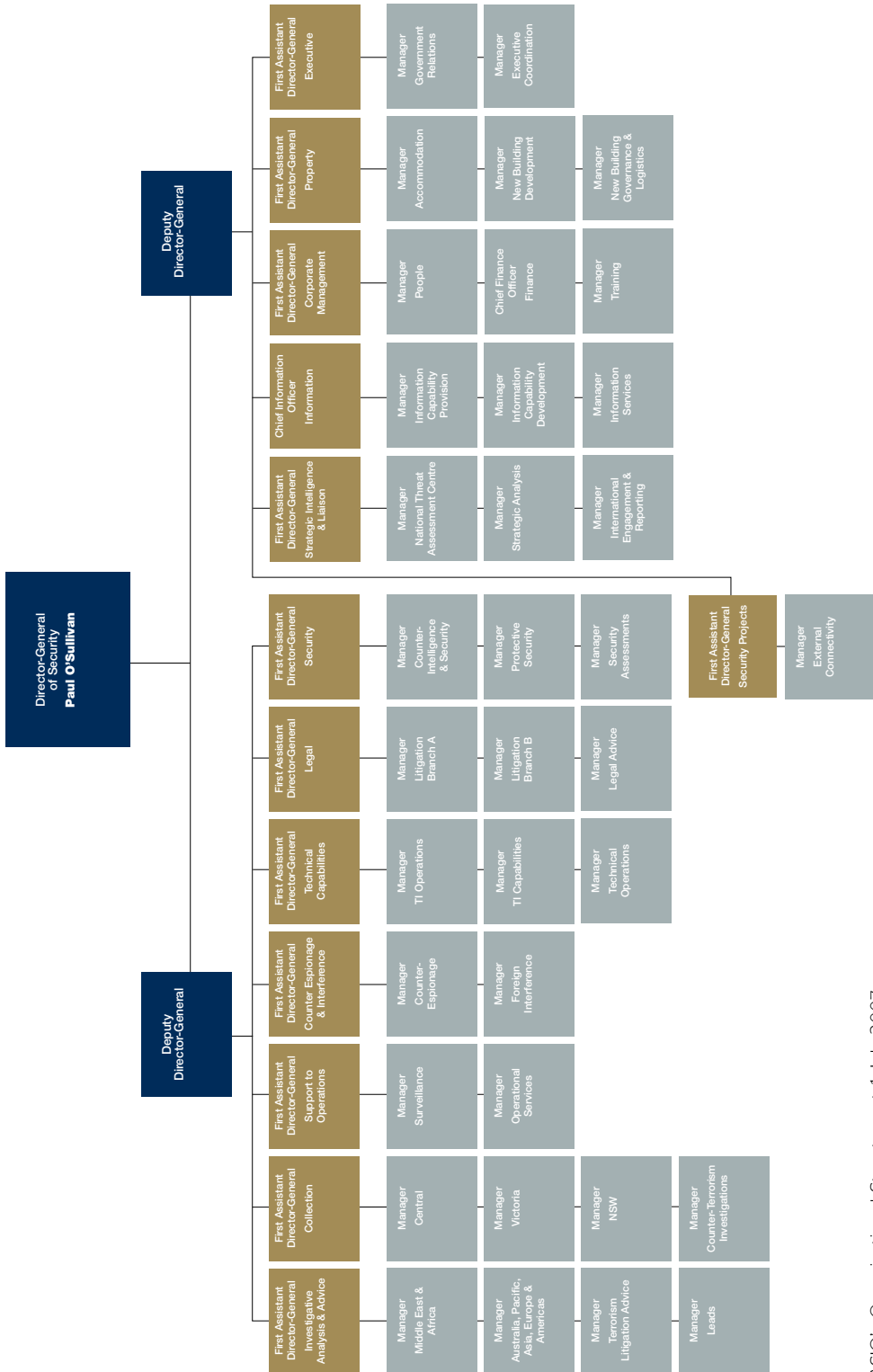
While clients believed senior-level engagement and coordination is working well, more still can be done at middle and working levels to promote understanding of ASIO's role and priorities. New initiatives are being developed and existing programs expanded to address this issue.

Private sector clients are generally satisfied with their relationship with ASIO, principally conducted via the Business Liaison Unit (BLU). The value of a central contact point for industry was specifically noted, as was the BLU's general responsiveness and focus on meeting client requirements.

## Organisational Structure

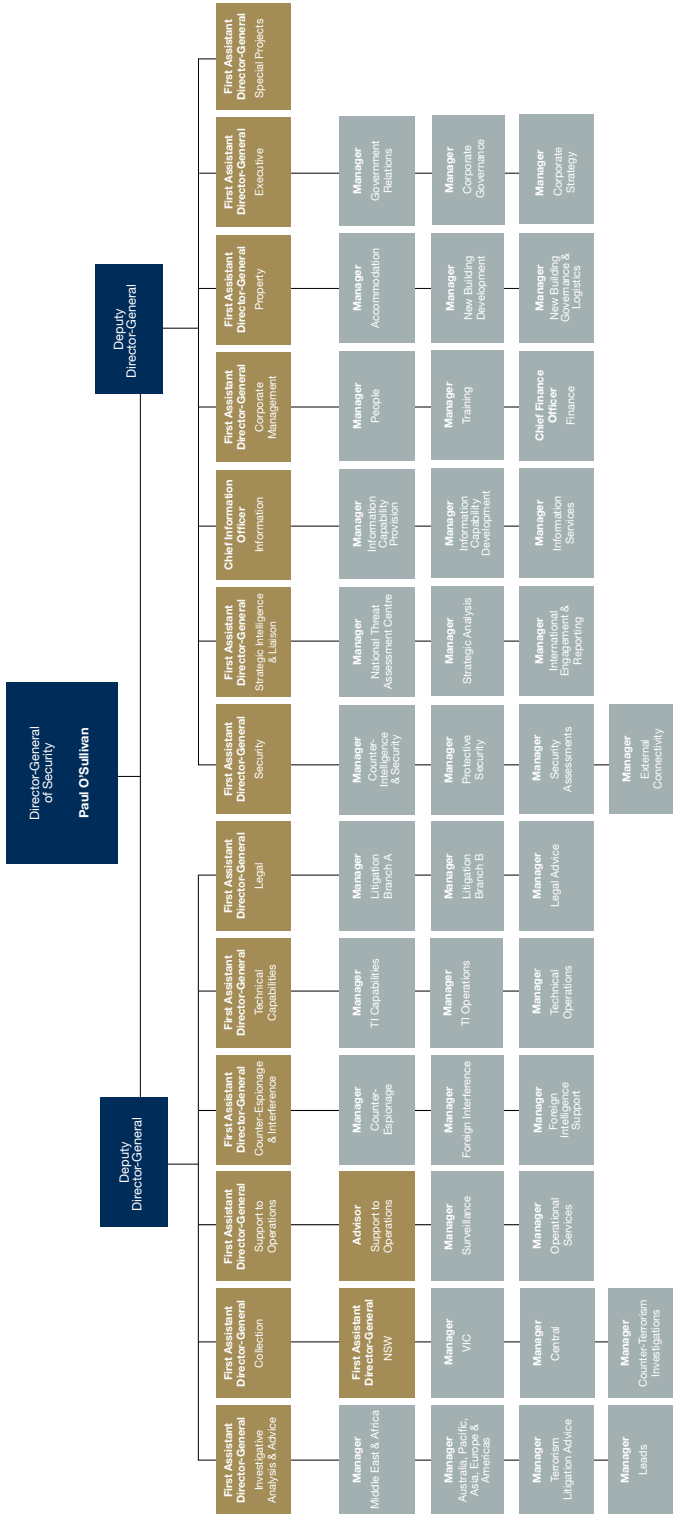
In 2007–08, an expanded 12 Division organisational structure took effect. In July 2008, ASIO will implement a number of further adjustments, including:

- expansion of Executive Division from two to three Branches – Government Relations, Corporate Governance and Corporate Strategy – strengthening further ASIO's strategic planning, priority setting, and governance framework. Executive Division plays a central role in strengthening engagement with key partners and supporting ASIO's contribution to government policy initiatives and reviews;
- an additional Branch in Counter-Espionage and Interference Division – Foreign Intelligence Support – reflecting the increased workload and complexities emerging in this important area;
- discontinuation of the temporary position of First Assistant Director-General Security Projects, as much of ASIO's high-level work to drive the implementation of policy and connectivity associated with ASIO's Security Assessments process has been completed. The important work of this area will be carried forward by External Connectivity Branch, which will be absorbed within Security Division; and
- a new temporary position, First Assistant Director-General Special Projects, to oversee a range of critical and high-level initiatives, and implementation of review outcomes.



ASIO's Organisational Structure at 1 July 2007





ASIO's Organisational Structure at 30 June 2008

## Guide to the Report

ASIO produces a classified and an unclassified version of its *Annual Report*. Section 94 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) requires the Director-General of Security, as soon as practicable after 30 June, to furnish the Minister with a report on the activities of ASIO. The Minister is required to table an unclassified version of this report in the Parliament within 20 sitting days of receipt.

ASIO is the only Australian intelligence agency to produce an unclassified *Report to Parliament*, and it has done so for almost 30 years.

## Guide to Outcome and Outputs Structure

In support of the Australian Government's 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
- Output 2 – Protective Security Advice
- Output 3 – Security Intelligence Investigation and Capabilities
- Output 4 – Foreign Intelligence Collection

# PART 1

---

THREATS TO AUSTRALIA IN 2007–08



## Threats to Australia in 2007–08

In 2007–08, the major security threats to Australia and Australian interests continued to reflect primarily developments overseas. Terrorism remained the most visible and immediate security threat globally, and this threat was linked in large part to the Middle East and South Asia.

Terrorism is not, however, the only security threat facing Australia. Australia will continue to be a target for espionage and foreign interference. Espionage is typically difficult to detect and can cause immediate and long-term harm to Australia's national security. Espionage and foreign interference can erode fundamental Australian institutions and values, degrade Australia's ability to promote and protect its vital national interests, and undermine its crucial alliance relationships.

A number of second-order threats also continue to require ASIO's attention. These include violent protest and communal violence.

### Terrorism

ASIO is responsible for providing security intelligence advice on politically motivated violence (PMV). This includes acts or threats of violence or unlawful harm intended to achieve a political objective, and acts that are likely to lead to violence and are intended to overthrow Australia's system of government. Terrorism falls within the definition of PMV in the ASIO Act, and due to the severity of the threat and its potential consequences, currently commands the majority of ASIO's operational attention and resources.

### The Global Militant Jihad

The primary terrorist threat to Australia and its interests continues to come from violent jihadists who act on the belief that it is a religious and moral duty of every Muslim to attack 'Crusaders' – the United States and its allies – and apostate Muslims wherever they can. Australia and Australians are considered a legitimate target. While this is an aberrant and simplistic interpretation of Islamic doctrine, it nonetheless carries substantial appeal for its proponents.

While headway is being made to counter Islamic extremism, it is likely to remain a virulent component of the global security environment for at least a generation – both in its global and local forms. Its ideology appeals across generations and continues to attract new adherents.

Al-Qa'ida continues to be the vanguard of the international jihadist movement. It has itself planned and undertaken attacks, funded and facilitated attacks by others, established a sophisticated global propaganda campaign and become an inspiration to other jihadists. It continues to seek opportunities to undertake its own attacks, and provides guidance and support to other jihadist groups and 'home-grown' terrorists, such as those who undertook the July 2005 London bombings. It has also linked up with 'franchises' – groups engaged in local insurgencies with nationalistic or ethnic dimensions that have come to view their struggle in global terms, or previously independent jihadist groups that have taken the name 'al-Qa'ida' in relation to a specific geographic region (such as al-Qa'ida in the Lands of the Islamic Maghreb – AQIM).

The international jihadist movement has never depended on a single overarching group or any formal organisation. There are linkages between the diverse array of terrorists and terrorist groups in the world, but they do not form any single definable organisation. The fluid and decentralised nature of the global jihad is exemplified in the phenomenon of 'home-grown' jihadists – those, largely in developed countries, who have radicalised and organised independently. Increasingly, extremists are emerging independently and in locations

and communities where they have not previously been seen, their only connection to al-Qa'ida being their identification with its broad message and ideology.

Al-Qa'ida's core leadership operates from the tribal areas of Pakistan – a safe haven that has given al-Qa'ida the time and space to reconstitute itself. It maintains its influence over extremists in a range of countries including across North and East Africa. While authorities have had some success in reducing the terrorist threat from al-Qa'ida in Iraq (AQI), terrorism in North and East Africa, particularly the activities of AQIM, has expanded across the region and increased in tempo. This trend is expected to continue.

## Incidents Affecting Australians

Globally, in 2007–08, terrorist attacks or incidents affecting Australian civilians included:

- on 10 July 2007, private security contractor Darryl de Thierry died in Iraq as a result of an improvised explosive device (IED) attack;
- on 14 January 2008, the Serena Hotel in Kabul, Afghanistan – the temporary home of the Australian Embassy – was attacked by Islamic militants; and
- on 29 April 2008, an Australian journalist travelling in a police convoy in Nangharar Province, Afghanistan, was injured by a suicide bomber. At least 18 Afghans were killed and 35 injured.

Additionally, four members of the Australian Defence Force were killed during counter-terrorism related operations in Afghanistan.

Statements by extremist elements, including groups associated with al-Qa'ida, continue to mention Australia. On 2 April 2008, al-Qa'ida's media arm, as-Sahab, posted to jihadist Internet forums an audio file of Ayman al-Zawahiri responding to questions from forum participants. Al-Zawahiri justified attacks against the United States and its allies, including Australia, saying these countries supported Israel.

## Asia and the Subcontinent

The threat environment continues to be volatile in parts of South Asia, particularly Pakistan and Afghanistan. ASIO remains focused on al-Qa'ida in Waziristan and the Federally Administered Tribal Areas (FATA) of Pakistan.

In Afghanistan, Anti-Coalition Militia (ACM) attacks against Coalition forces continue. Australian civilians have also been the victims of anti-Western attacks.

Since November 2007, a series of coordinated bombings in India have killed in excess of 100 people and injured many others. Responsibility for the attacks has been claimed by a group calling itself the Indian Mujahideen.

## South-East Asia

The counter-terrorism outlook for South-East Asia is generally improving but remains serious. There were no major attacks against Western interests during the period. Jemaah Islamiyah (JI) no longer has the strategic reach it once enjoyed. However, JI is a resilient organisation and has not abandoned its violent Islamist goals, so its future direction remains a concern.

While the threat from JI has diminished, the terrorist threat in South-East Asia has not gone away. South-East Asia's most wanted terrorist, Noordin Mohammad Top, remains at large and capable of attacking Australians.

Three of Top's associates, Amrozi, Mukhlas, and Imam Samudra, have been sentenced to death in Indonesia for their roles in the 2002 Bali bombings.

A terrorist cell in Palembang, Indonesia – possibly associated with Top and allegedly intending to conduct anti-Western attacks – was disrupted in late June 2008 by Indonesian authorities. The recovery of a number of IEDs provided evidence of ongoing terrorist intent and capability among Indonesian Islamic extremists.

## Developments in Australia

Terrorism-related activity continues to take place in Australia. ASIO and its partners have previously disrupted significant terrorism planning and ASIO continues to assess that without preventative actions taken by Australian authorities, attacks would have occurred here.

ASIO is aware of a significant number of Australians who hold, or have held, extremist views. Some of these Australians have shown a willingness to put these views into action – some have travelled overseas to train with terrorist groups or engage in jihad activities, and some have been charged or convicted of terrorist offences.

## Proscription of Terrorist Organisations

In Australia terrorist groups are prohibited through a process of proscription. ASIO's role is to provide advice to the Attorney-General by means of a 'statement of reasons', recommending that a group be listed under the *Criminal Code Act 1995* regulations. ASIO assesses a range of factors when considering organisations for proscription. These may include engagement in terrorism, ideology, links to other terrorist networks, threats to Australian interests, or proscription by the United Nations or other countries.

The Minister (Attorney-General) must be satisfied on reasonable grounds that the organisation to be proscribed:

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

At 30 June 2008, 19 groups were proscribed in Australia (see Appendix A).

On 8 September 2007, the following proscribed terrorist groups were re-listed under Australian law after meeting one or both of the grounds described above:

- Lashkar-e-Tayyiba (LeT);
- Hamas' Izz al-Din al-Qassam Brigades; and
- Palestinian Islamic Jihad.

The Kurdistan Worker's Party (PKK) was re-listed on 28 September 2007. As part of the re-listing process for the PKK, an ASIO Deputy Director-General appeared in-camera before the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on 20 March 2008. On 25 June 2008, the report of the PJCIS endorsing the PKK being re-listed as a terrorist organisation was tabled in Parliament.

## Chemical, Biological, Radiological, Nuclear, and Explosives Terrorist Weaponry

The ability to identify new terrorist capability, tactics, techniques and procedures is an important component of ASIO's counter-terrorism efforts. The development and acquisition of more lethal weaponry and capability is an objective for some terrorist operatives. Terrorist acquisition of weapons of mass destruction would be a grave development with strategic consequences.

In 2007–08, ASIO enhanced its ability to provide chemical, biological, radiological, nuclear, and explosive terrorist (CBRNET) weaponry advice. ASIO's CBRNET team worked closely with other experts across the Australian Intelligence Community (AIC), the Australian Federal Police (AFP), and other parts of Government with responsibility for health, radiological and chemical matters.

Conventional explosives remain the most prominent form of terrorist weaponry, as demonstrated by continued use against Coalition forces in Iraq and Afghanistan, and in attack planning such as that disrupted in Palembang, Indonesia.

Although far less prevalent than explosives, terrorist pursuit of chemical, biological, and radiological (CBR) weaponry continues.

### Foreign Interference

ASIO is responsible for countering foreign interference in Australian affairs – such as clandestine activities by a foreign power to influence governmental processes in Australia, or inappropriate interference in the affairs of expatriates in Australia.

Foreign diplomats and officials are known to collect information on – and sometimes actively target – individuals in Australia whom they consider to be dissident, disloyal or otherwise of interest. Some of this activity is conducted overtly in the course of regular consular or community liaison by foreign officials.

Measures taken by foreign powers can involve individuals being detained, threatened or coerced when they travel from Australia to other countries, particularly their country-of-origin. ASIO is also aware of instances where threats have been made against associates and relatives in attempts to coerce Australians to cooperate with police or intelligence services.

In 2007–08, ASIO continued to undertake enquiries and investigations to identify foreign interference in Australia.

### Espionage

Criminal offences relating to espionage are set out in the *Criminal Code Act 1995* and in the *Crimes Act 1914*. In broad terms, espionage is the theft of information or capability by persons acting on behalf of a foreign power. Australia's geographic position, strategic posture, economic wealth, military technology, and close alliance with the United States make Australia a potential target for espionage.

Some espionage can arise from foreign interference activity, where a country's foreign intelligence service finds opportunity to cajole or coerce into cooperation one of its former nationals with access to sensitive Australian information. The original purpose of their targeting may not have been directed at espionage, but intelligence services are opportunistic and will often try to turn such opportunities to their advantage.



In other cases espionage arises from deliberate efforts by foreign intelligence services to penetrate governments, their intelligence services, their departments and agencies, and strategic sectors of industry in pursuit of secret information for commercial or economic advantage.

Increasing pressure to gain an edge in both public and private sectors is fuelling a trade in sensitive information. And as the incentives to undertake espionage continue to evolve, so too do the types of actors prepared to undertake them. Individuals, companies, and terrorist groups may seek to gain access to sensitive information. ASIO anticipates it will need to respond more often to these non-traditional espionage threats.

Counter-espionage work can be particularly complex and challenging. ASIO has boosted the level of resources devoted to this function, and has plans to build further capability through to 2010–11.

## Proliferation

ASIO's counter-proliferation work focused on detecting and preventing attempts to exploit Australia's industrial, technological and educational resources for the illicit development of Weapons of Mass Destruction (WMD).

Australia has legislated obligations to ensure compliance with various United Nations Security Council Resolutions that are aimed at preventing the spread of WMD, with particular emphasis on Iran.

## Violent Protest

Most protest activity in Australia is peaceful and lawful and therefore not of concern to ASIO. Section 17A of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) mandates that the Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent.

However, a small number of individuals consider the promotion and use of violent protest tactics are justified in order to influence government policy or to achieve other political ends. The activities of these individuals can fall within the definition of politically motivated violence in the ASIO Act and, therefore, be of interest to ASIO.

In 2007–08, issue motivated groups (IMGs) protested over matters including:

- the series of APEC forum meetings held in venues across Australia;
- the conflicts in Iraq and Afghanistan;
- climate change and global warming;
- military exercises, including the Talisman Sabre exercises in Queensland; and
- issues linked to the 2007 Federal Election.

No significant violent protest occurred in Australia during 2007–08.



# PART 2

---

OUTPUT PERFORMANCE



## Output 1: Security Intelligence Analysis and Advice

### Output at a glance

ASIO provided high-quality, timely and accurate security intelligence analysis and advice to a broad customer base. It produced a range of tailored strategic and investigative analytical products and Threat Assessments. It also provided advice on protecting Australia's critical infrastructure and on border security (including through visa security assessments). ASIO information was used to support legal processes, including terrorism prosecutions.

ASIO's expertise in major event security planning helped ensure the 2007 Asia-Pacific Economic Cooperation (APEC) forum occurred without significant security incident. ASIO also contributed to the security planning for the 2007 Federal Election, the 2008 Anzac Day commemorations, the 2008 Olympic Torch Relay, and World Youth Day 2008, in each case working closely with law enforcement and other agencies.

ASIO diversified and tailored further its range of security intelligence reporting to meet the needs of its customers. ASIO produced 3,224 reports (an increase of 17% on 2006–07) including 2,075 Threat Assessments and related reports.

ASIO completed 72,688 permanent and temporary visa security assessments – representing an overall rise of 36% on 2006–07 – continuing the trend of increased workload in this area. ASIO made substantial improvements in reducing security assessment timeframes for visa applicants through the implementation of process improvements and the first two phases of the Next Generation Border Security initiative. ASIO issued two adverse security assessments on visa applicants.

ASIO completed a program commenced in 2004–05 to produce critical infrastructure sectoral threat assessments. Through the Business Liaison Unit (BLU), ASIO enhanced its engagement with industry. The BLU published 85 Business Security Reports and coordinated 10 'Executive Program' briefings by the Director-General of Security for company Chief Executive Officers (CEOs).

ASIO's involvement in legal processes, in particular terrorism prosecutions and civil and administrative proceedings, continued to increase. ASIO committed substantial resources to respond to subpoenas and provide material to support terrorism prosecutions. A growing challenge for ASIO is balancing the need to support Commonwealth involvement in legal processes with the need to protect sensitive sources, methods, and capabilities.

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

## 1.1 Strategic, Investigative and Complex Analysis

### ASIO's Product Range and Customer Base

As part of its security advice function, ASIO produces a range of formal assessments and reports to meet specific client requirements. These reports complement extensive day-to-day tactical and operational level engagement and information sharing. ASIO's range of clients is broad and includes Commonwealth, and State and Territory Government departments, agencies and police services, the private sector and international liaison partners.

In 2007–08, ASIO produced 3,224 formal reports and assessments for approximately 75 Commonwealth, and State and Territory departments, agencies and police services.

ASIO received positive feedback across its suite of products in 2007–08. Its intelligence reporting was considered timely, valuable and relevant. ASIO product aided a broad range of agencies to develop policy and operational responses, and increased clients' knowledge. Feedback indicated ASIO's reporting was viewed as authoritative.

### Security Intelligence Reporting

ASIO's security intelligence reporting informs Australian Government decision-making and threat response. Reports cover a broad range of topics such as Australians involved in extremist activity, terrorist tactics, counter-intelligence, counter-proliferation, and emerging protective security issues.

### Strategic Analysis

In addition to security intelligence reports that focus on investigative and tactical-level assessments, ASIO's strategic analysis examines longer-term trends and patterns. ASIO continued to deliver high-quality strategic analysis in 2007–08.

In April 2008, ASIO introduced a new line of reporting – *Insight* papers. They provide an executive snapshot and strategic context of current and emerging issues in the security environment to assist high-level customers develop policy settings. Feedback indicated the new product was well received, as it provided clients with a timely and concise summary of current security issues – particularly on how international issues manifested themselves domestically.

### Security Intelligence Seminar

For the first time, ASIO invited a selection of prominent academics and representatives from think tanks to a Security Intelligence Seminar held in June 2008 at ASIO's Central Office. There was a productive two-way exchange, and, given its success, ASIO intends to continue such activities.



*The Director-General of Security Mr Paul O'Sullivan with Security Intelligence Seminar participants*

## ASIO's Support to Special Events

ASIO has considerable expertise in providing intelligence and operational support to special events in Australia and overseas – including to the Sydney 2000 and Athens 2004 Olympic Games, the Commonwealth Heads of Government Meetings in 2002 in Queensland, and a variety of other senior economic and political forums. ASIO's role in supporting special events includes:

- Threat Assessments to inform security planning;
- security assessments to inform venue access control;
- security assessments for individuals applying to travel to Australia to participate in special events;
- physical security and risk management training and advice; and
- operational and technical support.

The APEC forum was a significant focus for ASIO during the reporting period, along with the Federal Election, Olympic Torch Relay and Anzac Day commemorations. In 2007–08, ASIO also began planning its security intelligence response for World Youth Day 2008 and the 2008 Beijing Olympics and Paralympics (which subsequently occurred without any major security incidents affecting Australians).

### The APEC forum

The APEC forum was the most significant series of international meetings ever hosted in Australia, culminating in the APEC Economic Leaders Week (AELW) Meeting held in Sydney in September 2007. Heads of government from 21 APEC economies attended the Leaders Meeting. ASIO worked closely with government agencies – in particular New South Wales Police, the Australian Federal Police (AFP) and the Department of the Prime Minister and Cabinet (PM&C) APEC 2007 Taskforce – in planning the security of APEC forum events.

