



Australian Government

Australian Security  
Intelligence Organisation

ASIO Submission to the  
Parliamentary Joint Committee on Intelligence and Security:

# REVIEW OF ADMINISTRATION AND EXPENDITURE

No.7; 2007-08

**ASIO**

# **AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION**

---

**Submission to the Parliamentary Joint Committee on Intelligence and Security**

**Review of Administration and Expenditure No 7 (2007–08)**

# CONTENTS

---

Executive Overview .....	4
Introduction and Security Environment in 2007-08.....	8
Expenditure .....	13
Structure of the Organisation .....	17
Direction and Strategic Planning.....	20
Legislative Changes in 2007–08.....	26
Security of ASIO and ASIO Security Assessments.....	28
Human Resource Management .....	37
Accommodation .....	47
Public Relations and Reporting.....	49

# FIGURES

---

Fig 1: Revenue from Government, 2001–02 to 2011–12 .....	13
Fig 2: Financial performance, 2001–02 to 2011–12.....	14
Fig 3: Purchase of capital items .....	15
Fig 4: Organisational structure at 1 July 2007 .....	18
Fig 5: Organisational structure at 30 June 2008.....	19
Fig 6: Corporate governance arrangements.....	22
Fig 7: Resource allocation.....	23
Fig 8: Visa security assessments process .....	31
Fig 9: Visa security assessments, 2001–07 to 2007–08 .....	32
Fig 10: Adverse visa security assessments, 2000–01 to 2007–08 .....	32
Fig 11: Personnel security assessments process.....	33
Fig 12: Personnel security assessments, 2000–01 to 2007–08 .....	34
Fig 13: Qualified or adverse personnel security assessments.....	34
Fig 14: Counter-terrorism security assessments process .....	35
Fig 15: Counter-terrorism assessments by type .....	36
Fig 16: Advertisements from 2007–08 Intelligence Analyst Campaign .....	38
Fig 17: Separations by percentage of total staff and reason.....	40
Fig 18: Age of staff.....	44
Fig 19: Gender balance by classification .....	45
Fig 20: Gender balance by main job family category .....	45

# EXECUTIVE OVERVIEW

---

## THE REVIEW

The Australian Security Intelligence Organisation's (ASIO) submission to the review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into Administration and Expenditure No. 7 provides a detailed account of ASIO's activities during 2007–08 covering:

- the security environment and an overview of 2007–08;
- expenditure;
- the structure of the Organisation and distribution of staff across ASIO;
- direction, strategic planning and pressures of expansion;
- legislative changes that have an impact on administration;
- security of ASIO and ASIO security assessments;
- human resource management;
- accommodation; and
- public relations and reporting.

### *The Security Environment and 2007–08 overview*

The terrorist threat evolved further in 2007–08. ASIO continued to focus on countering the threat from terrorism, while also building on its counter-espionage and counter-proliferation capabilities. Border security remained an important part of ASIO's work, with the continued operation of a 24/7 capability to contribute to border security.

ASIO produced 3,224 formal reports and assessments in 2007–08, including 2,075 Threat Assessments and related products.

### *Expenditure*

ASIO's revenue from Government increased 28% to \$291m in 2007–08, up from \$227m in 2006–07. ASIO recorded a small operating surplus of \$0.3m for the 2007–08 financial year, with break-even results budgeted for 2008–09 through to 2011–12.

Current Forward Estimates for 2008–09, 2009–10, 2010–11 and 2011–12 are \$353m, \$407m, \$413m and \$417m respectively.

The significant increase in ASIO's budget from 2006–07 predominantly arises from the *Review of ASIO Resourcing* (the Taylor Review).

## *Structure of the Organisation*

In 2007–08, an expanded 12 Division organisational structure took effect. In July 2008, ASIO implemented 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.

## *Direction and strategic planning*

ASIO's corporate governance arrangements reflect its needs as an intelligence agency and support critical measurement and evaluation of the Organisation's performance.

In 2007–08, the benefits from refinements made to the corporate governance structure in 2006–07 were evident, including tightly focused committee reporting, more effective performance evaluation and greater transparency.

ASIO's resource allocation across its four reporting outputs was consistent with 2006–07 allocations.

## *Legislative changes in 2007–08*

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

The *Telecommunications (Interception and Access) Amendment Act 2007* received Royal Assent on 28 September 2007. The *Telecommunications (Interception and Access) Amendment Act 2008* received Royal Assent on 26 May 2008.

## *Security of ASIO and ASIO security assessments*

All ASIO permanent staff are security cleared to Top Secret level. ASIO continued to demonstrate best practice by complying with the *Australian Government Protective Security Manual* (PSM) requirement of re-evaluating Top Secret clearance holders within a six-year time frame. During 2007–08, 125 re-evaluations were