The APEC forum was a significant test of ASIO's planning and response capabilities, requiring a sustained effort over many months and across a range of venues and locations.

ASIO had prime responsibility for collecting, analysing and disseminating security intelligence for the APEC forum, including through:

- provision of security intelligence advice to assist APEC preparations from June 2005;
- operation of the APEC Security Intelligence Centre, which coordinated security intelligence input from Australian and overseas agencies;
- conduct of security checking of 16,573 individuals requiring official APEC forum accreditation, including checking of visa applicants travelling under the APEC 2007 Travel Authority;
- provision of physical security and risk management training and advice to New South Wales and Western Australia Police;
- assistance in the production of, and participating in, a series of APEC-themed counter-terrorism exercises across Australia; and
- briefing of international partners in Australia and through ASIO's overseas liaison posts in the lead-up to, and during, AELW.

ASIO's sustained contribution to the security of the APEC forum series of meetings – and its capacity to provide intensive support during AELW – helped ensure the APEC forum was concluded without significant security incident.

### **2007 Federal Election**

The 2007 Federal Election was a major focus of ASIO threat reporting in October and November 2007. There were no significant security incidents.

### **2008 Beijing Olympic Torch Relay**

ASIO provided threat advice for the Olympic Torch Relay in Australia. While protests were largely incident free, several small scuffles and some verbal provocation occurred between pro- and anti-Peoples Republic of China (PRC) activists. Five individuals were arrested and charged with interfering with a special event.

ASIO worked closely with the AFP on security for the Torch Relay and provided officers to a Joint Intelligence Group established for the event.

### **2008 Anzac Day Commemorations**

In 2008, Anzac Day commemorations occurred without security incident. ASIO issued threat advice for the various commemoration ceremonies around the world.

### **World Youth Day 2008**

At the end of the reporting period, ASIO was well advanced in its preparation for World Youth Day 2008 (WYD). To be held from 15–20 July 2008 it was to be the largest single event ever held in Sydney. Approximately 500,000 participants were expected, including about 130,000 international visitors entering Australia through major airports. His Holiness Pope Benedict XVI, and numerous Cardinals and Bishops from around the world were also planning to attend.

ASIO's responsibility for WYD included coordinating security intelligence information from other agencies (both in Australia and overseas) for assessment and dissemination to New South Wales Police and relevant Commonwealth and State and Territory bodies.



During 2007–08, ASIO accelerated its engagement with Commonwealth, State and Territory agencies, the WYD Organisation and with the WYD Coordination Authority. ASIO participated in regular planning and preparation meetings with the New South Wales Police WYD Security Command.

During 2007–08, ASIO conducted security checks for accreditation of individuals requiring access to security controlled areas. Together with police checks, the accreditation process provided assurance that individuals with approved access to secure areas were unlikely to pose a security threat.

### 2008 Beijing Olympic and Paralympic Games

The 2008 Summer Olympics were to take place in Beijing between 8–24 August, followed by the Paralympic Games between 6–17 September.

ASIO was a member of the Security and Intelligence Specialists for the 2008 Beijing Olympics Games (SISBOG) – the official body for security and intelligence liaison. SISBOG's role was to provide advice to Games organisers on intelligence gathering and assessment, and counter-terrorism.

ASIO worked closely with international partners on potential threats to the Beijing Olympics.

ASIO's National Threat Assessment Centre (NTAC) published regular assessments of the threat to Australian interests in China for the Olympic period.

## ASIO's lead development and analysis

ASIO obtains thousands of intelligence leads each year. Leads are received by all operational units of ASIO and many arise from ASIO's operational activities. Leads from external sources can come from police services, other Australian Government agencies, international partners, open sources and the public, including those received via the National Security Hotline (NSH).

In ASIO, each lead is assessed to identify its relevance to security – specifically, whether or not there is a nexus between the lead information and the definition of security in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). ASIO is authorised to conduct inquiries to assist its assessment of a matter's relevance to security.

If ASIO is unable to identify any relevance to security the matter is not investigated further. ASIO does have some discretion to refer matters to other agencies – including police – if, for example, they relate to indictable criminal offences.

If, however, the matter is relevant to security, ASIO is authorised to undertake further investigative activity. In accordance with the *Attorney-General's Guidelines*, ASIO uses the least intrusive investigative means possible to collect information. The resources allocated to an investigation, and the level of intrusiveness adopted, is determined largely by the imminence and potential consequences of the assessed threat.

In 2007–08, ASIO continued to work closely with Commonwealth, State and Territory law enforcement authorities to resolve intelligence leads, particularly those arising from the NSH. This process involved close coordination and cooperation at the regional level. Regular inter-agency meetings were held in States and Territories to discuss progress of leads and to determine responsibility for follow-up activity.

## 1.2 Threat Assessments

ASIO's NTAC provides a 24-hour all-source threat assessment capability. Threat Assessments are the primary vehicle by which Australia's formal threat levels are set for people, places and events – both in Australia and overseas. They provide a vehicle for sensitive information to be taken into account by police and other agencies for protective security and tactical responses. And they are reflected in threat advice provided to the private sector, and can be drawn upon to inform public travel advisories issued by the Department of Foreign Affairs and Trade (DFAT).

ASIO brings an experienced and rigorous approach to assessing threat. ASIO has the information systems, data holdings, processes, and legislative and oversight arrangements to ensure that it is able to provide threat advice while appropriately handling sensitive information, including about Australian citizens and residents. ASIO is uniquely placed to combine intelligence from the full range of sources – including international partners, Australian departments and agencies, and open source information – to provide holistic security threat advice.

ASIO draws on the expertise of officers seconded to NTAC from a range of Australian Government agencies including DFAT, Office of National Assessments, Australian Secret Intelligence Service (ASIS), Defence Intelligence Organisation, Defence Signals Directorate (DSD), the AFP and the Department of Infrastructure, Transport, Regional Development and Local Government.

Representatives have access to their home agencies' computer systems. This facilitates coordination between government agencies and assists NTAC reflect all relevant information available in its Threat Assessments.

### Performance and Product

In 2007–08, NTAC developed further its suite of products, including:

- the *Outlook* report, which provides a monthly 'snapshot' of the security environment and the global threat to the lives of Australians, and Australia's vital interests;
- Threat Analysis Papers, which report on trends in the threat environment and provide background information, beyond that provided in Threat Assessments, on groups of security interest in Australia and overseas. In response to high customer interest, the number of papers produced during the reporting period increased significantly; and
- Country Reports that detail the threat environment in specific countries. NTAC also contributes relevant material from these reports to the Business Liaison Unit's Country Snapshots, which are made available to industry.

NTAC produced 2,075 products in 2007–08, comprising:

- 1,818 Threat Assessments;
- 12 *Outlook* reports;
- 147 Threat Analysis Papers; and
- 98 Country Reports.

Subject of Assessment	2004–05	2005–06	2006–07	2007–08
Australian interests (in Australia and overseas)	427	503	502	507
Australian dignitaries	676	755	403	500
Diplomatic premises in Australia	24	22	29	15
Visiting dignitaries	228	162	423	226
Special events (a)	37	58	81	68
Protective security	49	48	46	34
Vital infrastructure	29	20	33	14
Demonstration notifications	56	32	20	12
Liaison Threat Advice	347	492	183	305
Threat Analysis Papers	-	6	80	147
Country Reports	-	-	22	98
Outlook (b)	-	-	24	12
Incident Advices (c)	-	-	-	93
Other Threat Assessments	130	118	148	44
<b>TOTAL</b>	<b>2,003</b>	<b>2,216</b>	<b>1,994</b>	<b>2,075</b>

Table 2: Threat reporting by year and category

Notes:

(a) Special events for 2007–08 includes the APEC forum 2007, World Youth Day 2008 and the 2008 Beijing Olympic Games

(b) *Outlook* formerly known as the 'Fortnightly Threat Review'.

(c) Incident Advices formerly reported under the category 'Other Threat Assessments'.

NTAC intends to increase production of unclassified product for certain clients, to allow for broader dissemination of threat information.

## Coordination and Cooperation with Other Agencies

NTAC chairs the Terrorist Threat Coordination Group which considers current and emerging threat issues. The Group comprises the Australian Intelligence Community (AIC) agencies, the AFP, and DFAT. It meets monthly and convenes on an ad-hoc basis in the event of a crisis.

Throughout 2007–08, State and Territory police services provided important information on violent protest activity to inform ASIO Threat Assessments. The information was critical to ASIO's understanding of protest trends and in evaluating the accuracy of ASIO's assessments.

### 1.3 Border Security

ASIO contributes to the security of Australia's borders through:

- visa security assessments for travellers to Australia;
- liaison officers at Australia's ports;
- security intelligence advice for Australian agencies; and
- seaport and airport personnel security checking.

## Visa Security Assessments

Any person applying for a visa to travel to, or remain in, Australia may have their application referred by the Department of Immigration and Citizenship (DIAC) to ASIO for a security assessment – an assessment of the risk that the person's presence in Australia would pose to security (as defined in the ASIO Act).

In 2007–08, ASIO saw a substantial increase in the number of visa applications requiring ASIO assessment. Despite the increase in referrals, client service timeframes continued to improve.

Visa security checks are generally managed in order of referral from DIAC, taking into account any agreed priority caseloads (with particular emphasis on the refugee, humanitarian and protection caseloads and genuine compassionate or compelling cases). The current security environment and the increasing volume of intelligence – which often provides only partial insight – can complicate the assessment process.

In conducting security assessments, ASIO draws on classified and unclassified information to evaluate the subject's activities, associates, attitudes, background and character, taking into account the credibility and reliability of available information. Where there are inconsistencies or doubts, the person may be interviewed by ASIO.

ASIO is required to limit its consideration in security assessments to issues related to 'security' as it is defined in the ASIO Act (other factors affecting the issue of a visa, such as health or criminal grounds, are not within ASIO's remit). Where ASIO determines that a person's presence in Australia would pose a direct or indirect risk to security, ASIO may recommend against the issue of a visa.

### ASIO's use of the Movement Alert List

DIAC's Movement Alert List (MAL) is used by ASIO to identify known persons of security interest who are attempting to obtain an Australian visa.

### Permanent and temporary visas

In 2007–08, ASIO completed 72,688 visa security assessments (see Table 3). These comprised 16,562 assessments for permanent visa holders and 56,126 assessments for temporary visa holders.

### Protection visas

In 2007–08, ASIO completed 1,311 assessments for protection visa applicants. This represented an increase of 14% from 2006–07.

ASIO conducts security assessments of protection visa applicants, including:

- unauthorised arrivals (those who travel by boat or air using false or no documentation); and
- applicants who arrive legally in Australia on a valid visa and who subsequently claim protection.

The *Migration Act 1958* requires the Minister for Immigration and Citizenship to make a decision on protection visa applications within 90 days. ASIO devotes specialist resources to assist in meeting these timeframes. In 2007–08, 62% of protection visa applications referred to ASIO for assessment were completed within the required timeframe, up from 52% in 2006–07. ASIO continues to allocate resources to improve the timeliness of protection visa security assessments.

Type of entry	2003–04	2004–05*	2005–06*	2006–07*	2007–08*	% increase from 2006–07
Temporary	30,841	39,015	39,973	44,197	56,126	27%
Permanent	13,881	13,402	13,174	9,190	16,562	80%
<b>TOTAL</b>	<b>44,722</b>	<b>52,417</b>	<b>53,147</b>	<b>53,387</b>	<b>72,688</b>	<b>36%</b>

\*From 2004–05, figures include protection visas

Table 3: Visa security assessments 2003–04 to 2007–08

### Maritime Crew Visas

Maritime Crew Visas (MCVs) were introduced on 1 July 2007 and became mandatory on 1 January 2008. MCVs apply to non-Australian crew members of maritime vessels intending to berth at an Australian port. The MCV regime brings the visa checking requirements for crew of foreign vessels into line with other temporary visa checking regimes.

In 2007–08, ASIO completed 2,718 assessments for MCVs.

### Adverse and qualified security assessments

Two visa applicants were assessed by ASIO in 2007–08 to pose a direct or indirect risk to security, and adverse assessments were subsequently issued against them.

### Improving security assessment timeframes and outcomes

ASIO reduced substantially the time required to complete visa security assessments in 2007–08. This reflected ASIO's ongoing improvement of processes, rigorous prioritisation of workloads, and the implementation of phases one and two of the Next Generation Border Security initiative. These phases enabled a transition from paper-based to semi-automated processes for certain temporary visa referrals through a new electronic system known as the Security Referral Service (SRS). The SRS connects specialised DIAC and ASIO computer systems and delivers significant improvements in the security assessment process, enhancing the auditing and tracking of cases and improving processing times.

### Passport cancellations

In 2007–08, the Minister for Foreign Affairs cancelled two Australian passports following the issue of security assessments by ASIO.

## The Next Generation Border Security initiative

Australia is in a strong position to develop further an intelligence-led border control system that includes more efficient visa security checking and the flexibility to respond more quickly to changes in the security environment.

The Next Generation Border Security (NGBS) initiative – predominantly involving ASIO and DIAC – is designed to improve the effectiveness and efficiency of security checking processes conducted by ASIO for applicants for Australian visas. The initiative will provide better identification and prevention of entry to Australia of people of security concern, while ensuring that legitimate international travellers to Australia do not suffer unwarranted delays in visa issue.

A central feature of the NGBS initiative is the creation of direct electronic connectivity for the transmission of certain visa applications from DIAC to ASIO for assessment – known as security referrals. This allows for faster and more reliable assessment of the potential threat, and an electronic response to DIAC.

Implementation of the NGBS is well advanced and already contributing to improvements in security assessment service timeframes and outcomes. Funding for phases one to three of the initiative was provided in February 2008 (\$35.9m total over four years).

### Security Intelligence Advice to Border Security Authorities

ASIO provides security intelligence reporting and regular briefings on border security issues for senior managers and operational staff within border security agencies such as DIAC and Australian Customs Service (ACS).

### Seaport and Airport Personnel Security Checking

ASIO conducts security checks on personnel requiring access to security-controlled areas at Australian seaports and airports. These checks are an important part of the process for determining a person's suitability to hold an Aviation Security Identity Card or Maritime Security Identity Card. (See p. 26 for details.)

### Border Liaison Officers

ASIO's Border Liaison Officers provide an interface between ASIO and Australia's border security community. Since 2003, ASIO has based Airport Liaison Officers (ALOs) at a number of major airports around Australia. ALOs work closely with key airport partners including the AFP, ACS, DIAC, airline operators and airport security staff. ASIO also has Maritime Security Liaison Officers who perform a similar security liaison role at Australia's major seaports.

## 1.4 Critical Infrastructure Protection

Critical infrastructure consists of physical facilities, systems, information technologies and networks that if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence or ensure national security.

Commonwealth, State and Territory Governments – as well as private industry – make decisions about the protection of critical infrastructure on the basis of risk. Judgements about risk are substantially informed by an assessment of the threat to a particular ‘sector’ (for example, the Energy sector) or a ‘vital asset’.

As part of the Australian Government’s framework for the protection of critical infrastructure – and under the direction of the National Counter-Terrorism Committee (NCTC) – ASIO:

- is responsible for a national database of critical infrastructure assets on behalf of the NCTC;
- provides assessments on the threat from terrorism to Australia’s 11 nationally critical infrastructure sectors and sub-sectors (see Table 4);
- assesses the terrorist threat to specific individual assets categorised as ‘nationally vital’;
- provides advice and assessments on terrorist and other threats to the National Information Infrastructure (NII); and
- provides briefings to government and private sector stakeholders on the threat to critical infrastructure.

### Nationally Vital Critical Infrastructure Sectors

Food Supply

Health

Energy

Utilities

Transport

Essential Manufacturing

Communications

Finance

Emergency Services

Government Services

Icons and Public Gatherings

Table 4: Critical infrastructure sectors

ASIO also provides a range of analytical, liaison and technical activities including:

- protective risk reviews of vital Commonwealth assets;
- liaison with State and Territory police and emergency services, as well as relevant industry associations, owners, and operations and security managers of critical infrastructure;
- briefings – in cooperation with the Attorney-General’s Department – to industry sectors on the considerations underpinning ASIO’s sectoral Threat Assessments;
- an intelligence interface with industry through ASIO’s BLU, created specifically to share information – both locally derived and from international partner agencies – with the private sector;
- contributing to the ‘E-Security National Agenda’ through security guidance to the E-Security Policy and Coordination Committee; and
- within the terms of a formal arrangement with DSD and the AFP High Tech Crime Centre, investigating cyber-incidents of national significance.

## Assessing the Threat to Critical Infrastructure

Classified ASIO Threat Assessments for each of the 11 critical infrastructure sectors and nationally vital assets are a key component of Australia's protective security arrangements. ASIO's assessments are conducted in close cooperation with Commonwealth, State and Territory Governments and private sector stakeholders. They underpin consideration of security risks and mitigation strategies.

During 2007–08, ASIO achieved a significant milestone in completing the first 'cycle' of critical infrastructure sectoral threat assessments (commenced in 2004–05) and embarked on a new phase of updating assessments. ASIO produced 11 papers providing sectoral critical infrastructure threat advice (two of these were released to liaison partners) and three updates of Threat Assessments for nationally vital critical infrastructure assets. ASIO also provided 56 briefings during 2007–08.

The NII comprises electronic systems that underpin critical services such as telecommunications, banking and finance, transport and distribution, and energy and utilities. Under Joint Operating Arrangements (JOA) – a formal agreement between ASIO, DSD and the AFP – ASIO responds to threats to the NII that have a national security dimension. In addition, ASIO prepares Threat Assessments on the NII for policy-makers and security risk managers.

## National Critical Infrastructure Database

A database of Australia's critical infrastructure is maintained by ASIO and compiled with the assistance of State and Territory bodies. Asset entries are ranked for criticality – vital, major, significant, low, or unspecified. The database is continually reviewed and updated.

### The Business Liaison Unit

ASIO's Business Liaison Unit (BLU) provides an interface between ASIO and Australia's private sector. The BLU distributes unclassified security reporting to businesses in Australia to enable them to understand better the security environment and the threats they face, and to provide them with a basis for security planning.

The BLU draws from the full range of ASIO's information holdings and expertise, including the National Threat Assessment Centre (NTAC), ASIO's Critical Infrastructure Protection area, and international liaison reporting. It sanitises intelligence and distributes it as unclassified Business Security Reports for specific industries (e.g. oil and gas, transport, banking and finance) and also provides a range of other general security and incident reporting.

BLU reports are made available via a secure website offered free to businesses on a subscription basis. Subscribers also receive a quarterly BLU Bulletin, which provides news and updates about ASIO's work.

At the end of the reporting period there were 398 subscribers to the BLU website – compared to 247 in 2006–07 – with significant interest shown from the transport sector (aviation, maritime, freight, and mass-transit), the energy and resources sector (exploration, production, consulting engineering), banking and finance, telecommunications, stadium operators, shopping centres, property management and utilities.



The BLU currently has 140 Business Security Reports available on its website – compared to 55 in 2006–07. Reporting covers domestic security, overseas security, information protection, the security environment, incident and major event briefings and a range of other general interest security topics.

The BLU works closely with Commonwealth agencies responsible for the protection of critical infrastructure and transport security, as well as with State and Territory Governments. Its engagement with the Australian business community, both in Australia and overseas, is extensive. In 2007–08, ASIO participated in 17 forums and contributed to two trade journals.

In 2007–08, the BLU coordinated 10 ‘Executive Program’ meetings between the Director-General of Security and company CEOs.

In concert with NTAC, the BLU is developing a Register of Australian Interests Overseas. This important initiative will enable ASIO to identify how emerging threats might impact upon Australian business infrastructure overseas. Through knowing where Australian business interests are located overseas ASIO will be in a position to warn companies of relevant threats.

## 1.5 ASIO’s Involvement in Criminal and Civil Litigation

ASIO provides information to support terrorism prosecutions, civil litigation and review of administrative decisions. Sometimes the information sought from ASIO has been obtained through sensitive collection techniques or liaison relationships. ASIO aims, therefore, to balance the need to protect its sources, methods, and liaison partnerships with the need to support prosecutions and legal processes. Demand for such material, both from government legal representatives and from defendants and applicants, has significantly increased.

### ASIO’s Involvement in Litigation

In 2007–08, ASIO was involved in over 60 litigation matters. They ranged from security-related criminal proceedings (including terrorism prosecutions), to judicial and administrative reviews of security assessments, to civil actions. Although growth in the overall number of legal proceedings involving ASIO stabilised – with figures comparable to 2006–07 – the workload increased substantially as a number of cases moved from the charge phase to prosecution.

ASIO’s significantly increased involvement in court processes has led to a range of related demands. During 2007–08, ASIO provided many thousands of pages of its product in response to subpoenas, in addition to hundreds of hours of recorded conversations and multiple still and filmed images.

In 2007–08, trial proceedings commenced in Sydney and Melbourne against individuals charged with terrorism and other offences resulting from police and ASIO operations that culminated in 2005. These operations have become known by the police codename, “Pendennis”. The Pendennis prosecutions are the largest terrorism prosecutions in Australian history. The use of ASIO intelligence as evidence has resulted in ASIO documents being produced, including in witness statements and in response to numerous subpoenas.

ASIO was directly involved in two actions in 2007–08 initiated by Mr Mamdouh Habib – a challenge by way of administrative review to the Director-General of Security’s assessment of Mr Habib as a risk to security and Mr Habib’s lawsuit against the Commonwealth alleging defamation and negligence. In November 2007, the Administrative Appeals Tribunal upheld the adverse security assessment and in April 2008 the Federal Court

rejected Mr Habib's allegation that he was interrogated in the Australian High Commission in Islamabad in 2001. Mr Habib has appealed these decisions. ASIO's role in these proceedings has been significant and resource intensive.

During the reporting period, ASIO was also subpoenaed in Mr Habib's defamation lawsuit against Nationwide News. In March 2008 the NSW Supreme Court dismissed this defamation claim. Mr Habib has appealed the Court's decision.

The prosecution of Mr Matthew Francis O'Ryan and former ASIO officer Mr James Seivers, for unauthorised communication of national security intelligence proceeded to trial during the reporting period. Of the Crown witnesses, a number were ASIO officers. The jury was unable to reach a unanimous verdict and the Commonwealth Director of Public Prosecutions (CDPP) has indicated that he will retry both Defendants.

To support effectively terrorism prosecutions – and to meet legal needs across ASIO – a Legal Division was created in July 2007. ASIO continued to invest in the growth of its legal team throughout 2007–08.

ASIO is reviewing its policies and procedures to ensure operational practices minimise organisational vulnerabilities where intelligence product is likely to be used as evidence. Lessons learnt from recent prosecutions have been integrated into operational policies and practices.

## Protecting ASIO's Capabilities and Information

ASIO's priority investigations often occur in uncertain and rapidly evolving environments. These investigations frequently rely on highly sensitive collection capabilities, including human sources and technical operations.

Extremists internationally have increased their broad knowledge of intelligence methodologies in recent years. This has led to many operating in a more sophisticated way, making them more difficult to monitor.

A key objective in ASIO's intelligence operations is protection of life and property. Where the best means to achieve this is through prosecution for terrorism or other offences, ASIO information may be called upon to assist. There are significant challenges in transforming intelligence into evidence for legal proceedings. ASIO seeks to support the requirements of open justice, while at the same time protecting its collection capability.

Requests by police or the CDPP to use ASIO material as evidence are considered carefully by ASIO, and in the majority of cases ASIO is able to assist. Some of the material ASIO provides must, because of its sensitivity, retain a national security classification. This material is generally provided in closed court and, where the Court so determines, does not form part of the publicly available record of the trial.

ASIO has worked closely with the legal community to ensure suitable arrangements are in place to protect the identity of ASIO witnesses. Unauthorised identification of ASIO officers and employees is an offence under section 92 of the ASIO Act. Disclosure in any public forum, including courts, may lead to increased intelligence targeting of staff by foreign intelligence agencies, politically motivated groups, issue motivated groups and others who seek to gain unofficial access to ASIO or otherwise threaten officers' well being.

## Output 2: Protective Security Advice

### Output at a glance

ASIO provided protective security advice to government departments and agencies through its counter-terrorism and personnel security assessment functions. Physical security advice was also provided to the government and private sector agencies through ASIO's T4 protective security group. ASIO played a leading role within the Australian Government in the development of security-related policy.

ASIO completed 89,290 counter-terrorism assessments in the reporting period. This was a decrease of 34% from 2006–07, reflecting a decline in the requirement for new Aviation and Maritime Security Identity Cards. No adverse or qualified security assessments were issued and 99% of counter-terrorism assessments were completed within 10 days.

ASIO completed 21,386 personnel security assessments, a slight increase on 2006–07. This reflected a long-term growth trend in ASIO's personnel security assessment workload. Two qualified personnel security assessments were issued.

ASIO provided high quality protective security advice to a range of government agencies and private sector clients on a cost recovery basis. In 2007–08, ASIO completed 10 Protective Security Risk Reviews and Vulnerability Assessments, with efforts focused on Australia's major airports and critical infrastructure rated as 'vital'. ASIO also certified 57 new Australian Top Secret sites and conducted technical surveillance countermeasures tests to protect government sites from unauthorised monitoring.

The Australian Government Contact Reporting Scheme identified attempts to gain unauthorised access to sensitive government information. The number of contact reports reached a plateau this year, following several years of steady growth. To enhance the effectiveness and reach of the scheme, ASIO will promote it to State and Territory agencies in 2008–09.

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

## ASIO's Role in Counter-Terrorism and Personnel Security Assessments

One of ASIO's core functions is to provide security assessments to Commonwealth agencies to assist them determine whether an individual should have access to controlled places, information, or materials. ASIO provides:

- counter-terrorism security assessments, which provide advice to agencies needing to limit access to controlled materials or places; and
- personnel security assessments to assist government departments and agencies in deciding whether to grant individuals access to national security classified information.

In conducting a security assessment, ASIO takes into account matters such as the activities, associates, attitudes, and character of the individual, as these relate to 'security' as defined in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

On completion of an assessment ASIO provides either:

- a non-prejudicial assessment, meaning no issues of concern have been identified;
- a qualified assessment that does not recommend against access but includes information ASIO considers may be relevant to the agency's decision and may help minimise risk; or
- an adverse assessment that recommends against access.

Requesting agencies determine the applicant's suitability for access on the basis of ASIO's security assessment advice, as well as their own enquiries. The final decision of whether or not to grant access always rests with the requesting agency.

In instances where ASIO has issued a qualified or adverse assessment, applicants are notified in writing and have a right of appeal to the Administrative Appeals Tribunal (AAT).

### 2.1 Counter-Terrorism Security Assessments

ASIO's counter-terrorism security assessments are carried out at the request of government authorities who are responsible for accreditations, usually the Australian Federal Police (AFP) and AusCheck. Established in 2007, AusCheck is a division of the Attorney-General's Department with responsibility for coordination and assessment of background checks for Aviation Security Identity Cards (ASICs) and Maritime Security Identity Cards (MSICs).

ASIO completed 89,290 counter-terrorism security assessments in 2007–08 (see Table 5), 99% of which were completed within 10 days. These assessments included:

- 70,084 security assessments for ASICs for pilots, trainee pilots, air crew, and persons requiring access to controlled areas at airports, and MSICs for sea vessel crew and persons requiring access to controlled areas at sea ports (see also p. 20);
- 4,502 security assessments for persons requiring licences to access ammonium nitrate;
- 1,251 security assessments for staff and visitors to the Australian Nuclear Science and Technology Organisation (ANSTO) facility at Lucas Heights, Sydney; and
- 13,453 security assessments for persons requiring accreditation for special events such as the Asia-Pacific Economic Cooperation (APEC) forum and World Youth Day (WYD).

## Adverse and Qualified Security Assessments

No adverse or qualified security assessments were issued as a result of counter-terrorism security assessments during 2007–08, although a number of detailed investigations were initiated.

### Trends

There has been steady growth in ASIO's counter-terrorism security assessment responsibilities since 2003–04, although variations in workload from year to year have been marked. For example, in 2007–08 a substantial reduction in requests for new ASIC and MSIC checks led to an overall decline of 34%. The variation has also been driven by the introduction of additional categories of checking (such as ammonium nitrate access) and surges in the lead up to major events. This is likely to continue for the foreseeable future.

Type of assessment	2003–04	2004–05	2005–06	2006–07	2007–08
Aviation/Maritime Security Identity Cards	58,147	38,466	71,733	118,118	70,084
Ammonium Nitrate	-	1,634	7,428	6,419	4,502
ANSTO	-	-	-	1,027	1,251
Commonwealth Games	-	-	56,149	-	-
G20 Finance Ministers' Meeting	-	-	-	1,580	-
APEC and WYD	-	-	-	7,837	13,453
<b>Total</b>	<b>58,147</b>	<b>40,100</b>	<b>135,310</b>	<b>134,981</b>	<b>89,290</b>

Table 5: Counter-terrorism checking 2003–04 to 2007–08

## 2.2 Personnel Security Assessments

ASIO provides personnel security assessments to assist government departments and agencies in deciding whether to grant access to national security classified information. Applicants for security clearances must provide detailed background information to their sponsoring agency and ASIO. ASIO's personnel security assessments take into account intelligence information held by ASIO, as well as known risk factors. ASIO completed 21,386 personnel security assessments in 2007–08, which continued a long-term trend of growth in the overall personnel security assessment workload.

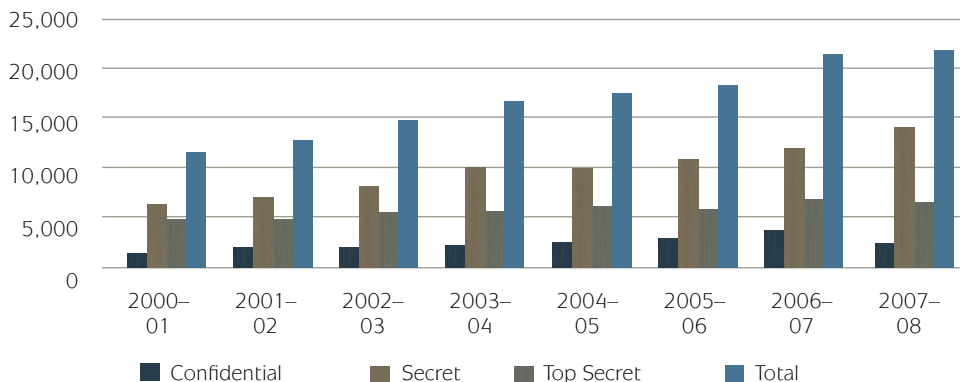


Figure 1: Personnel security assessments 2000–08

## Adverse and Qualified Assessments

Two qualified personnel security assessments were issued during the year. These assessments provided information to assist the respective departments in managing potential risks. ASIO also initiated a number of detailed investigations for personnel security assessment applicants in 2007–08.

Adverse or qualified personnel security assessments may be appealed to the AAT. There were no appeals in 2007–08.

## 2.3 Physical Security

ASIO provides protective security advice to the Australian Government, and with approval from the Attorney-General, to State and Territory Governments and private sector companies.

Within ASIO, T4 is the primary area that provides protective security advice. T4's role is derived from section 17(1)(d) of the ASIO Act. Unlike other parts of the ASIO Act, this section does not limit ASIO's advice to matters contained within the definition of 'security' in section 4 of the ASIO Act. This section was added to ASIO's legislative functions in 1986 in response to recommendations by the Hope Royal Commission and in recognition of the broader utility of the protective security advice that ASIO can provide. In practice, the majority of T4's advice is directed towards protection from terrorism, espionage and sabotage.

ASIO's protective security advice services are provided on a cost recovery basis and include:

- Protective Security Risk Reviews;
- vulnerability assessments;
- Ministerial office security;
- certification of Top Secret facilities;
- technical surveillance countermeasures (TSCM) testing;
- protective security and risk management training; and
- evaluation of security equipment, security consultants, locksmiths, couriers and classified waste services.

### Protective Security Risk Reviews and Vulnerability Assessments

ASIO provides Protective Security Risk Reviews and vulnerability assessments for government and industry clients. Protective Security Risk Reviews assess physical, information, administrative and personnel security risks. Vulnerability assessments assist clients to identify weaknesses in their existing protective security arrangements. ASIO recommendations are often used by clients as the basis for engaging private industry security consultants, who are best placed to implement protective security solutions suggested by ASIO.

In 2007–08, ASIO completed 10 Protective Security Risk Reviews and/or vulnerability assessments, with efforts focused on critical infrastructure rated as 'vital' and Australia's major airports.

### Top Secret Site certifications

The *Australian Government Protective Security Manual* produced by the Attorney-General's Department mandates ASIO as the certifying authority for Australian Top Secret facilities. Re-certification of these sites is required every five years.

ASIO certified 57 sites in 2007–08.

## Technical Surveillance Countermeasures Testing

ASIO's TSCM testing protects classified and sensitive discussions from unauthorised monitoring. It includes electronic surveys, monitoring of premises for possible hostile electronic activity, and physical security inspections.

Demand for TSCM testing remained high in 2007–08.

## Protective security and risk management training

In 2007–08, ASIO assisted the Protective Security Coordination Centre with five training courses for government security practitioners. ASIO also twice conducted its separate specialised course – *Practical Application of Protective Security within Government*. As part of the annual Security in Government Conference, ASIO hosted a special briefing in December 2007 for Commonwealth Agency Security Advisers.

## Evaluation of security equipment and consultants, locksmiths, couriers and classified waste services

The *Australian Government Security Equipment Catalogue* lists security products that have been approved for use in government applications. On behalf of the Interdepartmental Security Construction and Equipment Committee (SCEC), ASIO tests and evaluates security products. In 2007–08, ASIO conducted 74 such evaluations.

ASIO also evaluates private industry security practitioners to determine their suitability as SCEC-endorsed security consultants. Prequalification and experience requirements were increased during 2007–08, to ensure consultants maintained high standards. ASIO delivered two evaluation courses in 2007–08, with nine consultants gaining SCEC endorsement and a further 21 consultants being re-certified under a refresher program.

ASIO also evaluates locksmiths who work with SCEC-endorsed security containers and locks. In the reporting period, 27 locksmiths were recommended for SCEC endorsement.

In consultation with stakeholders ASIO reviewed the requirements for high-security alarm systems that are used to protect national security material and assets. As a consequence, new specifications were issued in March 2008.

## Cost recovery

ASIO recovered \$1,109,264 in costs for protective security advice and services in 2007–08.

## 2.4 Policy Contribution

### Inter-Agency Security Forum

The Inter-Agency Security Forum (IASF) was established as a result of the *Inquiry into Security Issues* conducted in 2000 by the then Inspector-General of Intelligence and Security, Mr WJ Blick AM PSM. It provides a consultative forum on security issues for the Australian Intelligence Community (AIC) and related policy departments. ASIO provides the chair and secretariat for the IASF and its three expert working groups – on personnel, information management, and physical and administrative security.

ASIO promoted a more strategic and critical agenda for the IASF in 2007–08. Its work program included:

- analysing emerging issues for government protective security regimes;
- reviewing and streamlining requirements for Top Secret Positive Vet clearances;
- a self-evaluation review; and
- a review of annual security status reporting to Government.

### **Annual reporting on the security status of IASF agencies**

As IASF chair, ASIO produces an annual overview report on the protective security status of IASF agencies. The 2006–07 report covered aspects of physical, information and personnel security. It noted that the IASF continues to establish and maintain security best practice through inter-agency engagement and policy development.

### **Contact Reporting Scheme**

The *Australian Government Protective Security Manual* requires Australian Government employees to report suspicious, unusual, or persistent contact with foreign nationals as part of the Australian Government Contact Reporting Scheme. The reporting scheme is particularly valuable to ASIO in its efforts to identify attempts to gain unauthorised access to sensitive information.

The number of reports received reached a plateau this year, following several years of growth. ASIO promotes the scheme with a program of presentations – 98 were provided during the period – but expected a natural peak would be reached. In 2008–09, ASIO will promote the scheme to State and Territory agencies.



## Output 3: Security Intelligence Investigations and Capabilities

### Output at a glance

ASIO enhanced further its national capacity for physical surveillance with the recruitment of additional Surveillance Officers.

All security intelligence warrant requests put to the Attorney-General were approved. No questioning warrant or questioning and detention warrants were requested.

ASIO enhanced its capability for complex and advanced analysis and introduced new analytical techniques to sort and exploit data. Specialised training was provided for Intelligence Officers and Intelligence Analysts.

ASIO participated in a series of counter-terrorism exercises designed to test security preparations for World Youth Day (WYD) 2008, and to practice national counter-terrorism arrangements. ASIO also participated in two counter-terrorism exercises with international partners.

ASIO's liaison relationships with its national partners continued to be strong and effective. ASIO expanded its network of overseas liaison offices. ASIO had 311 approved liaison relationships with international partner agencies in 120 countries.

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

### 3.1 Maintenance and Enhancement of All-Source Security Intelligence Collection Capability

As a collection and analysis agency, ASIO draws on information from a variety of sources – both classified and unclassified – to assist in identifying, providing advice on, and responding to threats to Australia's security. This information may be drawn from:

- open sources;
- physical surveillance;
- human source intelligence;
- technical collection sources; and
- special powers operations under warrant.

Individual collection capabilities usually only provide partial insights. Analytical judgements or intelligence pictures are typically built on information from multiple sources. Each intelligence challenge is unique, and requires a flexible – and often innovative – use of resources.

In employing its intelligence collection capability, ASIO's activities are governed by the principle of proportionality – the means for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence. Inquiries and investigations into individuals and groups are undertaken with as little intrusion into individual privacy as possible. Consistent with this graduated approach, the more intrusive the investigative technique, the higher the management level required to approve its use. The principle of proportionality is reflected in *Attorney-General's Guidelines* which were updated and re-issued during the reporting period.

ASIO's access to information and intelligence collection capability is crucial for building a comprehensive and accurate picture of the threat environment, for managing identified threats and to identify threats that are not yet known. As such, ASIO devotes considerable resources to the development, maintenance, and enhancement of its ability to collect intelligence, and is careful to protect sources and methods.

ASIO's partnerships – both within Australia and internationally – are a collection multiplier. They provide ASIO with access to information and capabilities that it could not replicate on its own.

#### Open Source Intelligence

Open sources provide a wealth of information. International news services provide continuous, near real-time, monitoring of global events. Publications, the Internet and databases can provide valuable input to ASIO's analytical and investigative work. Managing the sheer volume of publicly available information can, however, be challenging, and the veracity of information in the public domain must often be tested against other sources.

Specialised open-source support to analysis and operational activity is provided by ASIO's Research and Monitoring Unit (RMU). The RMU operates on a 24/7 basis, and is also ASIO's conduit for time-sensitive reporting of security-related information – both classified and unclassified – including from ASIO's overseas liaison offices, the National Security Hotline and elsewhere.

#### Physical Surveillance

Physical surveillance is resource intensive. It remains, nonetheless, an essential capability. During the reporting period ASIO introduced an improved national surveillance tasking system to strengthen management of surveillance assets. The improved system ensures priority investigations are adequately resourced and helps planning for future contingencies.

A nationwide Surveillance Officer recruitment campaign began in February 2008, and was aimed at expanding further ASIO's surveillance capability. Interest in the positions was high.

## Human Source Intelligence Collection

Human sources provide a unique window into the activities, attitudes, thoughts and intentions of individuals, groups or communities. Unlike other ASIO collection capabilities, which tend to be passive in nature, human sources are active collectors and are a particularly sensitive capability.

### Community contact and interviews

Complementing covert human source intelligence collection, ASIO also conducts interviews with members of the public and individuals of interest. These interviews assist in intelligence collection and resolving leads, and they provide background and context for specific investigations.

### Technical Collection Sources

Technically derived intelligence contributes significantly to ASIO's security intelligence collection. Technical intelligence collection may be conducted as part of ASIO's special powers operations (such as telecommunications interception).

### Telecommunications interception capabilities

The cooperation of telecommunications carriers and carriage service providers (C/CSPs) is central to the ability of each of the lawful interception agencies – including ASIO – to intercept communications. Under the *Telecommunications Act 1997* (the Telecommunications Act), C/CSPs are required – at their cost – to develop, install and maintain interception capabilities, unless specifically exempted. The Telecommunications 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, on a cost-recovery basis.

ASIO is the Attorney-General's designated 'lead house' in managing the development of interception and delivery capabilities for use by Commonwealth, State and Territory law enforcement agencies. ASIO works closely with the telecommunications industry to ensure comprehensive interception capabilities are available. As 'lead house' ASIO:

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

ASIO continued to work closely with the Attorney-General's Department, the Department of Broadband and the Digital Economy, and the Australian Communications and Media Authority, on policy issues with implications for telecommunications interception.

### Special Powers Operations Under Warrant

ASIO's governing legislation permits it – subject to a warrant approved by the Attorney-General – to use methods of investigation such as telecommunications interception and access, listening devices, entry and search of premises, computer access, tracking devices and examination of postal and delivery service articles.

ASIO's use of warrant powers is guided strictly by the principle of proportionality – the means for obtaining information must be proportionate to the gravity of the threat. This is required by the *Attorney-General's Guidelines*.

With the Attorney-General's consent, ASIO is also able to seek a warrant from an independent issuing authority (a Federal Magistrate or Federal Judge) to compel a person to appear before a prescribed authority (a former Federal Judge, current State Judge or the President or Deputy President of the Administrative Appeals Tribunal) to answer questions relating to terrorism matters. Any questioning pursuant to a warrant must be conducted in the presence of a prescribed authority under conditions determined by the prescribed authority. The Inspector-General of Intelligence and Security may attend any questioning or detention under the warrant. In 2007–08, no questioning or questioning and detention warrants were issued (see Appendix B).

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

ASIO warrants are issued for specified periods. At the expiry of each warrant, ASIO must report to the Attorney-General on the extent to which the operation helped ASIO carry out its functions.

The number of active warrants varies in response to changes in the security environment. All warrant requests put to the Attorney-General in 2007–08 were approved.

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

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

## ASIO's Security Intelligence Priority Setting Arrangements

ASIO has a priority-setting framework that is rigorous, comprehensive and accountable. It is founded on the management of risk, regular critical review and flexible allocation of resources in a fast-paced threat environment. The framework is specifically tailored for Australia's security intelligence arrangements, particularly considering that:

- the *Australian Security Intelligence Organisation Act 1979* effectively provides a set of strategic level priorities in its definition of 'security';
- because security intelligence routinely involves information about Australian citizens, privacy principles must be observed, particularly as information collected by ASIO will often confirm the absence of ill-intent rather than threat; and
- ASIO is both a collector and assessor of intelligence, so a major customer of ASIO's collection work is its own analytical and investigative areas.
- At a strategic level, ASIO's priorities are set by the Intelligence Coordination Committee (ICC). The ICC is chaired by a Deputy Director-General and comprises ASIO's senior management team involved in the intelligence process.

In the event of a quickly emerging and potentially imminent threat, the ICC will meet out-of-session to determine immediate investigative objectives, identify other agencies that need to be alerted to the threat, and, if required, coordinate a joint operational response.

## 3.2 Complex Tactical and Technical Analysis

With a more complex security environment and the widespread use of computers and information technology, the range and volume of data collected by ASIO is increasing rapidly. This will continue for the foreseeable future.

ASIO needs to be able to exploit, sort and display this data quickly to identify trends, incidents, and indicators of activities of security concern. There is a high priority, therefore, on the development of complex analysis methods utilising new techniques and technologies.

Complex analysis capability development is focused on:

- collating, searching and sorting unstructured text data, typically obtained from written documents and computer files, and in a variety of formats and languages; and
- working with data to detect events, patterns and linkages that are significant but not obvious.

These new approaches to investigative analysis do not replace traditional methods. Rather, they augment them by allowing ASIO to manage a greater range and quantity of information. They also provide new avenues for advancing investigations.

Effective use of complex analysis tools requires continual enhancement of information technology capabilities, and advanced training of Intelligence Analysts and Intelligence Officers. ASIO is meeting these challenges through enhanced in-house training programs and ongoing development of information technology infrastructure. ASIO has co-located its analysts working on complex analysis with information technology officers. This allows software to be adapted in real-time in response to new challenges and helps information technology specialists identify and develop new analysis capabilities.

ASIO's capabilities for undertaking complex and advanced analysis were enhanced in 2007–08. ASIO adapted and applied numerical and statistical techniques for analysing structured data sets to help resolve complex investigative and analytic problems.

In 2007–08, ASIO also commenced projects, using advanced analytical techniques, to provide more comprehensive data exploitation of immigration-related information that is available to ASIO. This will inform the Next Generation Border Security initiative.

ASIO's tactical financial investigation and analysis capability also continued to develop, providing increased support to security intelligence investigations.

ASIO seeks to leverage the expertise of others as a way of enhancing its complex analysis capability. For example, ASIO works with the Defence Science and Technology Organisation (DSTO) on emerging technologies and analysis techniques, participates in user groups and engages with software vendors.

## 3.3 Technical Research and Development

ASIO's considerable investment in research and development helps provide secure, timely and specialised capabilities. Research and development also supports operational capability and underpins development of new capabilities

ASIO's research and development is underpinned by:

- in-house research and development;
- collaboration with Australian partners;

- engagement with industry and academia; and
- a broad-based program of human resource development.

### Defence Science & Technology Organisation

In 2008, ASIO and DSTO renewed a Memorandum of Understanding (MoU) under which DSTO provides scientific and technological support to ASIO. A senior DSTO officer is a full member of ASIO's Research and Development Committee (see also p. 57).



As part of broader research and development work across Government, ASIO is a member of the Publicly Funded Agencies Collaborative Counter-Terrorism group. Through this forum, ASIO helps prioritise counter-terrorism work conducted by publicly funded scientific and research agencies.

### Engagement with Industry and Academia

ASIO established a new position of Science Adviser during the reporting period. The Science Adviser pursues ASIO's Research and Development interests through strategic engagement with industry, academia and government funded research agencies such as DSTO.

## 3.4 Counter-Terrorism Response

ASIO's contribution to national counter-terrorism response arrangements is an important element of Australia's overall counter-terrorism capability.

Counter-terrorism response arrangements centre on the National Counter-Terrorism Committee (NCTC). The NCTC – established in 2002 under the *Inter-Governmental Agreement on Australia's National Counter-Terrorism Arrangements* – is responsible for whole-of-government counter-terrorism policy coordination and national counter-terrorism arrangements, including Australia's National Counter-Terrorism Plan (NCTP).

The NCTC is supported nationally by a number of other bodies including inter-departmental committees and subject-specific working groups. ASIO is a member of several of them, including:

- the Australian Government Counter-Terrorism Policy Committee (AGCTPC) which is chaired by the Department of the Prime Minister and Cabinet and is responsible for coordinating strategic policy on counter-terrorism issues. ASIO provides regular security environment briefings to this body; and
- the Australian Government Counter-Terrorism Committee (AGCTC) which is chaired by the Protective Security Coordination Centre and which regularly reviews the national counter-terrorism alert level.

The NCTP identifies four key components of counter-terrorism activity – prevention, preparation, response and recovery.

Under the NCTP, ASIO is responsible for:

- the National Intelligence Group, which coordinates and disseminates intelligence to support operational commanders and senior government decision-makers in the event of a major terrorist incident, or in support of Inter-departmental Emergency Taskforce arrangements;
- leading a multi-agency Forward Intelligence Analysis Team that would be deployed overseas in response to a terrorist incident in another country; and
- maintaining a capability to deploy intelligence support overseas.

### **The Technical Support Unit**

ASIO's Technical Support Unit (TSU) can be deployed under the NCTP framework to assist Commonwealth or State or Territory authorities in response to a terrorist incident. The TSU provides technical support to the commander managing the incident and technical units gathering covert intelligence at the scene. ASIO can also provide support directly to operational commanders through deployment of intelligence officers and supporting staff to the Joint Intelligence Group and Police Forward Command Post, which would be located at or near the site of a terrorist incident.

### **Training and Exercises**

The NCTC coordinates training courses and exercises. Exercises bring together Commonwealth and State and Territory law enforcement and emergency management agencies to test and improve response arrangements across jurisdictions and organisations.

The NCTC's training program includes:

- the Joint Intelligence Group Officer Skills Enhancement Course (JIGOSEC), which aims to enhance skill levels and understanding of intelligence processes and structures under NCTC arrangements; and
- the Intelligence Analysis Skills Enhancement Course (INTASEC), designed to give primarily state-based analysts enhanced skills and familiarisation with analytical tools.

ASIO provides instructors and students to these courses. In 2007–08, ASIO was involved in four JIGOSEC courses and two INTASEC courses.

During the reporting period, ASIO also participated in a series of counter-terrorism exercises designed to test security preparations for World Youth Day 2008, and to practice national counter-terrorism arrangements. Exercises were held in New South Wales, Tasmania, the Australian Capital Territory, Victoria, South Australia and the Northern Territory.

During these exercises ASIO tested interoperability in a multi-agency environment, particularly intelligence arrangements and information flow under the NCTP and National Counter-Terrorism Handbook.

ASIO also participated in two international counter-terrorism exercises with international partners.

### 3.5 National Liaison

One of ASIO's strengths is that it functions effectively in, and contributes to, several different environments – domestic and international, Commonwealth and State, and intelligence and law enforcement. ASIO's relations with State and Territory police services – themselves an integral and critical component of Australia's counter-terrorism capability – are close and long-standing. ASIO also cooperates and collaborates extensively with other departments and agencies, particularly, the AIC and key operational partners.

Coordination of effort between ASIO and its Australian Government partners occurs through:

- meetings and informal contacts, including regular agency-head level Senior Management Meetings;
- attachments and exchange of officers (see p. 48); and
- collaborative efforts such as the National Threat Assessment Centre.

#### Engagement with Law Enforcement Agencies

ASIO's partnerships with law enforcement agencies continued to be strong and effective throughout 2007–08. Engagement with police is constant, and a routine aspect of business across ASIO's investigative, analytical and operational areas.

ASIO and AFP senior executives (led by the Director-General of Security and the AFP Commissioner) meet for strategic-level discussions, with a focus on counter-terrorism activities.

The Director-General of Security also regularly meets State and Territory Police Commissioners through the year and is a member of the Australian Crime Commission Board. Through visits and NCTC meetings senior level liaison also occurs between ASIO's Deputy Directors-General and their State and Territory police counterparts.

ASIO holds quarterly law enforcement intelligence updates in ASIO's Canberra Office. This provides a forum for senior police engaged in counter-terrorism from all jurisdictions to meet with ASIO officers and discuss priorities and emerging issues.

At the operational and tactical levels, ASIO and the police work closely together through:

- executive meetings in ASIO's State and Territory offices to discuss operational and tactical issues;
- meetings between ASIO and police officers to discuss relevant cases;
- the attachment of ASIO officers to State or AFP offices at times of high operational tempo; and
- regular meetings in Canberra between ASIO and AFP Senior Executive Service counter-terrorism managers to discuss emerging issues.

ASIO regularly provides places for police officers on specialised ASIO training courses. ASIO officers also attended courses hosted by the AFP and State and Territory police services.

As a result of the *Review of Interoperability between the AFP and its National Security Partners* by Sir Laurence Street AC KCMG QC – which was delivered during the reporting period – ASIO and the AFP began implementing



during 2007–08 a number of measures to promote further cooperation and information sharing. These included:

- a Chief Executive Interoperability Forum comprising the Director-General of Security, the Commissioner of the AFP, and the Commonwealth Director of Public Prosecutions (CDPP);
- a National Counter-Terrorism Protocol between ASIO and the AFP;
- Counter-Terrorism Prosecution Guidelines to formalise the role of CDPP in the early stages of investigations;
- placement of ASIO officers in the Joint Counter-Terrorism Teams in Sydney and Melbourne;
- a working group to develop joint training programs; and
- an AFP-ASIO executive-level staff exchange.

### **National Technical Cooperation**

Consistent with its ‘lead house’ role in telecommunications interception, ASIO continued to coordinate priorities for developing interception and delivery capabilities with the 14 Australian intercepting law enforcement agencies (ILEAs). In this role ASIO works closely with the ILEAs on a range of associated matters. Representatives of each agency and the Attorney-General’s Department meet quarterly.

ASIO liaises routinely with Australian Government departments responsible for telecommunications and interception (the Attorney-General’s Department and the Department of Broadband, Communications and the Digital Economy) as well as with the industry regulator, the Australian Communications and Media Authority.

## **3.6 International Liaison**

International liaison relationships are a force multiplier for ASIO. They enable it to draw on the information, expertise and capability of other services (both operational and analytical) and to pursue investigations that – as is often the case – cross international boundaries. Onshore threats can move quickly offshore, and vice-versa. ASIO officers deployed overseas are able to respond quickly to threats that have international linkages, and feed intelligence into ASIO’s 24/7 National Threat Assessment Centre and other operational areas.

ASIO’s capability to pursue threat-related information globally is crucial to its ability to identify new or emerging threats, and to provide advice on known threats. It is an important part of Australia’s border protection regime.

As threats can arise quickly and from a diverse range of sources there is significant value in maintaining international relationships over the longer-term, rather than building them from a low base in a time of crisis.

As at 30 June 2008, ASIO had 311 approved liaison relationships with international partner agencies in 120 countries.

### **Foreign Representation in Australia**

In 2007–08, there were visits to Australia by representatives from international partner agencies. These ranged from analytical-level exchanges to Heads of Service visits.

The Director-General of Security visited international partner agencies overseas.

## **International Exchange and Training**

ASIO provides training to overseas intelligence and security agencies. Established in 2005, the Counter-Terrorism Intelligence Training Program (CTITP) provides counter-terrorism training and capability building.

## Output 4: Foreign Intelligence Collection

### Output at a glance

Foreign intelligence deals broadly with the capabilities, intentions or activities of a foreign power. It can relate to threats against the security of Australia, but it mainly extends beyond threats into broader political, economic, and diplomatic matters. Australia's dedicated foreign intelligence collection agencies are the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO).

ASIO collects foreign intelligence in Australia under warrant and incidentally through human sources. The responsibility for foreign intelligence collection under warrant was given to ASIO as a result of the second Royal Commission into the Australian Intelligence Community (AIC) conducted by Justice Robert Hope – the Royal Commission on Australia's Security and Intelligence Agencies. Justice Hope concluded that legal authority for the collection of foreign intelligence within Australia should be given to ASIO, in recognition of the fact that "ASIO is the only service which has been given special statutory powers to collect intelligence within Australia, with the warrant of the Attorney-General, in ways which, without such a warrant, would involve a breach of Australian law."

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



# PART 3

---

CORPORATE MANAGEMENT AND  
ACCOUNTABILITY



## Corporate Management and Accountability – Enabling Functions

As at 30 June 2008, ASIO's total staffing was 1,492. This was 20% short of the target for the year, reflecting a tightening labour market and an increase in ASIO's separation rate. Nonetheless, staffing is above ASIO's overall growth target, and ASIO is confident it will reach its 2010–11 target of 1,860 staff. ASIO continued to focus on recruiting high-calibre staff through innovative recruitment campaigns.

In 2007–08, ASIO invested \$6.4m in staff learning and development, an increase of \$1.5m on 2006–07. ASIO established a Training Branch and introduced a Learning and Development Strategy to provide specialised training in areas such as operations, administration, and leadership.

ASIO implemented new and refreshed human resource policies to reflect the contemporary employment environment. These included improvements to the staff performance management system and the introduction of a New Employee Support Officer (NESO) scheme to assist new employees adjust to ASIO's specialised work environment.

ASIO upgraded a number of IT facilities, rolled-out new support software, achieved greater connectivity, and made enhancements to audio-visual facilities.

ASIO received 530 public applications for access to records, down from 582 applications in 2006–07. However the total number of folios (pages) examined was 63,932, up from 52,234 in 2006–07. In addition, ASIO contributed to a whole-of-government effort to assess and release the reports and records of the Royal Commission into Intelligence and Security (1974–1977) (the Hope Royal Commission), which totalled 26,597 folios.

In the 2007–08 Federal Budget the Government approved additional funding for a new purpose-built facility in Canberra to accommodate ASIO's Central Office. Design work progressed during 2007–08, and a secure site office was established to accommodate the project team.

ASIO's growth has also put pressure on accommodation in its State and Territory offices. Significant progress continues to be made to deliver new and refurbished accommodation nationally. All new or refurbished office fit-outs endeavour to achieve an Australian Greenhouse Building Rating of at least four stars.

ASIO cooperated closely with, and provided comprehensive submissions to, several reviews and inquiries. These included the *Homeland and Border Security Review* (the Smith Review), *Review of Interoperability between the Australian Federal Police (AFP) and its National Security Partners* (the Street Review), and the *Inquiry into the Case of Dr Mohamed Haneef* (the Clarke Inquiry).

ASIO engaged with other departments and agencies on changes to a range of legislation, including telecommunications interception legislation – the *Telecommunications (Interception and Access) Amendment Act 2007*; and the *Telecommunications (Interception and Access) Amendment Act 2008*.

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

## People Development and Management

ASIO's success is contingent on the calibre of its people. ASIO needs officers who are intelligent, flexible, resilient, loyal and dedicated. They must be able to engage effectively with members of the broader Australian community, with business and other government agencies, and with ASIO's partners in Australia and around the world.

In an employment marketplace where people of ability, drive and commitment are highly sought after by public and private sector agencies alike, ASIO needs to be innovative and focused in its efforts to recruit those who have the qualities required for success in a security intelligence environment. And it needs to ensure that it retains such people by offering both a career with meaning, and a workplace that values its people and is satisfying beyond financial rewards.

### Recruitment

Following the 2005 review of ASIO resourcing by Mr Allan Taylor AM, the Government committed additional resources to enhance ASIO's capability in response to the contemporary threat environment. This will see ASIO grow to 1,860 staff by 2010–11.

The tightening employment market – and an increase in ASIO's separation rate from 5.5% in 2006–07 to 7.6% in 2007–08 – meant that ASIO fell short of its net growth target of 170 for the year. Total staffing reached 1,492 by 30 June 2008, up from 1,356 at 30 June 2007. ASIO remains confident it will achieve its 2010–11 target.

ASIO continued to refresh its recruitment marketing strategy to encourage strong responses to advertised vacancies. ASIO's image in the marketplace was enhanced through visually appealing composite advertisements and use of a broader range of innovative on-line, electronic and radio advertising. ASIO participated in more than 30 university and other careers fairs around the country. It also began receiving job applications via the Internet.

The overall cost of ASIO's advertising in 2007–08 was \$2.192m, up from \$2.126m in 2006–07.

ASIO employees – including many contractors and consultants – are usually required to hold a Top Secret (Positive Vetting) national security clearance. Assessing individuals' suitability for this security clearance is conducted in accordance with the *Australian Government Protective Security Manual* and its classified supplement. It is necessarily a thorough and lengthy process. ASIO aims to minimise the impact of the security clearance process on recruitment and in 2007–08 conducted an external review of recruitment and vetting practices. The efficiencies and process improvements identified are being implemented.



A selection of ASIO recruitment advertisements



## Staffing Profile and Workforce Diversity

Although ASIO staff are not employed under the *Public Service Act 1999*, the conditions of service are similar. ASIO uses the annual Australian Public Service (APS) *State of the Service* as a comparison benchmark.

ASIO's staffing profile compares favourably to the broader APS. Recruitment and promotion policies will continue to be based on merit while seeking to achieve an appropriate gender balance and diverse workforce.

At 30 June 2008, 88% of ASIO's total staffing of 1,492 was working on a full-time basis. This equates to a full-time staff equivalent (FTE) of 1,374.

Around 8% (or 120) of ASIO's staff were employed on a part-time basis compared to around 11% in the APS in 2006–07. Most part-time staff 84% (or 101) were women with around half being in the 35–44 year age group.

Recruitment of new staff over recent years has boosted the diversity of skills and experience within ASIO. While two-thirds of ASIO's staff currently have been with ASIO for less than five years, the injection of knowledge, skills and experience gained elsewhere in the public or private sectors have been of benefit.

The median age of ASIO's workforce has been decreasing steadily as a result of its growth, and is now 37 years (compared to the APS median of 42 years in 2006–07). The largest grouping continues to be in the 25–35 year age group (36%). The average age of ASIO's workforce is now 38.3 years, a decrease from 40 over the last five years. Approximately 28% of ASIO's workforce is aged over 45 years compared to 41% in the APS.

While women now make up 45% of ASIO's workforce – an improving trend – they remain under-represented in the Senior Officer ranks (35%) and Senior Executive Service (SES) ranks (16%) compared to the APS norms of 42% and 23% respectively.

Officers from non-English speaking backgrounds now comprise 16.5% of ASIO staff.

Workforce statistics are at Appendix C.

## Staff Training and Development

ASIO operates in a fast-paced and complex environment where mistakes can have grave consequences. ASIO staff must, therefore, be capable and well-trained. Training and staff development is particularly important in a growing workforce, and remained a high priority in 2007–08. As well as building relevant technical and specialist skills, ASIO's training programs seek to develop advanced management and leadership practices.

In 2007–08, ASIO invested \$6.4m in staff learning and development, an increase of \$1.5m on 2006–07. The additional investment reflects ASIO's focus on excellence and high-standards of professionalism.

During 2007–08, ASIO continued to implement recommendations from an evaluation of training and development strategies conducted during the previous reporting period. A Training Branch was established on 1 July 2007 and ASIO implemented a *Learning & Development Strategy* which provides the mechanisms to identify, develop, evaluate and report on the knowledge and skills required by ASIO staff.

ASIO continues to place a strong emphasis on developing its SES and Senior Officers. During 2007–08, leadership development was enhanced through a range of learning activities. Three all-of-SES forums were held over the reporting period to focus on managing key corporate issues. There was also two combined SES and Senior Officer forums.

ASIO introduced a new study initiative in 2007–08, to help build ASIO's strategic capability and develop specific tertiary-level skills. Under the program, high potential individuals will undertake post-graduate studies for up to one year on a full-time basis.

ASIO provides a range of specialised in-house training for Intelligence Officers and Intelligence Analysts. Courses include theory and practical components and cover issues such as interviewing skills, management of human source operations, operational tradecraft, analytical techniques, and the preparation of ASIO security intelligence and other reports. The demand for training for Intelligence Officers and Intelligence Analysts during 2007–08 was at its highest level in more than a decade.

In 2007–08, ASIO sent a number of officers overseas for skills development.

ASIO invests substantially in the development of language skills to support operations and investigations, and to enable ASIO officers to maximise their engagement with international partners.

ASIO supports strongly Australian Intelligence Community (AIC)-wide training efforts and in 2007–08, provided presenters on AIC-wide induction courses, including the *AIC Senior Officer Course* and *Working in the AIC* program.

In response to the Street Review, a Joint Training Committee comprising the AFP, the Commonwealth Director of Public Prosecutions (CDPP) and ASIO was established during the reporting period (see also p. 63).

## Attachments

ASIO continues to have a highly-developed officer attachment program and hosts a number of representatives from other organisations. This develops interoperability with other agencies in Australia and overseas, and encourages the sharing of skills, capability, knowledge and information. Table 6 outlines officers from other agencies hosted by ASIO, and ASIO staff similarly out-posted.

Agency	Staff to ASIO	Staff from ASIO
Australian Federal Police (AFP)	✓	✓
Australian Secret Intelligence Service (ASIS)	✓	✓
Australian Transaction Reports and Analysis Centre (AUSTRAC)	✓	
Defence Imagery and Geospatial Organisation (DIGO)	✓	
Defence Intelligence Organisation (DIO)	✓	
Defence Security Authority (DSA)	✓	
Defence Signals Directorate (DSD)	✓	✓
Department of Defence (DoD)	✓	
Department of Foreign Affairs and Trade (DFAT)	✓	✓
Department of Immigration and Citizenship (DIAC)	✓	
Department of Infrastructure, Transport, Regional Development and Local Government (DITRDLG)	✓	
Department of the Prime Minister and Cabinet (PM&C)		✓
Office of National Assessments (ONA)	✓	✓

Table 6: ASIO and other agency attachments

## Human Resource Policy and Practice

### Performance Management

Enhancements to ASIO's Performance Management Framework included greater automation of the performance management process and the introduction of a four-point rating system. These enhancements resulted in higher levels of compliance with around 93% of staff having a current performance agreement in 2007–08. A continuing high-level focus on performance management is expected to result in higher levels of compliance in 2008–09.

### Support for New Staff

In 2007–08, ASIO introduced a New Employee Support Officer (NESO) scheme to enhance and strengthen existing mechanisms for inducting and integrating new staff into ASIO. On commencement, each new employee is allocated a NESO who is drawn from outside the new employee's work environment, and whose role is to provide supplementary support during the settling-in period. Initial feedback indicates the scheme is valuable to new staff at the same time as providing NESOs the opportunity to develop their mentoring and coaching skills.

### Harassment Free Workplace

In 2007–08, ASIO reviewed its policy on *Maintaining a Harassment Free Workplace* and its arrangements for the Harassment Contact Officer (HCO) Network. Training was provided to 11 HCOs. All ASIO Divisions had a HCO. There were no formal reports of harassment or discrimination in 2007–08.

### Workplace Relations and Reforms

ASIO officers received a pay rise on 1 January 2008 as part of ASIO's *Seventh Workplace Agreement*. The final pay rise under the current agreement is scheduled for 1 January 2009.

The ASIO Consultative Council, consisting of representatives of management and the ASIO Staff Association, continued to meet monthly to discuss workplace relations issues, including those relating to the *Seventh Workplace Agreement* (see also p. 58).

### Capability Enhancements

In 2007–08, ASIO commenced a major upgrade of its human resource information systems – including improvements to data quality – introducing greater automation of payroll processes and bringing on-line a range of other technology solutions to assist human resource management.

### SES Performance Pay

In 2007–08, 38 members of ASIO's SES were awarded performance pay for their work in 2006–07. The amounts paid ranged from \$1,465 to \$16,156. The average payment was \$7,781 and the total amount paid was \$295,679.

## Disability Strategy

Through ASIO's *Disability Action Plan 2005–09*, 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.

## Occupational Health and Safety

During 2007–08, ASIO continued to develop and implement a range of Occupational Health and Safety (OHS) initiatives to ensure legislative compliance with the OHS Management Arrangements and the prevention and management of injuries in the workplace. ASIO also continued to implement a rehabilitation framework that promotes early intervention and durable return to work outcomes for injured staff members.

During Health Week (17–21 September 2007), staff were provided with free health appraisals; skin checks and a range of health related activities and seminars; vaccinations for flu; workstation assessments; and training in manual handling to minimise the risk of back or overuse injuries. Tailored advice was provided to staff requiring individual attention.

The deployment of a trained Health and Safety Representative in each designated work group and strengthened First Aid capabilities was part of ASIO's broad strategy to prevent injury and provide a healthy and safe workplace.

In 2007–08, ASIO had 24 staff members with compensable injuries. An additional two staff members had claims that were under assessment by Comcare at the end of the reporting period.

In 2007–08, no incidents were notified to Comcare under section 68 of the *Occupational Health and Safety Act 1991*, compared with one in 2006–07.

Comcare conducted an investigation into ASIO's response to Improvement Notice No 31931N01 issued on 21 July 2006. The notice required improvements to stairway railings and access and egress from the roof area of ASIO's Central Office in Canberra. ASIO complied with the Improvement Notice and the matter was closed on 18 April 2008.

## Financial Services

### Purchasing

ASIO procurement activity is conducted in accordance with the *Chief Executive Instructions*, which require officers to have regard to the *Commonwealth Procurement Guidelines*, subject to authorised exemptions for the protection of national security. ASIO adheres to the Australian Government's procurement policy framework, and ensures that value for money is achieved through competitive procurement processes wherever practicable. The Chief Executive Instructions direct ASIO officers to refrain from publishing details about ASIO's procurement activities and contracts when such disclosure could reasonably be expected to cause damage to national security.

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 (PJCIS).

ASIO's annual investment program continued during the year, with procurement objectives focused on the acquisition of goods and services to support ASIO's capability enhancement. This included investment in enabling functions such as information technology infrastructure and accommodation to support growth.

In 2007–08, ASIO established a dedicated procurement capability.

## Consultants

During 2007–08, ASIO let two consultancy contracts, down from 16 in 2006–07. The total expenditure during the year on consultancy contracts valued at \$10,000 or more (including contracts let during the previous year) totalled \$0.942m, up from \$0.864m in 2006–07. Although the number of let contracts fell, expenditure increased as some let contracts in previous years continued.

Subject to authorised exemptions for the protection of national security, a list of consultancy let contracts to the value of \$10,000 or more (inclusive of GST), and the total value of each of those contracts, may be made available to members of Parliament as a confidential briefing, or to the PJCIS on request.

## Competitive Tendering and Contracting

ASIO released 14 Restricted Requests for Tender during 2007–08. The Requests for Tender were not advertised publicly for national security reasons – rather a restricted set of suppliers was invited to tender.

During 2007–08, ASIO established procurement panels for contractors, services and hardware/software, from which 12 contracts were awarded. These panels allow the procurement of items over \$80,000 without a separate tender for each purchase, and comply with the *Commonwealth Procurement Guidelines*.

## Information Services

As an intelligence agency, information is central to almost every aspect of ASIO's activity. ASIO must be able to store, collate, and retrieve data quickly and accurately. Reliable data streams are important for a range of activities, including security intelligence operations, the preparation of security intelligence reports, and ASIO's obligation to provide information to support legal and other processes.

ASIO invests substantially in technical information infrastructure, and in the people and processes that support it. The specialised nature of ASIO's work requires advanced and highly-specific systems, skills and capabilities. Developing and maintaining these can be resource intensive.

ASIO is expanding its information technology infrastructure in line with its overall strategy of capability enhancement. Meeting the requirements of increased staffing, accommodating a more diverse geographic spread of ASIO offices, and maintaining pace with technological developments are priorities. New capabilities are being introduced, and existing ones augmented. In 2007–08, ASIO upgraded a number of Information Technology (IT) facilities, rolled-out new support software, achieved greater connectivity, and made enhancements to audio-visual and video-conferencing facilities.

An Information Technology Traineeship Scheme was introduced in 2007–08, as part of strategy to recruit and build expertise in the current tight IT skills market.

ASIO also deployed a secure on-line recruiting website to enable more efficient management of recruitment. Applicants are now able to apply for ASIO job vacancies over the Internet.

ASIO introduced Wiki technology on its core information system in 2007–08. This encouraged collaboration on shared development efforts, and captured and shared knowledge across ASIO in a way that was not previously possible.

ASIO commenced a comprehensive review of business continuity documentation.



*An ASIO data centre in Canberra*

## Records Management

ASIO updated its (classified) *Record Keeping Policy* in 2007–08, and drew on the results of a staff survey to improve record keeping practices. This enhanced ASIO's capability to respond in an accurate and timely manner to requests for information, including from the Inspector-General of Intelligence and Security (IGIS) and in response to subpoenas.

### Release of ASIO Records

ASIO is an exempt agency under the *Freedom of Information Act 1982* but is subject to release of records under the *Archives Act 1983* (the Archives Act). The Archives Act provides for public access to Commonwealth records over 30 years old (described as the Open Access Period).

In May 2008, ASIO and the National Archives of Australia (NAA) formalised an arrangement under the Archives Act for assessment of ASIO records. When the NAA receives requests from the public for ASIO records that are at least 30 years old and not already publicly released, it passes the application to ASIO. ASIO locates any relevant records and advises the NAA whether there is information that should be exempt from public release because of potential to harm Australia's national security. In most cases the information is released. ASIO must ensure, however, that there is an appropriate balance between public access and the need to protect sensitive information. Once a record is assessed and released to the NAA, it is available for general public access.

ASIO received 530 applications for access to records in 2007–08, a decrease from 582 in 2006–07. The total number of folios (pages), however, examined during 2007–08, increased from 52,234 in 2006–07 to 63,932.

ASIO generally gives greater priority to requests from people seeking records on themselves or family members (known as ‘family requests’). There were 136 family requests completed in 2007–08, compared to 143 in 2006–07 – 87% of these were completed within the benchmark of 90 days compared with 98% for 2006–07.

Applicants dissatisfied with exemptions claimed by ASIO on national security grounds can request an internal reconsideration of the decision. These are undertaken in conjunction with the NAA. In 2007–08, there were 10 internal reconsiderations and in each case the NAA upheld ASIO exemptions. Applicants remaining dissatisfied can appeal to the Administrative Appeals Tribunal (AAT).

Applicants can also appeal to the AAT if their request is not completed within 90 days. Two applications to the AAT were lodged in 2007–08 on these grounds. One hearing resulted in an agreement with a researcher that a higher priority be given to one of their requests. The other matter is still to be heard by the AAT.

Table 7 illustrates ASIO’s commitment to making archival information available and demonstrates an improving performance over the past five years.

	2003–04	2004–05	2005–06	2006–07	2007–08
Percentage of Folio released without exemption	35%	48%	45%	53.6%	63%
Percentage of Folios released with part of text claimed as exempt	58%	46%	53%	43.8%	33%
Percentage of Folio claimed as totally exempt	7%	6%	2%	2.6%	4%
<b>Total folio assessed</b>	<b>32 708</b>	<b>41 181</b>	<b>45 454</b>	<b>52 234</b>	<b>63 932</b>

Table 7: Folios released by ASIO 2003–08.

## The Hope Royal Commission into Intelligence and Security

Throughout the reporting period, ASIO contributed to a whole-of-government effort to assess and release the reports and records of the Hope Royal Commission into Intelligence and Security (RCIS). Following the Commission in 1974, some findings deemed not prejudicial to national security were tabled publicly. The majority of the reports were not, however, released. At the time, Justice Hope QC had expressed the wish that these reports would be released in the future as an entire work.

The RCIS records were made available publicly on 27 May 2008. The majority of the documents assessed were deemed not of continuing security concern and released to the public.



Director-General of Security Mr Paul O'Sullivan, the NAA's Director-General Mr Ross Gibbs PSM, and Mr George Brownbill at the release of RCIS reports and records  
Photo courtesy of Marcus Hayman and the National Archives of Australia

## The Hope Royal Commission and ASIO

The Royal Commission into Intelligence and Security was established by Prime Minister Whitlam in 1974 to review Australia's security and intelligence agencies. At the time, ASIO was the only intelligence agency whose existence was known widely, and the only agency governed by legislation (the *Australian Security Intelligence Organisation Act 1956* – the '1956 Act').

Although Justice Hope QC found there were deficiencies within ASIO – and the broader intelligence community – he assessed that a need remained for an agency that could balance individual rights with the Government's obligation to protect against threats. He considered this was best achieved through a dedicated security intelligence service. His recommendations consequently led to a redevelopment of ASIO's legislative framework and the adoption of the *Australian Security Intelligence Organisation (ASIO) Act 1979* and the *Telecommunications (Interception and Access) Act 1979*. The legislation defined 'security', provided legislative parameters for ASIO's security assessments, mandated the political impartiality of ASIO, and set a framework for the use of telecommunications interception powers.

There is little comparison between the ASIO that Justice Hope reviewed in the 1970s and the ASIO of today. Today, ASIO operates within more carefully defined legislative parameters, which includes a strict oversight and accountability framework that incorporates an Inspector-General of Intelligence and Security (IGIS). The IGIS has powers similar to that of a standing Royal Commission.



## Property Management

ASIO's Central Office is located in Russell in the Australian Capital Territory. It is the only publicly declared ASIO office, although ASIO occupies premises in every Australian State and Territory. ASIO offices require strict security standards to ensure the protection of ASIO's information holdings, assets and staff. The growth in ASIO staffing (see p. 46) continues to place pressure on ASIO's accommodation.

### New Offices and Renovations

#### New Central Office

In the 2007–08 Federal Budget, the Government approved the development of a new purpose-built facility in Canberra to accommodate ASIO's Central Office. The new building is being designed and constructed in partnership with the Department of Finance and Deregulation and will be located on the site known as Section 49, Parkes, within the Parliamentary Triangle and in close proximity to the Russell precinct.

A design concept for ASIO's new building was developed in 2007–08. The building design will be in keeping with the National Capital Plan and the Griffin Legacy – under the guidance of the National Capital Authority – and include elements of environmentally sustainable design. The building is being designed to meet ASIO's needs well into the future. The design concept has been developed carefully to ensure the new building will take its place amongst Australia's national institutions in Canberra.

The new building will accommodate up to 1,800 people and operate 24 hours per day, with a level of security commensurate with ASIO's intelligence functions. The building will include offices and open plan work areas, technical workshops, data centre, training areas and staff amenities.

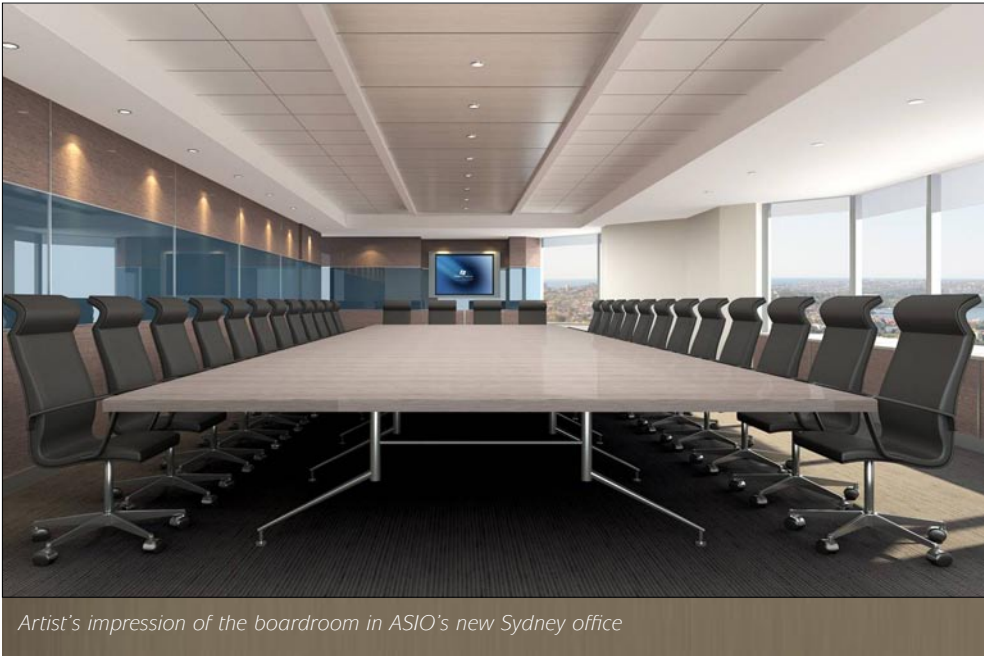
The general office space will be designed to the current standard of Commonwealth agencies in Canberra. The office environment will offer natural light, fresh air and other amenities to make the building an attractive workplace.

Technical workspaces will be purpose-designed for their particular function and include modern technology, as well as health and safety features.

In 2007–08, a secure site office was established to accommodate government project officers, along with the managing contractor, project architect and design consultants. A managing contractor and project architect were engaged to conduct the planning phase of the project, which is scheduled for completion in early 2008–09. Following this, the delivery phase will see development of the design and construction of the building to achieve an occupation date scheduled for 2012.

#### State and Territory Offices

ASIO's growth has also put pressure on accommodation in its State and Territory offices. In response, funding was provided in the 2005–06 Additional Estimates, and in both the 2006–07 and 2007–08 Budgets for the expansion of these offices. Significant progress continues to be made to deliver new and refurbished accommodation nationally. In each capital ASIO offices have – or will be – relocated to larger premises.



*Artist's impression of the boardroom in ASIO's new Sydney office*

## Environmental Performance

ASIO's demand for energy continues to climb as capabilities are enhanced in line with advances in technology. Increases in staff numbers, and the further expansion of ASIO's 24/7 operations, also continues to drive total energy demands upward.

All new or refurbished office fit-outs endeavour to achieve an Australian Greenhouse Building Rating of at least 4 stars. For example, the new main chiller unit installed in 2007–08 in ASIO's Central Office is designed to achieve approximately 20% more efficiency while providing 25% more capacity.

ASIO continues to recycle cardboard waste, computer packaging including polystyrene components, toner cartridges, unclassified IT equipment and fluorescent tubes. The protection of national security material prevents ASIO from recycling classified waste or classified IT equipment. All ASIO contracts incorporate clauses to ensure contractors and sub-contractors make the best use of recycled materials and remove fixtures and fittings to be recycled wherever possible.

## Corporate Governance

ASIO has a strong corporate governance framework that takes into account the particular needs of an intelligence agency and the importance that the public and Government places on ensuring ASIO is accountable, professional and impartial.

## Structures and Processes

Following on from the changes to ASIO's corporate governance structure in 2006–07, ASIO's corporate committee structure reflects its continued focus on building capability and managing growth. The benefits

of these enhancements were evident in 2007–08, including standardised and tightly focused committee reporting, more effective performance evaluation, and greater transparency.

At the core of ASIO's corporate governance framework are two high-level executive committees – the twice weekly Director-Generals Meeting and the twice monthly Corporate Executive Meeting.

The Director-General's Meeting comprises the Director-General of Security, Deputy Directors-General and First Assistant Directors-General. It manages the day-to-day business of ASIO, including corporate priorities and urgent or emerging issues requiring attention.

The Corporate Executive meets twice monthly and comprises the Director-General of Security, Deputy Directors-General and First Assistant Directors-General. Several managers on rotation and the Staff Association President attend as observers. It sets ASIO's strategic direction and oversees resource management, providing the main forum for managing strategic corporate priorities and resource issues. It also conducts detailed quarterly reviews of performance across ASIO.

The Director-General's Meeting and the Corporate Executive oversee eight ongoing corporate committees, as well as one non-ongoing committee (ASIO's New Building Project).

The Intelligence Coordination Committee, chaired by a Deputy Director-General, includes senior managers from across ASIO involved in the intelligence process. It sets security intelligence investigative priorities and allocates resources to these on a risk management basis. It undertakes quarterly reviews against strategic objectives and approves policies and procedures 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 Mandate, by setting priorities for audit, fraud control and evaluation planning. It 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 and including the Staff Association President, 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, comprising the two Deputy Directors-General, manages the strategic placement of staff across ASIO, addressing existing and longer-term priorities and capability gaps.

The Security Committee, chaired by the head of Security Division and including the Staff Association President, reviews and addresses key issues relevant to the security of ASIO's people, property and IT systems. It drives development of security policies and practices.

The Research and Development Committee, chaired by the head of Technical Capabilities Division includes ASIO's Science Adviser and a representative from the Defence Science and Technology Organisation. It 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 (ICT) program. Five program boards oversee ICT projects on a thematic basis, and report to the Information Management Committee.

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 is an advisory body, which makes recommendations to the Director-General of Security on personnel policies and practices. It facilitates management and staff discussion and resolution of issues of mutual interest and concern.

The New Building Committee (non-ongoing) provides strategic guidance on the New Building Project, including direction on significant design milestones, review of significant risk issues and oversight of the project budget and program.



Figure 2: ASIO's corporate governance arrangements

## Accountability

ASIO operates under a rigorous oversight and accountability framework which results in comprehensive scrutiny of ASIO's activities, and which recognises that much of ASIO's work necessarily occurs outside the public view. This framework – including Ministerial and Parliamentary oversight and the IGIS – ensures that ASIO operates professionally and with propriety, and that the appropriate balance is struck between the requirements of security and the individual rights of Australians.

## Oversight, Committees and Inquiries

### National Security Committee of Cabinet

The National Security Committee of Cabinet (NSC) is the Australian Government's peak decision-making body on security-related policy, strategy and resources. The NSC determines the strategic direction of Australia's intelligence effort, including resourcing for Australia's intelligence agencies, determining national security priorities, and monitoring performance against those priorities throughout the year. The NSC is supported by the Secretaries Committee on National Security (SCNS). The Director-General of Security participates in NSC meetings and is a member of SCNS.

### Attorney-General

ASIO falls within the Attorney-General's portfolio. ASIO keeps the Attorney-General informed of its operations, investigations, and other matters relevant to its functions through written submissions, the presentation of special powers warrant requests, and oral briefings as required.

Under section 8A(1)(a) of the ASIO Act, the Attorney-General may give the Director-General of Security written guidelines to be observed by ASIO in the performance of its functions. These were updated during the reporting period and released in late 2007. The revised *Attorney-General's Guidelines*:

- set out the Attorney-General's expectations of ASIO in the performance of its functions, including the collection and handling of personal information;
- provide guidance on when information obtained in an investigation is relevant to security;
- clarify when ASIO can communicate information it has in its possession, which, although not relevant to its security function, should nevertheless be communicated because there are public interest reasons for communicating the information;
- set out relevant principles that govern ASIO's work;
- clarify ASIO's use of new and advanced analytical and investigative methodologies in the performance of its functions;
- impose comprehensive requirements for the handling of personal information by ASIO; and
- incorporate the current definition of politically motivated violence and provide additional guidance relating to the investigation of violent protest activities relating to threats to various specified persons.

The Guidelines, which are available on ASIO's website, do not broaden ASIO's powers beyond what the ASIO Act allows.

In 2007–08, ASIO provided 249 written submissions to the Attorney-General, compared to 358 in 2006–07. The decline in submissions during 2007–08 was primarily due to the caretaker period and the handover of government.

### Parliamentary Joint Committee on Intelligence and Security

The PJCIS reviews ASIO's (and the other intelligence agencies') administration and expenditure, and may also conduct inquiries into matters relating to the intelligence agencies that have been referred to the PJCIS by the responsible Minister or by a resolution from either House of Parliament.

Specifically, with regard to ASIO, the PJCIS is also responsible for:

- reviewing the listing of an organisation as a terrorist organisation under the *Criminal Code Act 1995* (see also p. 5); and
- reviewing ASIO's questioning and detention powers.

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

## Other Parliamentary Oversight

ASIO responded to 26 Questions on Notice issued by both Houses of Parliament.

ASIO also appears before the Senate Standing Committee on Legal and Constitutional Affairs as part of the Budget Estimates process. The Director-General of Security appeared before the Committee on 19 February 2008 and 26 May 2008.

## Inspector-General of Intelligence and Security

The role of the IGIS is to ensure that ASIO and the five other agencies which comprise the Australian Intelligence Community 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;
- 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;
- provision of information on Australian persons to foreign liaisons;
- ASIO's policies and practices with regard to the retention of intelligence information on currently serving parliamentarians; and
- official use of alternate identification documentation in support of assumed identities (see also p. 63) and operational activities and investigations.

Based on the various monitoring, inspection and inquiry activities completed by the Office of the IGIS in 2007–08, the IGIS reported that few substantive concerns were identified and that those which were, were corrected or suitably addressed. A number of procedural points were raised, primarily through inspection activities, and the IGIS has indicated that these were also corrected and addressed satisfactorily. This increase is likely to be, at least in part, a reflection of the increased tempo and breadth of ASIO's operational activity and the rapid growth of the Organisation in recent years. ASIO will continue to work with the Office of the IGIS to identify early and reduce the number of procedural points.

In 2007–08, a monthly senior management meeting with the IGIS and his staff was instituted to strengthen coordination arrangements and to provide an efficient mechanism for communication and discussion of current issues.

Information on complaints received by the IGIS, and inquiries made by the IGIS, can be found in the IGIS Annual Report ([www.igis.gov.au](http://www.igis.gov.au)).

## Policies and Guidelines

ASIO's legislation empowers ASIO – under appropriate authorisations – to undertake collection operations that include intrusive operations against Australian citizens. It is important that ASIO has in place robust and unambiguous policies and procedures to guide its officers in the performance of these operations. These policies and procedures ensure that ASIO applies its legislative powers in a targeted, appropriate manner that balances Australia's security against the rights of the individual.

ASIO regularly develops and reviews policies and procedures for officers involved in intelligence collection operations. Strict accountability mechanisms are employed to ensure that activities (especially more intrusive activities) are approved by an appropriate level of Senior Officer after considering the merits of the case and alternative courses of action.

Policies and procedures provide advice to ASIO officers in the execution of operations, including warrant operations, human source operations and liaison with Australian and international agencies. They provide guidance on the legislative basis and risk management issues to be considered in planning operations, such as security and Occupational Health and Safety, and levels of authorisation.

In 2007–08, ASIO developed and refined policies, and issued new procedures to respond better to both operational and accountability needs.

The policies were expanded significantly to address and clarify matters that have arisen in legal cases and some of the IGIS's own inquiries and comments, as well as ASIO's practices and principles as applied over many years. The policies provide extensive guidance to case officers and managers in the planning, conduct and management of these activities. In doing this, ASIO maintains appropriate balances that enable it to meet legal or court obligations, while maintaining the approach necessary for the collection of intelligence as a security service.

Subsequent to the release of the *Attorney-General's Guidelines* in late 2007 (see p. 59) ASIO updated some of its operational policies accordingly.

The IGIS continues to be consulted in the development of ASIO's policies and guidelines.

## Public Accountability

Much of ASIO's work necessarily occurs outside the public view. Nevertheless, ASIO strives to provide public information on ASIO and its activities. Beyond ASIO's public statements through parliamentary accountability processes, the primary means by which ASIO provides information to the public are:

- ASIO's *Report to Parliament*;
- the ASIO website;
- responses to media enquiries; and
- public statements by the Director-General of Security.

ASIO produces a classified *Annual Report* which covers ASIO's operational and corporate activities in some detail. ASIO also produces an unclassified annual *Report to Parliament*, which provides a publicly available source of information on ASIO's activities. ASIO is the only agency within the AIC that produces a publicly available annual report.

The ASIO website is the primary source of public information about ASIO. It was updated frequently throughout 2007–08, including with transcripts of the Director-General of Security's speeches, and job vacancies. The website also provides publications such as *ASIO Reports to Parliament* and its *Corporate Plan 2007–2011*.

For recent recruitment rounds – such as ASIO's Intelligence Officer, Surveillance Officer and Intelligence Analyst campaigns – around two-thirds of all applicants became aware of the job vacancies via ASIO's or another website.

ASIO does not comment to the media on sensitive national security matters. It does, however, respond to general media enquiries through ASIO's Media Liaison Officer. In 2007–08, ASIO expanded its contact with journalists and the media, including through interviews on recruitment matters given by a Deputy Director-General on both radio and television, and a television interview by the Director-General about the release of the Hope Royal Commission Records.

In 2007–08, the Director-General of Security addressed conferences and audiences from business, government and academia. Eight of his speeches were available on the ASIO website and covered various themes, including countering espionage and risk management strategies for Australian businesses.

## Internal Audits and Fraud Control

ASIO has an active program of audit and fraud control which includes a dedicated Audit and Evaluation Committee that reports to the Director-General of Security.

During 2007–08, an internal review of the Audit and Evaluation Committee was conducted against the Australian National Audit Office (ANAO) *Better Practice Guide, Public Service Audit Committees*. This resulted in the adoption of a new charter for the Committee. ASIO's internal audit function was also benchmarked against the ANAO *Better Practice Guide, Public Sector Internal Audit*, resulting in a new *Internal Audit Mandate*.

In 2007–08, 13 internal audits and one evaluation in relation to recruiting were completed and were the subject of (classified) reporting to ASIO's Audit and Evaluation Committee.

Recommendations to address any administrative or procedural shortcomings arising from these audits were implemented or addressed. No loss of monies was reported. Fraud control in ASIO is a collective responsibility. Staff have two prime responsibilities – to not commit fraud and to report suspected instances of fraud. There were three incidents of fraud reported in 2007–08. Two were not proven while investigation of the third case has not been finalised.

During 2007–08, ASIO undertook a Fraud Risk Assessment which was the basis for its *Fraud Control Plan 2008–10*. It is a major component in the strategy to minimise fraud within ASIO. The Fraud Control Plan is due to be endorsed by the Audit and Evaluation Committee in early 2008–09.

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

One of ASIO's 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*. Briefings are provided for all staff



every five years through the newly-introduced Security Workshop and for all newly appointed Senior Officers on a Senior Officer Orientation Workshop.

### **Audit of Assumed Identities**

In addition to financial and asset fraud auditing and control, ASIO audits use of assumed identities that support intelligence operations.

An assumed identity may be used to protect the true identity of an ASIO officer undertaking official duties. An assumed identity is only to be used by the person to whom it has been issued and for the purpose approved.

All use of assumed identities by ASIO officers must be authorised by the Director-General of Security or an approved delegate under Part IAC of the *Crimes Act 1914*, and where evidence of an assumed identity is required from a New South Wales State Government agency, this will be also authorised under the *Law Enforcement and National Security (Assumed Identities) Act 1998* (NSW).

As required under both the Commonwealth and New South Wales assumed identity schemes, audits were conducted in July 2007 and January 2008 of records of authorisations under the schemes. No discrepancies were detected.

In addition, the IGIS regularly inspects documentation that supports ASIO's use of assumed identities. There were no instances identified of improper use of assumed identities. As required by the legislation, a report for 2007–08 on the number of authorisations, the general activity undertaken with the use of assumed identities, and relevant audit results has been provided to the IGIS.

## **Reviews and Inquiries**

ASIO cooperated closely with several government reviews during 2007–08, ensuring its responses and contributions were comprehensive, relevant, and timely.

### **Homeland and Border Security Review**

In February 2008, the Government appointed Mr Ric Smith PSM AO to lead a comprehensive *Homeland and Border Security Review*, to report by 30 June 2008. The purpose of the review was to consider the roles, responsibilities and functions of departments and agencies involved in domestic and border security and how their coordination and effectiveness could be optimised.

ASIO engaged closely with the review team throughout the process. It provided a comprehensive classified submission and a series of meetings were held with the review team on various aspects of ASIO's work and its interaction with other intelligence, law enforcement, and border security agencies.

### **Review of Interoperability Between the AFP and its National Security Partners**

In November 2007, the AFP Commissioner Mr Mick Keelty APM commissioned the Honourable Sir Laurence Street AC KCMG QC to undertake a *Review of Interoperability between the AFP and its National Security Partners*. The review considered and recommended improvements in the cooperation, information sharing and interoperability between the AFP and other Australian agencies involved in counter-terrorism activities, particularly ASIO.

ASIO contributed to the review, providing a classified written submission and meeting with the review team.

The review – handed down in March 2008 – made 10 recommendations that fell into four broad categories of operational decision making processes, joint taskforce arrangements, information sharing, and training and education. Six of the recommendations related directly to ASIO, including:

- establishment of an Advisory Board, involving the Director-General of Security, the AFP Commissioner, and the CDPP;
- development of a Joint Operations Protocol between the AFP and ASIO to facilitate information exchange, establishment of an accountable handover process for lead responsibility for a matter, and regular and frequent consultation at a senior level for review;
- appointment of a dedicated Senior Officer at the Office of the CDPP to oversee and coordinate all terrorism and national security prosecutions, and consultation by the AFP and ASIO with CDPP at the operational planning phase;
- attachment and co-location, on a full-time basis, of ASIO officers to the joint counter-terrorism teams in Sydney and Melbourne, with direct IT connectivity to ASIO systems;
- development by the AFP of an integrated IT system that meets national security standards and establishment of an AFP/ASIO protocol for automated sharing of information via the system; and
- development of an AFP/ASIO training enhancement package.

ASIO accepted the recommendations in full, and is well advanced in implementing them in conjunction with the AFP and CDPP.

## The Clarke Inquiry

In April 2008, the Government appointed former New South Wales Supreme Court Judge, the Honourable MJ Clarke QC, to conduct an inquiry into the handling by Australian agencies of investigations following attempted bombings in the United Kingdom on 29 and 30 June 2007. The judicial inquiry is to examine Australian agencies' response to the bombings – including investigations into Queensland-based Indian national Dr Mohamed Haneef – focusing on agency actions, interactions, and provision of advice to Government.

ASIO provided a comprehensive classified submission on its role, actions, and advice, as well as an unclassified submission that was made available on the Inquiry's website. In addition, ASIO also made relevant officers involved in the investigation available for examination by the inquiry.

The inquiry is due to report by 14 November 2008.

## Legislative Change

In 2007–08, ASIO's engagement with other departments and agencies on legislative issues focused largely on changes to telecommunications interception legislation.

### Telecommunications (Interception and Access) Amendment Act 2007

The *Telecommunications (Interception and Access) Amendment Act 2007* (the Amendment Act 2007) received Royal Assent on 28 September 2007. It transferred provisions relating to access to telecommunications data for national security and law enforcement agencies from the *Telecommunications Act 1997* to the *Telecommunications (Interception and Access) Act 1997* (the TIA Act).

The Amendment Act 2007 distinguishes access to historical (in existence at the time of the request) and prospective (collected as it is created and forwarded to the agency in near real-time) telecommunications data. With appropriate authorisation, ASIO may have prospective access to telecommunications data for up to 90 days. An authorisation must be revoked where the grounds for access no longer exist – that is, where access to telecommunications data is no longer connected with or necessary for the performance of ASIO functions. ASIO can also access historical telecommunications data where it is connected with the performance of ASIO functions. Like ASIO's use of special powers under warrant, access to telecommunications data is subject to oversight by the IGIS.

The Amendment Act 2007 also provides for secondary disclosure and use of telecommunications data in certain circumstances. This allows law enforcement agencies to pass information to ASIO where it is reasonably necessary for ASIO to carry out its functions.

### **Telecommunications (Interception and Access) Amendment Act 2008**

The *Telecommunications (Interception and Access) Amendment Act 2008* received Royal Assent on 26 May 2008. Key changes made to the TIA Act include extending the network protection exceptions for specified agencies (including ASIO) to 12 December 2009. These allow monitoring of all communications within corporate networks, for the purpose of protecting and maintaining the networks and maintaining professional standards.

### **Security of ASIO**

As a security service, ASIO's core business is to identify and collect intelligence on threats to the security of Australia, and to advise the Government on them. In doing so, ASIO collects and stores sensitive information, sometimes provided by international partners and often relating to Australian citizens and residents. Compromise of ASIO information or operations can cause harm to Australia's national security. It is crucial, therefore, that ASIO information is protected from unauthorised disclosure, misuse, or inappropriate handling.

ASIO's Security Division is responsible for ensuring ASIO's security integrity. Best practice security is ultimately, however, reliant upon staff. ASIO staff undergo stringent vetting processes that include extensive background and suitability checking. ASIO has a strong security culture supported by clear, comprehensive and accessible policies, and a regime to ensure compliance.

ASIO security policies and practices meet or exceed the standards laid down in the *Australian Government Protective Security Manual (PSM)* and its classified supplement, and the *Australian Government Information and Communications Technology Security Manual*.

ASIO continued to improve its security regime throughout 2007–08. An enhanced security awareness program was developed and security procedures were refined. ASIO's security audit capability was enhanced and security accountability reporting extended.

### **Policies, Processes and Practices**

ASIO's security policies are consistent with Inter-Agency Security Forum security best practice guidelines. ASIO conducts regular security audits to ensure adherence to security standards and to identify areas where improvement is required.

In 2007–08, ASIO completed its annual review of its (classified) *ASIO Security Plan 2005–2009*. The plan identifies ASIO's security risks and outlines mitigation strategies. Following the review, the Plan now includes

greater contextualisation and a more comprehensive analysis of the threats facing ASIO, ways to mitigate those threats, and updated performance indicators.

The (classified) *ASIO Security Instructions* (ASI) consolidate security instructions for staff, placing the mandatory security standards set by Government into the ASIO context. ASIO staff are required to read the ASI annually and are expected to apply the instructions in their daily business. A major review of the ASI commenced in 2006–07 and concluded in 2007–08. As a result, the ASI is now a more user-friendly, comprehensive, 'living' document that reflects the contemporary security environment.

In 2007–08, ASIO also finished a comprehensive set of generic security policies and instructions for ASIO staff located at overseas posts.

Psychologists and other security professionals are available to provide counselling and advice as part of ASIO's Employee Assistance Program. The program enhances ASIO's security and contributes favourably towards the health and well-being of staff.

Recognising that good security practice is integral to ASIO's work and must be reinforced constantly, in 2007–08 ASIO initiated a new communication strategy for delivering key security messages to staff. It incorporates an ongoing program of security workshops to remind staff of security threats and their responsibilities.

### **Security Clearance Re-evaluations**

All ASIO permanent staff are security cleared to Top Secret level. ASIO continued to demonstrate best practice by complying with the PSM requirement of re-evaluating Top Secret clearance holders within a six-year time frame. ASIO also conducts a 30-month revalidation for all staff.

During the reporting period, 125 re-evaluations were completed, compared with 118 during 2006–07.

### **Physical Security**

Ensuring that ASIO facilities are physically secure allows ASIO staff to have confidence in their work environment and protects classified information. ASIO's physical security standards meet PSM and accreditation requirements for Top Secret facilities.

ASIO's physical security arrangements are reviewed and upgraded continuously in line with advances in physical security technologies (including access control, camera and alarm systems, blast mitigation strategies and vehicle barriers) and changes to threat levels.

During the reporting period, customised training was developed and provided to the ASIO Security Force to enhance skills in dealing with potentially hazardous situations.

### **Information Security**

Protecting sensitive information is a core element of ASIO's security regime. By limiting access to classified material to persons with the appropriate security clearance and with a need-to-know, ASIO minimises the potential for compromise. At the same time, ASIO also adopts a responsibility-to-share culture, to ensure that information is shared appropriately. ASIO's practices for the storage, handling, removal and destruction of classified material meet or exceed relevant standards.

Security audits of classified hardcopy material and ICT systems are conducted regularly to ensure information is not being inappropriately accessed.

Information technology security is a rapidly changing and challenging area. ASIO needs to ensure it is agile and responsive in its adoption of new technologies whilst ensuring ASIO's information and communications technology systems and data holdings are secure and protected from unauthorised access.

In 2007–08, ASIO undertook a major review of its policy on the control of removable data storage media and electronic devices. The updated policy reflects more accurately rapidly changing technology and attitudes to its use, and provides advice to assist ASIO officers in using new technologies in a secure manner.

### **Counter-Intelligence Security**

Counter-intelligence incorporates measures taken to counter security threats to ASIO and its staff. Counter-intelligence measures include the identification and investigation of threats to ASIO operations, security briefings to staff and contractors, management of the Contact Reporting Scheme (see also p. 30), and investigation of suspicious incidents. ASIO staff are encouraged to report suspicious incidents and these are investigated accordingly.

In 2007–08, ASIO produced a report based on analysis of information from the Contact Reporting Scheme. The report was distributed to Agency Security Advisers throughout the Australian Government and provided an analysis of trends in contact reporting that will support presentations to promote the scheme and underline its importance.



# PART 4

---

FINANCIAL STATEMENTS







## INDEPENDENT AUDITOR'S 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 2008, which comprise: a Statement by the Director-General; Income Statement; Balance Sheet; Statement of Changes in Equity; Cash Flow Statement; Schedule of Commitments; Schedule of Contingencies and Notes to and forming part of the Financial Statements, including a Summary of Significant Accounting Policies.

### *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 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 on the financial statements based on my audit. 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 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 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***

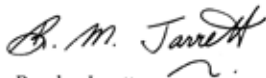
In conducting the audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

**Auditor's Opinion**

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

- (a) have been prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards; and
- (b) give a true and fair view of the matters required by the Finance Minister's Orders including the Australian Security Intelligence Organisation's financial position as at 30 June 2008 and its financial performance and cash flows for the year then ended.

Australian National Audit Office



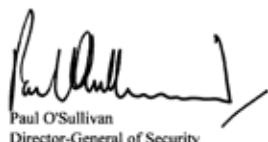
Brandon Jarrett  
Executive Director

Delegate of the Auditor-General

Canberra  
9 September 2008

**STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY**

In my opinion, the attached financial statements for the year ended 30 June 2008 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

9 September 2008



**INCOME STATEMENT***for the period ended 30 June 2008*

	Notes	2008 \$'000	2007 \$'000
<b>INCOME</b>			
<b>Revenue</b>			
Revenue from Government	3A	291,460	227,617
Sale of goods and rendering of services	3B	4,556	4,040
<b>Total revenue</b>		<u>296,016</u>	<u>231,657</u>
<b>Gains</b>			
Reversals of previous asset write-downs	3C	-	281
Other gains	3D	8,093	2,826
<b>Total gains</b>		<u>8,093</u>	<u>3,107</u>
<b>Total Income</b>		<u>304,109</u>	<u>234,764</u>
<b>EXPENSES</b>			
Employee benefits	4A	139,614	112,828
Suppliers	4B	120,722	79,970
Depreciation and amortisation	4C	42,399	36,029
Finance costs	4D	283	96
Write-down and impairment of assets	4E	714	2,434
Foreign exchange losses	4F	6	3
Losses from asset sales	4G	40	49
<b>Total Expenses</b>		<u>303,778</u>	<u>231,409</u>
<b>Surplus attributable to the Australian Government</b>		<u>331</u>	<u>3,355</u>

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

**BALANCE SHEET**  
as at 30 June 2008

	Notes	2008 \$'000	2007 \$'000
<b>ASSETS</b>			
<b>Financial Assets</b>			
Cash and cash equivalents	5A	29,168	16,314
Trade and other receivables	5B	207,373	85,904
Other financial assets	5C	1	1,801
<b>Total financial assets</b>		<b>236,542</b>	<b>104,019</b>
<b>Non-Financial Assets</b>			
Land and buildings	6A,C	59,264	48,457
Infrastructure, plant and equipment	6B,C	95,144	90,000
Intangibles	6D,E	26,369	15,157
Other non-financial assets	6F	12,582	10,560
<b>Total non-financial assets</b>		<b>193,359</b>	<b>164,174</b>
<b>Total Assets</b>		<b>429,901</b>	<b>268,193</b>
<b>LIABILITIES</b>			
<b>Payables</b>			
Suppliers	7A	-	15,994
Other payables	7B	18,611	5,742
<b>Total payables</b>		<b>18,611</b>	<b>21,736</b>
<b>Provisions</b>			
Employee provisions	8A	30,553	26,028
Other provisions	8B	5,987	4,671
<b>Total provisions</b>		<b>36,540</b>	<b>30,699</b>
<b>Total Liabilities</b>		<b>55,151</b>	<b>52,435</b>
<b>Net Assets</b>		<b>374,750</b>	<b>215,758</b>
<b>EQUITY</b>			
Contributed equity		353,970	195,309
Reserves		8,894	8,894
Retained earnings		11,886	11,555
<b>Total Equity</b>		<b>374,750</b>	<b>215,758</b>
<b>Current Assets</b>		<b>249,124</b>	<b>114,579</b>
<b>Non-Current Assets</b>		<b>180,777</b>	<b>153,614</b>
<b>Current Liabilities</b>		<b>41,841</b>	<b>40,311</b>
<b>Non-Current Liabilities</b>		<b>13,310</b>	<b>12,124</b>

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

**STATEMENT of CHANGES in EQUITY**  
as at 30 June 2008

	Retained Earnings		Asset Revaluation Reserves		Contributed Equity/Capital		Total Equity	
	2008 \$'000	2007 \$'000	2008 \$'000	2007 \$'000	2008 \$'000	2007 \$'000	2008 \$'000	2007 \$'000
<b>Opening balance</b>								
Balance carried forward from previous period	11,555	8,200	8,894	8,947	195,309	82,323	215,758	99,470
<b>Income and expenses</b>								
Net revaluation increments/ (decrements)	-	-	-	(53)	-	-	-	(53)
Surplus (Deficit) for the period	331	3,355	-	-	-	-	331	3,355
<b>Total income and expenses</b>	<b>331</b>	<b>3,355</b>	<b>-</b>	<b>(53)</b>	<b>-</b>	<b>-</b>	<b>331</b>	<b>3,302</b>
<b>Contributions by Owners</b>								
Appropriation (equity injection)	-	-	-	-	158,661	112,986	158,661	112,986
<b>Closing balance at 30 June</b>	<b>11,886</b>	<b>11,555</b>	<b>8,894</b>	<b>8,894</b>	<b>353,970</b>	<b>195,309</b>	<b>374,750</b>	<b>215,758</b>

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

**CASH FLOW STATEMENT**  
for the period ended 30 June 2008

	Notes	2008 \$'000	2007 \$'000
<b>OPERATING ACTIVITIES</b>			
<b>Cash received</b>			
Goods and services		3,226	5,141
Appropriations		214,623	195,933
Net GST received		18,234	12,169
Other cash received		6,718	2,523
<b>Total cash received</b>		<b>242,800</b>	<b>215,766</b>
<b>Cash used</b>			
Employees		135,089	108,449
Suppliers		139,469	94,364
<b>Total cash used</b>		<b>274,558</b>	<b>202,813</b>
<b>Net cash flows from or (used by) operating activities</b>	9	<b>(31,758)</b>	<b>12,953</b>
<b>INVESTING ACTIVITIES</b>			
<b>Cash received</b>			
Proceeds from sales of property, plant and equipment		1,071	419
<b>Total cash received</b>		<b>1,071</b>	<b>419</b>
<b>Cash used</b>			
Purchase of property, plant and equipment		54,630	100,289
Purchase of intangibles		16,755	12,578
<b>Total cash used</b>		<b>71,385</b>	<b>112,867</b>
<b>Net cash flows from or (used by) investing activities</b>		<b>(70,314)</b>	<b>(112,448)</b>
<b>FINANCING ACTIVITIES</b>			
<b>Cash received</b>			
Appropriations - contributed equity		114,926	103,067
<b>Total cash received</b>		<b>114,926</b>	<b>103,067</b>
<b>Net cash flows from or (used by) financing activities</b>		<b>114,926</b>	<b>103,067</b>
<b>Net increase or (decrease) in cash held</b>		<b>12,854</b>	<b>3,572</b>
Cash and cash equivalents at the beginning of the reporting period		16,314	12,742
<b>Cash and cash equivalents at the end of the reporting period</b>	5A	<b>29,168</b>	<b>16,314</b>

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



**SCHEDULE OF COMMITMENTS**

as at 30 June 2008

<b>BY TYPE</b>	<b>Notes</b>	<b>2008 S'000</b>	<b>2007 S'000</b>
<b>Commitments Receivable</b>			
Sublease rental income		1,877	1,484
GST recoverable on commitments		18,024	16,666
<b>Total commitments receivable</b>		<u>19,901</u>	<u>18,150</u>
<b>Capital commitments</b>			
Infrastructure, plant and equipment	A	32,316	4,316
Intangibles		203	-
Other capital commitments		20,452	-
<b>Total capital commitments</b>		<u>52,971</u>	<u>4,316</u>
<b>Other commitments</b>			
Operating leases	B	148,176	155,406
Other commitments		-	23,783
<b>Total other commitments</b>		<u>148,176</u>	<u>179,189</u>
<b>Net commitments by type</b>		<u>181,246</u>	<u>165,355</u>
<b>BY MATURITY</b>			
<b>Commitments receivable</b>			
<b>Operating lease income</b>			
One year or less		1,877	1,370
From one to five years		-	114
<b>Total operating lease income</b>		<u>1,877</u>	<u>1,484</u>
<b>Other commitments receivable</b>			
One year or less		6,714	3,944
From one to five years		6,776	6,068
Over five years		4,533	6,654
<b>Total other commitments receivable</b>		<u>18,024</u>	<u>16,666</u>
<b>Commitments payable</b>			
<b>Capital commitments</b>			
One year or less		52,971	4,316
<b>Total capital commitments</b>		<u>52,971</u>	<u>4,316</u>
<b>Operating lease commitments</b>			
One year or less		23,767	15,584
From one to five years		74,541	66,628
Over five years		49,868	73,194
<b>Total operating lease commitments</b>		<u>148,176</u>	<u>155,406</u>
<b>Other Commitments</b>			
One year or less		-	23,783
<b>Total other commitments</b>		<u>-</u>	<u>23,783</u>
<b>Net Commitments by Maturity</b>		<u>181,246</u>	<u>165,355</u>

NB: Commitments are GST inclusive where relevant.

- A. Infrastructure, 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: <ul style="list-style-type: none"> <li>- annual review based on upwards movement in the Consumer Price Index (CPI);</li> <li>- biennial review based on CPI; and</li> <li>- biennial review based on market appraisal.</li> </ul>
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 2008*

Contingent Liabilities	Claims for damages or costs		TOTAL	
	2008 \$'000	2007 \$'000	2008 \$'000	2007 \$'000
Balance from previous period	-	100	-	100
New	-	-	-	-
Re-measurement	-	(100)	-	(100)
Liabilities crystallised	-	-	-	-
Obligations expired	-	-	-	-
<b>Total Contingent Liabilities</b>	-	-	-	-
<b>Net Contingent Liabilities</b>	-	-	-	-

The above schedule should be read in conjunction with the accompanying notes. Refer Note 10.

**NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS  
FOR THE YEAR ENDED 30 JUNE 2008**

- Note 1: Summary of Significant Accounting Policies
- Note 2: Events after the Balance Sheet Date
- Note 3: Income
- Note 4: Expenses
- Note 5: Financial Assets
- Note 6: Non-Financial Assets
- Note 7: Payables
- Note 8: Provisions
- Note 9: Cash Flow Reconciliation
- Note 10: Contingent Liabilities and Assets
- Note 11: Senior Executive Remuneration
- Note 12: Remuneration of Auditors
- Note 13: Financial Instruments
- Note 14: Appropriations
- Note 15: Special Accounts
- Note 16: Compensation and Debt Relief
- Note 17: Reporting of Outcomes

## Note 1: Summary of Significant Accounting Policies

### 1.1 Objectives 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 the 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's 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 the *Financial Management and Accountability Act 1997* and are General Purpose Financial Statements.

The financial statements have been prepared in accordance with the:

- *Finance Minister's Orders* (FMOs) for reporting periods ending on or after 1 July 2007; and
- *Australian Accounting Standards and Interpretations* issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

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

The financial statements are 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 or a future sacrifice of economic benefits will be required 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 unrealised are reported in the Schedule of Commitments and the Schedule of Contingencies (other than unquantifiable or remote contingencies, which are reported at Note 10).

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, 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 judgements 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 amount of assets and liabilities within the next accounting period.

### 1.4 New Australian Accounting Standards requirements

#### Adoption of new Australian Accounting Standard requirements

No accounting standard has been adopted earlier than the application date as stated in the standard. The following new standards are applicable to the current reporting period:

#### Financial instrument disclosure

AASB 7 *Financial Instruments: Disclosures* 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 previously required. 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 statements.

The following new standards, amendments to standards or interpretations for the current financial year have no material financial impact or do not apply to ASIO.

#### Revised Standards:

- AASB 101 *Presentation of Financial Statements* (issued October 2006)
- AASB 1048 *Interpretation and Application of Standard*

#### Amendments:

- AASB 2007-1 *Amendments to Australian Accounting Standards arising from AASB Interpretation 11*
- AASB 2007-4 *Amendments to Australian Accounting Standards arising from ED 151 and Othe Amendments and Erratum: Proportionate Consolidation*
- AASB 2007-5 *Amendments to Australian Accounting Standard - Inventories Held for Distribution by Not-for-Profit Entities [AASB 102]*
- AASB 2007-7 *Amendments to Australian Accounting Standards [AASB 1, AASB 2, AASB 4, AASB 5, AASB 107 & AASB 128]*
- ERR Erratum *Proportionate Consolidation [AASB 101, AASB 107, AASB 121, AASB 127, Interpretation 113]*

#### Interpretations:

- AASB Interpretation 10 *Interim Financial Reporting and Impairment*
- AASB Interpretation 11 *AASB 2 - Group and Treasury Share Transactions*
- AASB Interpretation 1003 *Australian Petroleum Resource Rent Tax*

**Future Australian Accounting Standard requirements**

The following new/revised 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.

**New / Amended Standards:**

- AASB 3 *Business Combinations*
- AASB 8 *Operating Segment*
- AASB 101 *Presentation of Financial Statements* (issued September 2007)
- AASB 123 *Borrowing Costs*
- AASB 127 *Consolidated and Separate Financial Statements*
- AASB 1004 *Contributions*
- AASB 1050 *Administered Items*
- AASB 1051 *Land Under Roads*
- AASB 1052 *Disaggregated Disclosures*

**Amendments:**

- AASB 2007-2 *Amendments to Australian Accounting Standards arising from AASB Interpretation 12 [AASB 1, AASB 117, AASB 118, AASB 120, AASB 121, AASB 127, AASB 131 & AASB 139]*
- AASB 2007-3 *Amendments to Australian Accounting Standards arising from AASB 8*
- AASB 2007-6 *Amendments to Australian Accounting Standards arising from AASB 123*
- AASB 2007-8 *Amendments to Australian Accounting Standards arising from AASB 101*
- AASB 2007-9 *Amendments to Australian Accounting Standards arising from the Review of AASs 27, 29 and 31 [AASB 3, AASB 5, AASB 8, AASB 101, AASB 114, AASB 116, AASB 127 & AASB 137]*
- AASB 2008-1 *Amendments to Australian Accounting Standard - Share-based Payments: Vesting Conditions and Cancellations [AASB 2]*
- AASB 2008-2 *Amendments to Australian Accounting Standards - Puttable Financial Instruments and obligations arising on Liquidation [AASB 7, AASB 101, AASB 132, AASB 139 & Interpretation 2]*
- AASB 2008-3 *Amendments to Australian Accounting Standards arising from AASB 3 and AASB 127 [AASBs 1, 2, 4, 5, 7, 101, 107, 112, 114, 116, 121, 128, 131, 132, 133, 134, 136, 137, 138 & 139 and Interpretations 9 & 107]*
- AASB 2008-4 *Amendments to Australian Accounting Standard - Key Management Personnel Disclosures by Disclosing Entities [AASB 12]*

**Interpretations:**

- UIG Interpretation 1 *Changes in Existing Decommissioning, Restoration and Similar Liabilities*
- AASB Interpretation 4 *Determining Whether an Arrangement Contains a Lease*
- AASB Interpretation 12 *Service Concession Arrangements*
- AASB Interpretation 13 *Customer Loyalty Programmes*
- AASB Interpretation 14 *AASB 119 - The Limit on a Defined Benefit Asset, Minimum Funding Requirements and their Interaction*
- AASB Interpretation 129 *Service Concession Arrangements Disclosures*
- AASB Interpretation 1038 *Contributions by Owners Made To Wholly- Owned Public Sector Entities*

**Other**

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

**AASB 1049 *Whole of Government and General Government Sector Financial Reporting***

AASB 1049 specifies the reporting requirements for the General Government Sector. The FMOs do not apply to this reporting entity or the consolidated financial statements of the Australian Government.

**1.5 Revenue**

**Revenue from Government**

Amounts appropriated for departmental appropriations for the year (adjusted for any formal additions and reductions) are recognised as revenue when ASIO gains control of the appropriation, 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 ASIO.

Revenue from rendering of services 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 ASIO.

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 day terms, are recognised at the nominal amounts due less any allowance for impairment. Collectability of debts is reviewed at balance date. An allowance for impairment is made when collectability of the debt is no longer probable.

**1.6 Gains**

**Other 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 or Authority 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, i.e. whether they have been generated in the course of the ordinary activities of ASIO.

#### Sale of Assets

Gains from the disposal of non-current assets are 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.

#### Other distributions to owners

The FMOs require that distributions to owners be debited to contributed equity unless in the nature of a dividend. There have been no distributions to owners in 2007-08.

### **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 at 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 benefits 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. A review of staffing profile was undertaken to ensure that the actuarial review assessment was still current as at 30 June 2008. This was found to be the case.

#### Separation and Redundancy

Provision is made for separation and redundancy benefit payments. ASIO only 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. For the financial year 2007-08, no formal plan for terminations exist and thus, no provision for separation and redundancy has been recognised.

### **Superannuation**

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

The CSS and PSS are defined benefit schemes for the 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 current cost to the Government of the superannuation entitlements of ASIO's employees. ASIO accounts for the contributions as if they were contributions to defined contribution plans.

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

### **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 is 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.

### **1.10 Borrowing Costs**

All borrowing costs are expensed as incurred.

### **1.11 Cash**

Cash and cash equivalents includes notes and coins held and any deposits in bank accounts with an original maturity of 3 months or less that are readily convertible to known amounts of cash and subject to insignificant risk of changes in value. Cash is recognised at its nominal amount.

### **1.12 Financial assets**

ASIO classifies its financial assets as 'loans and receivables'.

The classification depends on the nature and purpose of the financial assets and is determined at the time of initial recognition.

Financial assets are recognised and derecognised upon 'trade date'.

### **Effective interest method**

The effective interest method is a method of calculating the amortised cost of a financial asset and of allocating interest income over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash receipts through the expected life of the financial asset, or, where appropriate, a shorter period.

Income is recognised on an effective interest rate basis except for financial assets 'at fair value through profit or loss'.

Loans and receivables

Trade receivables, loans and other receivables that have fixed or determinable payments that are not quoted in an active market are classified as 'loans and receivables'. They are included in current assets, except for maturities greater than 12 months after the balance sheet date. These are classified as non-current assets. Loans and receivables are measured at amortised cost using the effective interest method less impairment. Interest is recognised by applying the effective interest rate.

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.

**1.13 Financial Liabilities**

ASIO classifies its financial liabilities as 'at amortised cost'.

Financial liabilities are recognised and derecognised upon 'trade date'.

Other financial liabilities

Other financial liabilities, including borrowings, are initially measured at fair value, net of transaction costs.

Other financial liabilities are subsequently measured 'at amortised cost' using the effective interest method, with interest expense recognised on an effective yield basis.

The effective interest method is a method of calculating the amortised cost of a financial liability and of allocating interest expense over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash payments through the expected life of the financial liability, or, where appropriate, a shorter period.

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).

**1.14 Contingent Liabilities and Contingent Assets**

Contingent Liabilities and Contingent 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 asset or liability in respect of which settlement is not probable or which the amount cannot be reliably measured. Contingent assets are disclosed when settlement is probable but not virtually certain and contingent liabilities are disclosed when settlement is greater than remote.

### 1.15 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.

### 1.16 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' recognised.

#### Revaluations

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

<i>Asset Class</i>	<i>Fair value measured at:</i>
Land	Market selling price
Buildings excl. Leasehold improvements	Market selling price
Leasehold improvements	Depreciated replacement cost
Infrastructure, plant and 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 the carrying amounts of assets do not differ materially 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 type of depreciable asset are based on the following useful lives:

	2008	2007
Buildings on freehold land	25-40 years	25-40 years
Leasehold improvements	Lease term	Lease term
Infrastructure, Plant and Equipment	2-20 years	2-20 years

### ***Impairment***

All assets have been assessed for impairment at 30 June 2008. 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.

#### **1.17 Intangibles**

ASIO's intangible assets primarily comprise externally acquired and internally developed computer software for internal use. ASIO carries intangible assets at cost or, where an active market exists, at fair value.

Computer software and other intangibles are amortised on a straight-line basis over the anticipated useful life. The useful lives of ASIO's software is 3 years (2006-07: 3 years) and other intangibles is 4-5 years (2006-07: 4-5 years).

All intangible assets have been assessed for indications of impairment as at 30 June 2008.

#### **1.18 Taxation / Competitive Neutrality**

ASIO is exempt from all forms of taxation except fringe benefits tax (FBT) and the goods and services tax (GST).

Revenues, expenses and assets are recognised net of GST:

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

#### **1.19 Reporting of Administered Activities**

ASIO has no administered items.

#### **1.20 Comparative Figures**

Comparative figures have been adjusted to conform to changes in presentation in these financial statements where required.

**Note 2: Events after the Balance Sheet Date**

There were no events occurring after the reporting date which had an effect on the 2008 financial statements. (2007: Nil)

**Note 3: Income**

	<b>2008</b>	<b>2007</b>
<i>Revenue</i>	<b>\$'000</b>	<b>\$'000</b>
<b><u>Note 3A: Revenue from Government</u></b>		
Appropriations:		
Departmental outputs	<u>291,460</u>	<u>227,617</u>
<b>Total revenue from Government</b>	<b><u>291,460</u></b>	<b><u>227,617</u></b>
<b><u>Note 3B: Sale of goods and rendering of services</u></b>		
Provision of goods - related entities	8	25
Provision of goods - external parties	19	67
Rendering of services - related entities	4,302	3,704
Rendering of services - external parties	<u>227</u>	<u>244</u>
<b>Total sale of goods and rendering of services</b>	<b><u>4,556</u></b>	<b><u>4,040</u></b>
<b><u>Gains</u></b>		
<b><u>Note 3C: Reversals of previous asset write-downs</u></b>		
Asset revaluation increment	-	281
<b>Total reversals of previous asset write-downs</b>	<b><u>-</u></b>	<b><u>281</u></b>
<b><u>Note 3D: Other gains</u></b>		
Resources received free of charge	1,375	1,459
Rent	2,310	867
Repayment of costs shared by other Agencies	2,273	432
Miscellaneous	<u>2,135</u>	<u>68</u>
<b>Total other gains</b>	<b><u>8,093</u></b>	<b><u>2,826</u></b>

**Note 4: Expenses**

	2008 \$'000	2007 \$'000
<b>Note 4A: Employee benefits</b>		
Wages and salaries	98,982	83,216
Superannuation:		
Defined contribution plans	4,257	2,316
Defined benefit plans	14,849	13,736
Leave and other entitlements	8,587	3,461
Separation and redundancies	309	89
Other employee benefits	12,630	10,010
<b>Total employee benefits</b>	<b>139,614</b>	<b>112,828</b>
<b>Note 4B: Suppliers</b>		
Provision of goods – related entities	963	364
Provision of goods – external parties	16,651	16,326
Rendering of services – related entities	23,651	21,722
Rendering of services – external parties	62,348	29,794
Operating lease rentals:		
Minimum lease payments	16,336	11,201
Workers compensation premiums	773	563
<b>Total supplier expenses</b>	<b>120,722</b>	<b>79,970</b>
<b>Note 4C: Depreciation and amortisation</b>		
Depreciation:		
Infrastructure, plant and equipment	25,047	22,230
Buildings	10,097	7,671
<b>Total depreciation</b>	<b>35,144</b>	<b>29,901</b>
Amortisation:		
Intangibles - Computer Software	6,721	6,128
Other Intangibles	534	-
<b>Total amortisation</b>	<b>7,255</b>	<b>6,128</b>
<b>Total depreciation and amortisation</b>	<b>42,399</b>	<b>36,029</b>
<b>Note 4D: Finance costs</b>		
Interest	-	1
Unwinding of discount	283	95
<b>Total finance costs</b>	<b>283</b>	<b>96</b>
<b>Note 4E: Write-down and impairment of assets</b>		
Asset Write-Downs from:		
Impairment of receivables	2	1
Impairment of property, plant and equipment	712	2,384
Impairment of intangible assets	-	49
<b>Total write-down and impairment of assets</b>	<b>714</b>	<b>2,434</b>
<b>Note 4F: Foreign exchange losses</b>		
Non-speculative	6	3
<b>Total foreign exchange losses</b>	<b>6</b>	<b>3</b>



	<b>2008</b>	2007
	<b>\$'000</b>	\$'000
<b><u>Note 4G: Losses from asset sales</u></b>		
Land and buildings:		
Proceeds from sale	<b>(541)</b>	-
Carrying value of assets sold	<b>533</b>	-
Selling expense	-	-
Infrastructure, plant and equipment:		
Proceeds from sale	<b>(530)</b>	(419)
Carrying value of assets sold	<b>578</b>	468
Selling expense	-	-
<b><i>Net loss from asset sales</i></b>	<b><u>40</u></b>	<b><u>49</u></b>

**Note 5: Financial Assets**

	2008	2,007
	\$'000	\$'000
<b>Note 5A: Cash and cash equivalents</b>		
Cash on hand or on deposit	29,168	16,314
<b>Total cash and cash equivalents</b>	<b>29,168</b>	<b>16,314</b>
<b>Note 5B: Trade and other receivables</b>		
Goods and services	5,904	1,737
Appropriations receivable:		
for existing outputs	198,154	77,582
GST receivable from the Australian Taxation Office	3,315	6,585
<b>Total trade and other receivables (gross)</b>	<b>207,373</b>	<b>85,904</b>
Less allowance for impairment:		
Goods and services	-	-
<b>Total trade and other receivables (net)</b>	<b>207,373</b>	<b>85,904</b>
Receivables are represented by:		
Current	207,373	85,904
Non-current	-	-
<b>Total trade and other receivables (net)</b>	<b>207,373</b>	<b>85,904</b>
Receivables are aged as follows:		
Not overdue	203,795	84,689
Overdue by:		
Less than 30 days	448	461
30 to 60 days	69	55
61 to 90 days	69	32
More than 90 days	2,992	667
<b>Total receivables (gross)</b>	<b>207,373</b>	<b>85,904</b>
<b>Note 5C: Other financial assets</b>		
Accrued revenue	1	1,801
<b>Total other financial assets</b>	<b>1</b>	<b>1,801</b>

**Note 6: Non-Financial Assets**

	2008	2007
	\$'000	\$'000
<b>Note 6A: Land and buildings</b>		
Freehold land at gross carrying value (at fair value)	1,385	1,730
Buildings on freehold land:		
- fair value	6,885	3,212
- accumulated depreciation	(237)	-
<b>Total buildings on freehold land</b>	<b>6,648</b>	<b>3,212</b>
Leasehold improvements		
- work in progress	10,131	-
- fair value	52,666	45,226
- accumulated depreciation	(11,566)	(1,711)
<b>Total leasehold improvements</b>	<b>51,231</b>	<b>43,515</b>
<b>Total land and buildings (non-current)</b>	<b>59,264</b>	<b>48,457</b>

No indicators of impairment were found for land and buildings.

**Note 6B: Infrastructure, plant and equipment**

Infrastructure, plant and equipment:		
- work in progress	9,007	2,815
- gross carrying value (at fair value)	112,741	90,370
- accumulated depreciation	(26,604)	(3,185)
<b>Total infrastructure, plant and equipment (non-current)</b>	<b>95,144</b>	<b>90,000</b>

All revaluations are conducted in accordance with the revaluation policy stated in Note 1. On 30 June 2007, 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)
Infrastructure, plant and equipment	-	784
	-	(53)

No indicators of impairment were found for infrastructure, plant and equipment.

**Note 6C: Analysis of property, plant and equipment****TABLE A – Reconciliation of the opening and closing balances of property, plant and equipment (2007-08)**

	Land		Buildings - Total Land Leasehold		Buildings & Improvement		IP & E		Total	
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>As at 1 July 2007</b>										
Gross book value	1,730	3,212	45,226	(1,711)	50,168	(1,711)	93,185	143,353		
Accumulated depreciation/amortisation and impairment	-	-	(1,711)		(1,711)		(3,185)	(4,896)		
<b>Net book value 1 July 2007</b>	<b>1,730</b>	<b>3,212</b>	<b>43,515</b>		<b>48,457</b>		<b>90,000</b>	<b>138,457</b>		
<b>Additions:</b>										
by purchase	-	3,863	17,574		21,437		33,193	54,630		
Depreciation/amortisation expense	-	(239)	(9,858)		(10,097)		(25,047)	(35,144)		
Reclassifications	-	-	-		-		(1,712)	(1,712)		
Revaluations and impairments through equity	-	-	-		-		-	-		
Disposals:										
Other disposals	(345)	(188)	-		(533)		(1,290)	(1,823)		
<b>Net book value 30 June 2008</b>	<b>1,385</b>	<b>6,648</b>	<b>51,231</b>		<b>59,264</b>		<b>95,144</b>	<b>154,408</b>		
<b>Net book value as of 30 June 2008 represented by:</b>										
Gross book value	1,385	6,885	62,797		71,067		121,748	192,815		
Accumulated depreciation/amortisation and impairment	-	(237)	(11,566)		(11,803)		(26,604)	(38,407)		
	<b>1,385</b>	<b>6,648</b>	<b>51,231</b>		<b>59,264</b>		<b>95,144</b>	<b>154,408</b>		

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

	Land \$'000	Buildings \$'000	Buildings Improvement \$'000	Buildings - Total Land & Leasehold Buildings \$'000	IP & E \$'000	Total \$'000
<b>As at 1 July 2006</b>						
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)
<b>Net book value 1 July 2006</b>	<b>1,575</b>	<b>1,950</b>	<b>21,118</b>	<b>24,643</b>	<b>46,099</b>	<b>70,742</b>
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)
<b>Net book value 30 June 2007</b>	<b>1,730</b>	<b>3,212</b>	<b>43,515</b>	<b>48,457</b>	<b>90,000</b>	<b>138,457</b>
<b>Net book value as of 30 June 2007 represented by:</b>						
Gross book value	1,730	3,212	45,226	50,168	93,185	143,553
Accumulated depreciation/amortisation and impairment	-	-	(1,711)	(1,711)	(3,185)	(4,896)
	<b>1,730</b>	<b>3,212</b>	<b>43,515</b>	<b>48,457</b>	<b>90,000</b>	<b>138,457</b>

	2008 \$'000	2007 \$'000
<b><u>Note 6D: Intangibles</u></b>		
<b><i>Computer software</i></b>		
Computer software at cost:		
Purchased - at cost	19,679	9,779
Internally developed – in progress	5,009	2,910
Internally developed – in use	16,689	14,170
Accumulated amortisation	<u>(16,186)</u>	<u>(11,702)</u>
<b><i>Total Computer Software</i></b>	<b><u>25,191</u></b>	<b><u>15,157</u></b>
 <b><i>Other Intangibles</i></b>		
Other Intangibles - at cost	1,937	-
Accumulated amortisation	<u>(759)</u>	<u>-</u>
<b><i>Total Other Intangibles</i></b>	<b><u>1,178</u></b>	<b><u>-</u></b>
 <b>Total intangibles (non-current)</b>	 <b><u>26,369</u></b>	 <b><u>15,157</u></b>

No indicators of impairment were found for intangible assets.

**Note 6E: Intangibles****Table A: Reconciliation of the opening and closing balances of Intangibles (2007-08)**

	Computer software internally developed \$'000	Computer software purchased \$'000	Total Computer Software \$'000	Other Intangibles \$'000	Total \$'000
<b>As at 1 July 2007</b>					
Gross book value	17,080	9,779	26,859	-	26,859
Accumulated depreciation/amortisation and impairment	(3,327)	(8,375)	(11,702)	-	(11,702)
<b>Net book value 1 July 2007</b>	<b>13,753</b>	<b>1,404</b>	<b>15,157</b>	<b>-</b>	<b>15,157</b>
Additions:					
by purchase or internally developed	6,762	9,993	16,755	-	16,755
Reclassification	-	-	-	1,712	1,712
Amortisation	(5,282)	(1,439)	(6,721)	(534)	(7,255)
Disposals:					
other disposals	-	-	-	-	-
<b>Net book value 30 June 2008</b>	<b>15,233</b>	<b>9,958</b>	<b>25,191</b>	<b>1,178</b>	<b>26,369</b>
<b>Net book value as of 30 June 2008 represented by:</b>					
Gross book value	21,698	19,679	41,377	1,937	43,314
Accumulated depreciation/amortisation and impairment	(6,465)	(9,721)	(16,186)	(759)	(16,945)
	<b>15,233</b>	<b>9,958</b>	<b>25,191</b>	<b>1,178</b>	<b>26,369</b>

*Table B: Reconciliation of the opening and closing balances of intangibles (2006-07)*

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



	<b>2008</b>	2007
	<b>\$'000</b>	\$'000
<b><u>Note 6F: Other non-financial assets</u></b>		
Prepayments	<u>12,582</u>	<u>10,560</u>
<b><i>Total other non-financial assets</i></b>	<b><u>12,582</u></b>	<b><u>10,560</u></b>

All other non-financial assets are current assets.

No indicators of impairment were found for other non-financial assets.

**Note 7: Payables**

	2008	2007
	\$'000	\$'000
<b>Note 7A: Suppliers</b>		
Trade creditors	-	15,994
<b>Total supplier payables</b>	<b>-</b>	<b>15,994</b>
Supplier payables are represented by:		
Current	-	15,994
Non-current	-	-
<b>Total supplier payables</b>	<b>-</b>	<b>15,994</b>

Settlement is usually made up to net 30 days (2007: net 30 days).  
There were no invoices on hand at 30 June 2008.

**Note 7B: Other Payables**

Accrued expenses	16,022	2,578
Lease incentives	2,589	3,164
<b>Total Other Payables</b>	<b>18,611</b>	<b>5,742</b>
Other payables are represented by:		
Current	16,719	3,254
Non-current	1,892	2,488
<b>Total Other Payables</b>	<b>18,611</b>	<b>5,742</b>

**Note 8: Provisions**

	2008	2007
	\$'000	\$'000
<b>Note 8A: Employee provisions</b>		
Salaries and wages	1,763	1,209
Leave	28,283	24,404
Superannuation	228	130
Other	279	285
<b>Total employee provisions</b>	<b>30,553</b>	<b>26,028</b>
Employee provisions are represented by:		
Current	24,480	21,063
Non-current	6,073	4,965
<b>Total employee provisions</b>	<b>30,553</b>	<b>26,028</b>

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 \$19,341,403 (2007: \$16,281,068), in excess of one year \$11,211,390 (2007: \$9,746,957).

**Note 8B: Other provisions**

Restoration obligations	5,987	4,671
<b>Total other provisions</b>	<b>5,987</b>	<b>4,671</b>

Other provisions are represented by:

Current	641	4
Non-current	5,345	4,667
<b>Total other provisions</b>	<b>5,987</b>	<b>4,671</b>

**Provision for restoration**

Carrying amount 1 July 2007	4,671
Additional provisions made	1,045
Amounts used	-
Amounts reversed	-
Unwinding of discount or change in discount rate	271
<b>Closing balance 2008</b>	<b>5,987</b>

ASIO 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.

**Note 9: Cash flow reconciliation**

	2008	2007
	\$'000	\$'000
<b>Reconciliation of cash and cash equivalents as per Balance Sheet to Cash Flow Statement</b>		
<b>Report cash and cash equivalents as per:</b>		
Cash Flow Statement	29,168	16,314
Balance Sheet	29,168	16,314
<b>Reconciliation of operating result to net cash from operating activities:</b>		
Operating result	331	3,355
Depreciation /amortisation	42,399	36,029
Net write down of non-financial assets	712	2,152
(Gain) / loss on disposal of assets	40	49
(Increase) / decrease in receivables	(77,734)	(35,247)
(Increase) / decrease in accrued revenue	1,800	(1,636)
(Increase) / decrease in prepayments	(2,022)	(9,223)
Increase / (decrease) in supplier payables	(15,994)	9,994
Increase / (decrease) in other payables	12,869	948
Increase / (decrease) in employee provisions	4,525	4,379
Increase / (decrease) in other provisions	1,316	2,153
<i>Net cash from / (used by) operating activities</i>	<u>(31,758)</u>	<u>12,953</u>

**Note 10: Contingent Liabilities and Assets**

**Unquantifiable Contingencies**

At 30 June 2008 (and 30 June 2007), ASIO had a number of claims against it. ASIO has denied liability and is defending the claims. It is not possible to estimate the amounts of any eventual payments that may be required in relation to these claims.

**Note 11: Senior Executive Remuneration**

	2008	2007
The number of senior executives who received or were due to receive total remuneration of \$130,000 or more:		
\$130 000 to \$144 999	-	-
\$145 000 to \$159 999	5	-
\$160 000 to \$174 999	-	-
\$175 000 to \$189 999	1	1
\$190 000 to \$204 999	6	6
\$205 000 to \$219 999	4	6
\$220 000 to \$234 999	8	6
\$235 000 to \$249 999	6	3
\$250 000 to \$264 999	2	2
\$265 000 to \$279 999	8	1
\$280 000 to \$294 999	1	6
\$295 000 to \$309 999	1	2
\$310 000 to \$324 999	2	1
\$325 000 to \$339 999	4	-
\$340 000 to \$354 999	2	1
\$355 000 to \$369 999	-	1
\$370 000 to \$384 999	-	-
\$385 000 to \$399 999	1	-
\$400 000 to \$414 999	-	1
<b>Total</b>	<b><u>51</u></b>	<b><u>37</u></b>
The aggregate amount of total remuneration of senior executives shown above.	\$12,585,453	\$9,287,036
The aggregate amount of separation and redundancy/termination benefit payments during the year to executives shown above.	\$104,843	\$115,204

**Note 12: Remuneration of Auditors**

	2008	2007
	\$	\$

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

The fair value of the services provided was:

Australian National Audit Office	<u>86,980</u>	<u>86,900</u>
----------------------------------	---------------	---------------

No other services were provided by the Auditor-General.

**Note 13: Financial Instruments**

	2008 \$'000	2007 \$'000
<b>Note 13A: Categories of financial instruments</b>		
<b>Financial Assets</b>		
<b>Loans and receivables</b>		
Cash and cash equivalents	29,168	16,314
Trade receivables	5,904	1,737
Accrued revenue	1	1,801
<b>Carrying amount of financial assets</b>	<b>35,073</b>	<b>19,852</b>
<b>Financial Liabilities</b>		
<b>At amortised cost</b>		
Trade creditors	-	15,994
Accrued expenses	16,022	2,578
<b>Carrying amount of financial liabilities</b>	<b>16,022</b>	<b>18,572</b>

**Note 13B: Net income and expense from financial assets**

There is no net income and expense from financial assets through the profit and loss for the period ending 30 June 2008. (2006-07: Nil).

**Note 13C: Net income and expense from financial liabilities**

<b>At amortised cost</b>		
Interest expense	-	1
<b>Net gain/(loss) financial liabilities - at amortised cost</b>	<b>-</b>	<b>1</b>
<b>Net gain/(loss) financial liabilities</b>	<b>-</b>	<b>1</b>

There is no net income and expense from financial liabilities through profit or loss for the period ending 30 June 2008 (2006-07: \$1,000).

**Note 13D: Fee Income and Expense**

There is no fee income and expenses from financial assets and liabilities for the period ending 30 June 2008 (2006-07: Nil).

**Note 13E: Fair value of financial instruments**

	Carrying amount 2008 \$'000	Fair value 2008 \$'000	Carrying amount 2007 \$'000	Fair value 2007 \$'000
<b>FINANCIAL ASSETS</b>				
<b>Loans and receivables</b>				
Cash and cash equivalents	29,168	29,168	16,314	16,314
Trade receivables (net)	5,904	5,904	1,737	1,737
Accrued revenue	1	1	1,801	1,801
<b>Total</b>	<b>35,073</b>	<b>35,073</b>	<b>19,852</b>	<b>19,852</b>
<b>FINANCIAL LIABILITIES</b>				
<b>At amortised cost</b>				
Trade creditors	-	-	15,994	15,994
Accrued expenses	16,022	16,022	2,578	2,578
<b>Total</b>	<b>16,022</b>	<b>16,022</b>	<b>18,572</b>	<b>18,572</b>



**Note 13F: Credit risk**

ASIO's maximum exposures to credit risk at the 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 is exposed to minimal credit risk in relation to potential debtor default. ASIO provides for this risk through the recognition of an allowance for impairment where necessary.

ASIO manages its debtors by undertaking recovery processes for those receivables which are considered to be overdue. The risk of overdue debts arising is negated through the implementation of credit assessments on potential customers.

ASIO's credit risk profile has not changed from the prior financial year.

The following table illustrates ASIO's gross exposure to credit risk, excluding any collateral or credit enhancements.

	2008	2007
	\$'000	\$'000
<b>FINANCIAL ASSETS</b>		
<b>Loans and receivables</b>		
Cash and cash equivalents	29,168	16,314
Trade receivables	5,904	1,737
Accrued revenue	1	1,801
<b>Total</b>	<b>35,073</b>	<b>19,852</b>
<b>FINANCIAL LIABILITIES</b>		
<b>At amortised cost</b>		
Trade creditors	-	15,994
Accrued Expenses	16,022	2,578
<b>Total</b>	<b>16,022</b>	<b>18,572</b>

The credit quality of financial instruments not past due or individually determined as impaired:

	Not Past Due Nor Impaired		Past due or impaired	
	2008 \$'000	2007 \$'000	2008 \$'000	2007 \$'000
<b>Loans and receivables</b>				
Cash and cash equivalents <sup>1</sup>	29,168	16,314	-	-
Trade receivables <sup>2</sup>	2,326	522	3,578	1,215
Accrued revenue <sup>3</sup>	1	1,801	-	-
<b>Total</b>	<b>31,495</b>	<b>18,637</b>	<b>3,578</b>	<b>1,215</b>

<sup>1</sup> Cash and cash equivalents are subject to minimal credit risk as cash holdings are held with the Reserve Bank of Australia.

<sup>2</sup> Trade and other receivables are subject to minimal credit risk, the majority of which will be recovered on a timely basis.

<sup>3</sup> Accrued revenue is subject to minimal credit risk as full recovery is expected.

**Note 13F: Credit risk (continued)**

Ageing of financial assets that are past due but not impaired for 2008

	0 to 30 days \$'000	31 to 60 days \$'000	61 to 90 days \$'000	90+ days \$'000	Total \$'000
<b>Loans and receivables</b>					
Trade and other receivables	448	69	69	2,992	3,578
<b>Total</b>	<b>448</b>	<b>69</b>	<b>69</b>	<b>2,992</b>	<b>3,578</b>

Ageing of financial assets that are past due but not impaired for 2007

	0 to 30 days \$'000	31 to 60 days \$'000	61 to 90 days \$'000	90+ days \$'000	Total \$'000
<b>Loans and receivables</b>					
Trade and other receivables	461	55	32	667	1,215
<b>Total</b>	<b>461</b>	<b>55</b>	<b>32</b>	<b>667</b>	<b>1,215</b>

**Note 13G: Liquidity risk**

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

ASIO analyses measures of liquidity, such as the relationship between current assets and current liabilities. Such processes, together with the application of full cost recovery, ensures that at any point in time, ASIO has appropriate resources available to meet its financial obligations as and when they fall due.

ASIO manages liquidity risk by ensuring all financial liabilities are paid in accordance with terms and conditions on demand.

ASIO's liquidity risk profile has not changed from 2006-07.

The following table illustrates the maturities for financial liabilities.

	On demand 2008 \$'000	within 1 year 2008 \$'000	1 to 5 years 2008 \$'000	> 5 years 2008 \$'000	Total 2008 \$'000
<b>At amortised cost</b>					
Trade creditors	-	-	-	-	-
Accrued expenses	-	16,022	-	-	16,022
<b>Total</b>	<b>-</b>	<b>16,022</b>	<b>-</b>	<b>-</b>	<b>16,022</b>

	On demand 2007 \$'000	within 1 year 2007 \$'000	1 to 5 years 2007 \$'000	> 5 years 2007 \$'000	Total 2007 \$'000
<b>At amortised cost</b>					
Trade creditors	-	15,994	-	-	15,994
Accrued expenses	-	2,578	-	-	2,578
<b>Total</b>	<b>-</b>	<b>18,572</b>	<b>-</b>	<b>-</b>	<b>18,572</b>

**Note 13H: Market risk**

ASIO holds basic financial instruments that do not expose it to certain market risks. ASIO's market risk profile has not changed from 2006-07.

ASIO is not exposed to 'Currency risk', 'Other price risk' or 'Interest rate risk'.

**Note 14: Appropriations****Table A: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriations**

<b>Particulars</b>	<b>2008 \$'000</b>	<b>2007 \$'000</b>
Balance brought forward from previous period	70,931	30,705
<b>Appropriation Act:</b>		
Appropriation Act (No.1) 2007-08	290,871	227,617
Appropriation Act (No.3) 2007-08	589	-
<b>FMA Act:</b>		
Refunds credited (FMA section 30)	5,741	1,156
Appropriations to take account of recoverable GST (FMA section 31)	11,271	7,188
Annotations to 'net appropriations' (FMA section 31)	5,274	6,928
<b>Total appropriation available for payments</b>	<b>384,677</b>	<b>273,594</b>
Cash payments made during the year (GST inclusive)	224,056	202,663
<b>Balance of Authority to Draw Cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriations</b>	<b>160,621</b>	<b>70,931</b>
<i>Represented by:</i>		
Cash at bank and on hand	29,168	16,314
Departmental appropriations receivable	131,453	54,617
<b>Total</b>	<b>160,621</b>	<b>70,931</b>

**Table B: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriations**

<b>Particulars</b>	<b>2008 \$'000</b>	<b>2007 \$'000</b>
Balance brought forward from previous period	22,965	18,015
<b>Appropriation Act:</b>		
Appropriation Act (No.2) 2007-08	149,616	112,986
Appropriation Act (No.4) 2007-08	9,045	-
<b>FMA Act:</b>		
Appropriations to take account of recoverable GST (FMA section 31)	6,963	4,980
<b>Total appropriations available for payments</b>	<b>188,589</b>	<b>135,981</b>
Cash payments made during the year (GST inclusive)	121,888	113,016
<b>Balance of Authority to Draw Cash from the Consolidated Revenue Fund for Other Than Ordinary Annual Services Appropriations</b>	<b>66,701</b>	<b>22,965</b>
<i>Represented by:</i>		
Appropriation receivable	66,701	22,965

**Note 15: Special Accounts**

ASIO has an Other Trust Monies Account and 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).

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.

On 26 February 2008, the Other Trust Monies Special Account and Services for Other Government & Non-Agency Bodies Account were abolished. Both special accounts had nil balances on abolition (2007: Nil) and there were no transactions debited or credited to them for the year ended 30 June 2008 (2007: No transactions).

**Note 16: Compensation and Debt Relief**

No payments were made during the reporting period. (2007: Nil payments made).

**Note 17: Reporting of Outcomes****Note 17A: Net Cost of Outcome Delivery**

	<b>2008</b>	2007
	<b>\$'000</b>	\$'000
<b>Expenses</b>		
Departmental	<b>303,778</b>	231,409
<b>Costs recovered from provision of goods and services to the non government sector</b>		
Departmental	<b>4,654</b>	811
<b>Other external revenues</b>		
Departmental	<b>6,620</b>	4,596
<b>Net cost/(contribution) of outcome</b>	<b>292,504</b>	226,002

Net costs shown include intra-government costs that are eliminated in calculating the actual Budget Outcome.

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





# PART 5

---

APPENDICES



## Appendix A: Proscribed Terrorist Organisations at 30 June 2008

- Abu Sayyaf Group (ASG)
- Al-Qa'ida
- Tanzim Qa'idat al-Jihad fi Bilad al Rafidayn (TQJBR), also known as al-Qa'ida in Iraq
- Ansar Al-Sunna (also known as Ansar Al-Islam)
- Armed Islamic Group (GIA)
- Asbat al-Ansar
- Egyptian Islamic Jihad (EIJ)
- Hamas' Izz al-Din al-Qassam Brigades
- Hizballah External Security Organisation
- Islamic Army of Aden
- Islamic Movement of Uzbekistan (IMU)
- Jaish-e-Mohammed (JeM)
- Jamiat ul-Ansar (JuA) (formerly known as Harakat Ul-Mujahideen)
- Jemaah Islamiyah (JI)
- Kurdistan Workers Party (PKK)
- Lashkar-e Jhangvi (LJ)
- Lashkar-e-Tayyiba (LeT)
- Palestinian Islamic Jihad (PIJ)
- Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) (formerly known as Salafist Group for Call and Combat (GSPC))

## Appendix B: Mandatory Reporting Requirements under section 94 of the ASIO Act

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

Table 8: Mandatory reporting requirements under section 94 of the *Australian Security Intelligence Organisation Act 1979*

## Appendix C: Workforce Statistics

	2003–04	2004–05	2005–06	2006–07	2007–08
Ongoing Full-time	603	693	800	1,125	1,263
Non-ongoing Full time <sup>1</sup>	103	155	178	55	52
Ongoing Part time	38	43	50	94	108
Non-ongoing Part time	28	22	27	18	12
Non-ongoing Casual	33	42	55	64	57
<b>Total</b>	<b>805</b>	<b>955</b>	<b>1,110</b>	<b>1,356</b>	<b>1,492</b>

<sup>1</sup> Includes attachments, locally engaged staff and contractors/consultants held against positions in the structure.

Table 9: Composition of workforce 2003–04 to 2007–08

		2003–04	2004–05	2005–06	2006–07	2007–08
Band 1	Female	2	4	5	7	6
	Male	9	10	17	17	29
Band 2	Female	1	1	1	2	2
	Male	4	4	4	8	11
Band 3	Male	1	1	1	1	2
<b>Total</b>		<b>17</b>	<b>20</b>	<b>28</b>	<b>35</b>	<b>50</b>

(Note: does not include the Director-General of Security)

Table 10: SES classification and gender 2003–04 to 2007–08

Group	Total Staff <sup>1</sup>	Women	Race / Ethnicity <sup>2</sup>	ATSI <sup>3</sup>	PWD <sup>4</sup>	Available EEO Data <sup>5</sup>
SES (excl DG)	50	8	0	0	2	45
Senior Officers <sup>6</sup>	359	128	43	0	4	320
AO5 <sup>7</sup>	427	212	77	2	4	369
AO1 – 4 <sup>8</sup>	560	314	78	1	7	481
ITO1 – 2 <sup>9</sup>	91	16	17	1	1	86
ENG1 – 2 <sup>10</sup>	5	0	0	0	0	5
<b>Total</b>	<b>1,492</b>	<b>678</b>	<b>215</b>	<b>4</b>	<b>18</b>	<b>1,306</b>

<sup>1</sup> Based on staff salary classifications recorded in ASIO's human resource information system.

<sup>2</sup> Previously Non-English speaking background (NESB1 and NESB2).

<sup>3</sup> Aboriginal and Torres Strait Islander.

<sup>4</sup> People with a disability.

<sup>5</sup> Provision of EEO data is voluntary.

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

<sup>7</sup> ASIO Officer Grade 5 group translates to APS Level 6.

<sup>8</sup> Translates to span the APS 1 to 5 classification levels.

<sup>9</sup> Information Technology Officers Grades 1 and 2.

<sup>10</sup> Engineers Grades 1 and 2.

Table 11: Representation of designated groups within ASIO at 30 June 2008

Group	2003–04 %	2004–05 %	2005–06 %	2006–07 %	2007–08 %
Women <sup>1</sup>	41	43.14	45.9	45.50	45.44
Race/Ethnicity <sup>2</sup>	11	14.64	16.16	15.81	16.46
ATSI <sup>3</sup>	0.41	0.45	0.38	0.31	0.31
PWD <sup>4</sup>	2	1.59	1.36	1.17	1.38

<sup>1</sup> Percentages for women are based on total staff. Percentages for other groups based on staff for whom EEO data was available.

<sup>2</sup> Previously Non-English speaking background.

<sup>3</sup> Aboriginal and Torres Strait Islander.

<sup>4</sup> People with a disability.

Table 12: Percentage of representation of designated groups in ASIO 2003–04 – 2007–08

## Appendix D: ASIO Salary Classification Structure at 30 June 2008

ASIO MANAGERS			
SES Band 3	\$185,469		minimum point
SES Band 2	\$146,595		minimum point
SES Band 1	\$122,953		minimum point
AEO3	\$106,834		
AEO2	\$96,919	to	\$106,834
AEO1	\$85,460	to	\$92,248
INTELLIGENCE OFFICERS			
IO	\$65,256	to	\$74,433
ASIO OFFICERS			
ASIO Officer 5	\$65,256	to	\$74,433
ASIO Officer 4	\$53,820	to	\$58,749
ASIO Officer 3	\$46,933	to	\$50,571
ASIO Officer 2	\$41,330	to	\$45,718
ASIO Officer 1	\$36,633	to	\$40,383
ASIO INFORMATION TECHNOLOGY OFFICERS			
SITOA	\$106,834		
SITOB	\$96,919	to	\$106,834
SITOC	\$85,460	to	\$92,248
ITO2	\$65,256	to	\$74,433
ITO1	\$50,571	to	\$58,749
ASIO ENGINEERS			
SIO(E)5	\$108,531		
SIO(E)4	\$96,919	to	\$106,834
SIO(E)3	\$85,460	to	\$92,248
SIO(E)2	\$65,256	to	\$74,433
SIO(E)1	\$50,571	to	\$58,749

Table 13: ASIO Salary Classification Structure at 30 June 2008





## Compliance Index

Part of Report	Annual Report requirements	Page
	Letter of transmittal	III
	Table of contents	V
	Index	131
	Glossary	129
	Contact officer(s)	Back cover
	Internet home page address and Internet address for report	Back cover
<b>Review by Secretary</b>	Review by departmental secretary (Director-General of Security)	VII
<b>Departmental Overview</b>	Overview description of department	XII
	Role and functions	XII
	Organisational structure	XV–XVII
	Outcome and output structure	XVIII
	Where outcome and output structure differ from PBS format, details of variation and reason for change	N/A
<b>Report on Performance</b>	Review of performance during the year in relation to outputs and contribution to outcomes	9–41
	Actual performance in relation to performance targets set out in PBS	9–41
	Performance of purchaser/provider arrangements	N/A
	Where performance targets differ from the PBS, details of both former and new targets, and reasons for the change	N/A
	Narrative discussion and analysis of performance	9–41
	Performance against service charter customer service standards, complaints data, and the department's response to complaints	53, 60
	Discussion and analysis of the department's financial performance	XIV
	Summary resource tables by outcomes	XIV
	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
<b>Corporate Governance</b>	Statement of the main corporate governance practices in place	56–58
	Agency heads are required to certify that their agency comply with the Commonwealth Fraud Control Guidelines	III

<b>External Scrutiny</b>	Significant developments in external scrutiny	60, 63–64
	Judicial decisions and decisions of administrative tribunals	23–24, 28, 53
	Reports by the Auditor-General, a Parliamentary Committee of the Commonwealth Ombudsman	N/A
<b>Management of Human Resources</b>	Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	47–50
	Statistics on staffing	123
	Certified agreements and AWAs	N/A
	Performance pay	49
<b>Purchasing</b>	Assessment of purchasing against core policies and principles	50
<b>Assets Management</b>	Assessment of effectiveness of assets management	N/A
<b>Consultants</b>	A summary of statements detailing the number of new consultancy services contracts; the total actual expenditure on 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). Statement noting that information on contracts and consultancies is available through the AusTender website	51
<b>Australian National Audit Office Access Clauses</b>	Absence of provisions in contracts allowing access by the Auditor-General	N/A
<b>Exempt Contracts</b>	Contracts exempt from the AusTender	51
<b>Commonwealth Disability Strategy</b>	Report on performance in implementing the Commonwealth Disability Strategy	50
<b>Financial Statements</b>	Financial statements	69–118
<b>Other Information</b>	Reporting requirements under section 94 of the ASIO Act	122
	Occupational health and safety	50
	Freedom of Information	52
	Advertising and Market Research	46
	Ecologically sustainable development and environmental performance	56
<b>Other</b>	Discretionary Grants	N/A
	Correction of material errors in previous annual report	N/A

## Glossary

AAT	Administrative Appeals Tribunal
ACS	Australian Customs Service
AELW	APEC Economic Leaders' Week
AFP	Australian Federal Police
AIC	Australian Intelligence Community
ANAO	Australian National Audit Office
ANSTO	Australian Nuclear Science and Technology Organisation
APEC	Asia-Pacific Economic Cooperation
ASIO	Australian Security Intelligence Organisation
ASIO Act	Australian Security Intelligence Organisation Act 1979
APS	Australian Public Service
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
BLU	Business Liaison Unit
C/CSP	Carriers and Carriage Service Providers
CDPP	Commonwealth Director of Public Prosecutions
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DSA	Defence Security Authority
DSD	Defence Signals Directorate
DSTO	Defence Science and Technology Organisation
IASF	Inter-Agency Security Forum
ICT	information and communications technology
IGIS	Inspector-General of Intelligence and Security
NAA	National Archives of Australia

NCTC	National Counter-Terrorism Committee
NCTP	National Counter-Terrorism Plan
NSH	National Security Hotline
NSC	National Security Committee of Cabinet
NTAC	National Threat Assessment Centre
ONA	Office of National Assessments
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PM&C	Department of the Prime Minister and Cabinet
PMV	Politically Motivated Violence
PSM	Australian Government Protective Security Manual
RCIS	Royal Commission into Intelligence and Security
SCEC	Security Construction and Equipment Committee
SCNS	Secretaries Committee on National Security
SES	Senior Executive Service
SISBOG	Security and Intelligence Specialists for the 2008 Beijing Olympics Games
TIA Act	Telecommunications (Interception and Access) Act 1979
WYD	World Youth Day 2008

## General Index

### A

- AAT, *see* Administrative Appeals Tribunal
- Abu Sayyaf Group, 121
- accommodation, XIV, 45, 50, 55
- accountability, VII, XI, XIII, 45, 54, 58–64,
- ACM, *see* Anti-Coalition Militia
- ACS, *see* Australian Customs Service
- Administrative Appeals Tribunal (AAT), 23, 26, 28, 34, 53
- adverse and qualified assessments, 19, 23, 25, 26–28
- advertising, 46
- Afghanistan, 4, 6, 7
- AFP, *see* Australian Federal Police
- AGCTC, *see* Australian Government Counter-Terrorism Committee
- AGCTPC, *see* Australian Government Counter-Terrorism Policy Committee
- AIC, *see* Australian Intelligence Community
- al-Qa'ida in Iraq (AQI), 4, 121
- al-Qa'ida in the Lands of the Islamic Maghreb (AQIM), 3, 4, 121
- al-Qa'ida, IX, 3–4, 121
- al-Zawahiri, Ayman, 4
- ammonium nitrate, 26, 27
- ANAO, *see* Australian National Audit Office
- Ansar Al-Sunna, 121
- ANSTO, *see* Australian Nuclear Science and Technology Organisation
- Anti-Coalition Militia (ACM), 4
- Anzac Day, XI, 11, 13, 14
- APEC, *see* Asia-Pacific Economic Cooperation
- AQI, *see* al-Qa'ida in Iraq
- AQIM, *see* al-Qa'ida in the Lands of the Islamic Maghreb
- Archives Act 1983*, 52, 60
- Armed Islamic Group, 121
- Asbat al-Ansar, 121
- Asia and the Subcontinent, 4
- Asia-Pacific Economic Cooperation (APEC), VIII, XI, 7, 11, 13–14, 17, 26, 27
- ASICs, *see* Aviation Security Identity Cards
- ASIO Act, *see* Australian Security Intelligence Organisation Act 1979
- ASIO Consultative Council, 49, 58
- ASIS, *see* Australian Secret Intelligence Service
- as-Sahab, 4
- assumed identities, 60, 63
- Attachments, X, 38, 48, 123
- attacks, VII, IX, XII, 3, 4, 5
- Attorney-General, VI, XI, XII, 5, 28, 31, 33, 41, 59, 60
- Attorney-Generals Department, 21, 26, 28, 33, 39
- Attorney-General's Guidelines*, 15, 32, 34, 59, 61
- Audit and Evaluation Committee (ASIO), 57, 58, 62
- AusCheck, 26
- AUSTRAC, *see* Australian Transaction Reports and Analysis Centre
- Australian Communications and Media Authority (ACMA), 33, 39
- Australian Customs Service (ACS), 20
- Australian Federal Police (AFP), VII, X, 6, 13, 14, 16, 17, 20, 21, 22, 26, 38–39, 45, 48, 62, 63–64
- Australian Government Counter-Terrorism Policy Committee (AGCTPC), 37
- Australian Government Counter-Terrorism Committee (AGCTC), 37
- Australian Government Information and Communications Technology Security Manual*, 65
- Australian Government Protective Security Manual*, *see* Protective Security Manual (PSM)
- Australian Intelligence Community (AIC), XII, 6, 17, 29, 38, 41, 48, 60, 61
- Australian National Audit Office (ANAO), 57, 58, 62
- Australian Nuclear Science and Technology Organisation (ANSTO), 26, 27
- Australian partners, VII, X, 31, 36, 38–39
- Australian Secret Intelligence Service (ASIS), 16, 48
- Australian Security Intelligence Organisation Act 1979* (ASIO Act), XII, XIII, XVIII, 3, 7, 15, 18, 24, 26, 28, 34, 54, 59, 122
- Australian Transaction Reports and Analysis Centre (AUSTRAC), 48, 60
- Aviation Security Identity Cards (ASICs), 20, 25, 26, 27
- aviation security, 20, 22, 25, 26, 27

**B**

Beijing Olympic and Paralympic Games, 13, 15, 17  
 Beijing Olympic Torch Relay, XI, 11, 13, 14  
 Blick, Mr WJ, AM PSM, 29  
 BLU, *see* Business Liaison Unit  
 Border Liaison Officers, 20  
 border security, VII, X, XI, 11, 17–20, 35, 45, 63  
 Business Liaison Unit (BLU), VIII, X, XV, 11, 16, 21, 22–23

**C**

C/CSPs, *see* Carriers/Carriage Service Providers  
 Carriers/Carriage Service Providers (C/CSPs), 33  
 CBR, *see* Chemical Biological and Radiological  
 CBRNET, *see* Chemical Biological Radiological Nuclear and Explosives Terrorist  
 CDPP *see* Commonwealth Director of Public Prosecutions  
 Chemical Biological and Radiological (CBR), 6  
 Chemical Biological Radiological Nuclear and Explosives Terrorist (CBRNET), 6  
 Chifley, Prime Minister Ben, XIII  
 China, *see* People's Republic of  
 Clarke Inquiry, the, XI, 45, 64  
 client satisfaction, XIV–XV  
 Comcare, 50  
 Commonwealth Director of Public Prosecutions (CDPP), VII, 24, 39, 48, 64  
 Commonwealth Games, 27  
 Commonwealth Heads of Government Meeting, 13  
 Commonwealth Procurement Guidelines, 50, 51  
 communal violence, XII, 3  
 compliance index, 127–128  
 consultants, 46, 51, 55, 123  
 Contact Reporting Scheme, 25, 30, 67  
 contractors, 46, 51, 56, 67, 123  
 coordination and cooperation with other agencies, VII, X, 15, 17, 21, 22, 39, 63  
 corporate governance, XVII, 56–58  
*Corporate Plan 2007–2011*, 62  
 cost recovery, 25, 28, 29, 33  
 counter-espionage, IX, XV, 7  
 counter-intelligence security, 67

counter-proliferation, 7, 12  
 counter-terrorism assessments, 25, 26–27  
 counter-terrorism exercises, 14, 31, 37, 38  
 Counter-Terrorism Intelligence Training Program (CTITP), 40  
 counter-terrorism, VII, IX, XIII, 4, 6, 14, 15, 21, 36, 37, 38, 39, 63, 64  
*Crimes Act 1914*, 6, 63  
*Criminal Code Act 1995*, 5, 6, 60  
 critical infrastructure protection, X, 20–23  
 critical infrastructure sectors, 21, 22  
 CTITP, *see* Counter-Terrorism Intelligence Training Program  
 customer base, VIII, X, 11, 12

**D**

Defence Imagery and Geospatial Organisation (DIGO), 41, 48  
 Defence Intelligence Organisation (DIO), 16, 48  
 Defence Science and Technology Organisation (DSTO), 35, 36, 57  
 Defence Signals Directorate (DSD), XII, 16, 21, 22, 41, 48  
 Department of Foreign Affairs and Trade (DFAT), 16, 17, 48  
 Department of Immigration and Citizenship (DIAC), VII, 18, 19, 20, 48  
 Department of Infrastructure, Transport, Regional Development and Local Government (DITRDLG), 16, 48  
 Department of the Prime Minister and Cabinet (PM&C), 13, 37, 48  
 DFAT, *see* Department of Foreign Affairs and Trade  
 DIAC, *see* Department of Immigration and Citizenship  
 DIGO, *see* Defence Imagery and Geospatial Organisation  
 DIO, *see* Defence Intelligence Organisation  
 Disability Strategy, 50  
 DITRDLG, *see* Department of Infrastructure, Transport, Regional Development and Local Government  
 DSD, *see* Defence Signals Directorate  
 DSTO, *see* Defence Science and Technology Organisation

**E**

East Africa, 4  
 EEO *see* Equal Employment Opportunity  
 Egyptian Islamic Jihad, 121  
 Employee Assistance Program, 66  
 environmental performance, 56  
 Equal Employment Opportunity (EEO), 124  
 e-security, 21  
 espionage, VII, IX, XII, XIII, 3, 6–7, 28, 62  
 ethics and accountability, 62  
 exchanges, 39, 48  
 extremism, 3

**F**

FATA, *see* Federally Administered Tribal Areas  
 Federal Election, XI, 7, 11, 13, 14  
 Federally Administered Tribal Areas (FATA), 4  
 Financial Statements, 69–118  
 foreign intelligence collection, XII, 41  
 foreign interference, VII, IX, XII, 3, 6  
 foreign liaison, *see* international partners  
 fraud control, 57, 62  
*Freedom of Information Act 1982*, 52  
 funding, XIV, 20, 45, 55

**G**

Global Militant Jihad, 3–4  
 governance, *see* corporate governance  
*Guide to Fraud Prevention, Detection and Reporting Procedures in ASIO*, 62  
 guide to outcome and output structure, XVIII  
 guide to the report, XVIII

**H**

Habib, Mamdouh, 23–24  
 Hamas' Izz al-Din al-Qassam Brigades, 5, 121  
 history and concept of security intelligence, the, XIII  
 Hizballah External Security Organisation, 121  
*Homeland and Border Security Review* (the Smith Review), XI, 45, 63  
 Hope, Robert, AC CMG QC, XIII, 28, 41, 45, 53–54  
 Hope Royal Commission into Intelligence and Security (RCIS), XIII, 45, 53–54, 62

human resource policy and practice, 45, 49–50  
 human source intelligence collection, XII, 32, 33

**I**

IASF, *see* Inter-Agency Security Forum  
 IGIS, *see* Inspector-General of Intelligence and Security  
 IMGs, *see* Issue Motivated Groups  
 incidents affecting Australians, 4, 13  
 India, 4  
 Indian Mujahideen, 4  
 Indonesia, IX, 5, 6  
 industry, engagement with, VII, X, XV, 11, 16, 21, 28, 33, 36  
 Information Management Committee (ASIO), 57, 58  
 information security, 66–67  
 inquiries and reviews, XI, 45, 59, 60, 63–64  
*Inquiry into Security Issues*, 29  
*Insight*, XIV, 12, 18, 32  
 Inspector-General of Intelligence and Security (IGIS), XII, 29, 34, 52, 54, 58, 60–61, 63, 65  
 Intelligence Analysts, 31, 35, 48  
 intelligence collection, XI, 32–34, 41, 57, 61  
 Intelligence Coordination Committee (ASIO), 34, 57, 58  
 Intelligence Officers, 31, 35, 37, 48  
 Inter-Agency Security Forum (IASF), 29–30, 65  
 internal audits, 57, 62–63  
 international partners, VII, X, 12, 14, 15, 16, 31, 32, 38, 48, 65  
 internet, IX, 4, 32, 46  
 interviews, XIV, 33, 62  
 intrusive methods of investigation, XII, 15, 32, 34, 61  
 Iran, 7  
 Iraq, 4, 6, 7  
 Islamabad, 24  
 Islamic Army of Aden, 121  
 islamic extremism, 3  
 Islamic Movement of Uzbekistan, 121  
 Israel, 4  
 Issue Motivated Groups (IMGs), 7, 24

**J**

Jaish-e-Mohammed (JeM), 121  
 JeM, *see* Jaish-e-Mohammed  
 Jemaah Islamiyah (JI), 4–5, 121  
 JI, *see* Jemaah Islamiyah  
 Joint Intelligence Group, 14, 37

**K**

Key statistics, VIII  
 Kurdistan Workers Party (PKK), 5, 121

**L**

Lashkar-e-Jhangvi, 121  
 Lashkar-e-Tayyiba (LeT), 5, 121  
 law enforcement agencies, XI, 33, 38, 39, 60, 64, 65,  
*see also* police  
*Law Enforcement and National Security (Assumed  
 Identities) Act 1998 (NSW)*, 63  
 Learning and Development Strategy, X, 45, 47  
 legal proceedings, *see* litigation  
 legislation, XII, XIII, 33, 45, 54, 61, 63, 64–65 (Acts  
 are indexed individually)  
 LeT, *see* Lashkar-e-Tayyiba  
 Letter of Transmittal, III  
 listening devices, 33  
 litigation, IX, XI, 11, 23–24  
 London bombings, 3  
 Lucas Heights, *see* Australian Nuclear Science and  
 Technology Organisation

**M**

MAL, *see* Movement Alert List  
 maritime crew visas, 19  
 Maritime Security Identity Cards (MSICs), 20, 25,  
 26, 27  
 Melbourne, 23, 39, 64  
 Message from the Director-General of Security, VII  
 Middle East, IX, 3  
*Migration Act 1958*, 18  
 Minister for Defence, XII  
 Minister for Foreign Affairs, XII, 19  
 Minister for Immigration and Citizenship, 18  
 Movement Alert List (MAL), 18  
 MSICs, *see* Maritime Security Identity Cards

**N**

National Archives of Australia (NAA), 52, 54  
 National Counter-Terrorism Committee (NCTC),  
 21, 36, 37, 38  
 National Counter-Terrorism Plan (NCTP), 36, 37, 38  
 National Critical Infrastructure Database, 22  
 National Information Infrastructure (NII), 21, 22  
 National Intelligence Group, 37  
 National Security Committee of Cabinet (NSC), 59  
 National Security Hotline (NSH), 15, 32  
 national technical cooperation, 39  
 National Threat Assessment Centre (NTAC), X, 15,  
 16–17, 22, 23, 38, 39  
 nationally vital assets, 22  
 NCTC, *see* National Counter-Terrorism Committee  
 NCTP, *see* National Counter-Terrorism Plan  
 Next Generation Border Security initiative, VII, X, 11,  
 19, 20, 35  
 NII, *see* National Information Infrastructure  
 North Africa, 4  
 NSC, *see* National Security Committee of Cabinet  
 NSH, *see* National Security Hotline  
 NTAC, *see* National Threat Assessment Centre

**O**

occupational health and safety, 50, 61  
 Office of National Assessments (ONA), 16, 48  
 Olympic Games, *see* Beijing Olympic and Paralympic  
 Games  
 ONA, *see* Office of National Assessments  
 open source intelligence, 32  
 organisational structure, XV–XVII  
 outputs, XIV, XVIII, 11, 25, 31, 41  
 oversight, XI, XII, XIII, 16, 54, 58–60, 65

**P**

Pakistan, 4  
 Palembang, 5, 6  
 Palestinian Islamic Jihad, 5, 121  
 Parliamentary Joint Committee on Intelligence and  
 Security (PJCIS), 5, 50, 51, 59–60  
 Parliamentary Oversight, 58, 60  
 passport cancellations, 19  
 Pendennis, 23



people development and management, 46–50  
 People's Republic of China, 14, 15  
 performance management, 49  
 performance pay, 49  
 personnel security assessments, VIII, 25, 26, 27–28  
 physical security, 13, 14, 25, 28–29, 66  
 physical surveillance, 31, 32–33  
 PJCIS, *see* Parliamentary Joint Committee on Intelligence and Security  
 PKK, *see* Kurdistan Workers Party  
 PM&C, *see* Department of the Prime Minister and Cabinet  
 PMV, *see* politically motivated violence  
 police, VII, X, XIII, XIV, 4, 6, 12, 13, 14, 15, 16, 17, 20, 21, 22, 23–24, 26, 37, 38–39, 45, 48, 62, 63, 64  
 politically motivated violence (PMV), *see also* terrorism and violent protest, XII, 3, 7, 59  
 Pope Benedict XVI, 14  
 product range, X, 12  
 proliferation, 7  
 promotion of communal violence, XII  
 property management, 22, 55–56  
 proscription, 5, 121  
 prosecutions *see* litigation  
 protection visas, 18, 19  
 protective security advice, XII, 25–30  
 Protective Security Coordination Centre, 29, 37  
*Protective Security Manual* (PSM), 28, 30, 46, 65, 66  
 protest activity, 7, 14, 17, 59  
 PSM, *see* *Protective Security Manual*  
 public statements, 61  
 purchasing, 50

## Q

questioning and detention warrants, 31, 34, 122  
 questioning warrants, 31, 34, 122

## R

RCIS, *see* Hope Royal Commission into Intelligence and Security  
 records management, 52  
 records, release of ASIO's, VII, 45, 52–54, 62  
 recruitment, IX, X, 31, 33, 45, 46, 47, 51, 61, 62

Reed, Justice Geoffrey, KC PJ, XIII  
*Report to Parliament*, XVIII, 61  
 research and development, X, 35–36, 57, 58  
 Research and Monitoring Unit (RMU), 32  
*Review of ASIO Resourcing* (the Taylor Review), IX, 46  
*Review of Interoperability Between the AFP and its National Security Partners* (the Street Review), VII, X, XI, 38–39, 45, 48, 63–64  
 reviews and inquiries, XI, 45, 59, 60, 63–64  
 RMU, *see* Research and Monitoring Unit  
 role and functions (ASIO), XII

## S

sabotage, XII, XIII, 28  
 Samudra, Amrozi, Mukhlas, and Imam, 5  
 SCEC *see* Security Construction and Equipment Committee  
 Science Adviser, X, 36, 57  
 SCNS, *see* Secretaries Committee on National Security  
 Secretaries Committee on National Security (SCNS), 59  
 sectoral threat assessments, 11, 21, 22  
 security audits, 65, 67  
 security clearances, 46, 66, *see also* personnel security assessments  
 Security Committee (ASIO), 57, 58  
 Security Construction and Equipment Committee, 29  
 security consultants, 28, 29  
 security environment, VII, IX, 3, 12, 16, 18, 22, 34, 37  
*Security Equipment Catalogue*, 29  
 Security in Government Conference, 29  
 security intelligence analysis and advice, 11–24  
 security intelligence investigations and capabilities, 31–40  
 security intelligence reporting, 11, 12, 20  
 security of ASIO, 65  
 Seivers, James, 24  
 Senate Standing Committee on Legal and Constitutional Affairs, 60  
 Senior Executive Service (SES), 38, 47, 49, 123, 124, 125  
 Senior Officer Orientation Workshop, 63

separation rate, 45, 46  
SES, *see* Senior Executive Service  
Smith Review, the, *see* *Homeland and Border Security Review*  
South Asia, IX, 3, 4  
South-East Asia, IX, 4–5  
special events, 13–15, 17, 26  
special powers, XII, 32, 33–34, 59, 60, 65  
Staff Association, 49, 57, 58  
staff survey, 52  
staffing profile, 47, 123–124  
state and territory offices, XIV, 38, 45, 55  
Street Review, the, *see* *Review of Interoperability Between the AFP and its National Security Partners*  
Sydney, 13, 14, 23, 26, 39, 56, 64

## T

Taylor Review, *see* Review of ASIO Resourcing  
Technical collection, X, 32, 33, 57  
Technical Support Unit (TSU), 37  
Technical Surveillance Countermeasures, VIII, 25, 28, 29  
telecommunications interception, 33, 39, 45, 54, 64, 65  
*Telecommunications (Interception and Access) Amendment Act 2007*, 45, 64–65  
*Telecommunications (Interception and Access) Amendment Act 2008*, 45, 65  
tendering and contracting, 51  
terrorism, VII, IX, XI, XII, XIII, 3–6, 11, 21, 23–24, 28, 34, 64, *see also* counter-terrorism  
Terrorist Threat Coordination Group, 17  
Threat Assessments, VIII, XIV, 11, 13, 16–17, 21, 22  
Top, Noordin Mohammad, IX, 5  
tracking devices, 33  
training, X, 13, 14, 28, 29, 31, 35, 37, 38, 39, 40, 45, 47–48, 49, 50, 64, 66  
TSCM, *see* Technical Surveillance Countermeasures  
TSU, *see* Technical Support Unit

## U

unauthorised arrivals, 18  
United Kingdom, 64  
United Nations, 5, 7  
United States, 3, 4, 6

## V

vetting, 46, 65  
violent protest, 3, 7, 17, 59  
visa security assessments, VII, 11, 17, 18–19

## W

warrant operations, 61  
warrant(s), XII, 31, 32, 33–34, 41, 59, 61, 65, 122  
Waziristan, 4  
weapons of mass destruction (WMD), 6, 7  
website, VIII, 22–23, 51, 59, 61, 62  
Whole-of-Government, 36, 45, 53  
WMD, *see* weapons of mass destruction  
Workforce diversity, 47  
Workforce statistics, 47, 123  
Workplace Agreement, 49  
workplace harassment policy, 49  
World Youth Day 2008 (WYD), 11, 13, 14–15, 17, 26, 31, 37  
WYD, *see* World Youth Day 2008

## Y

Year in Review, IX–XI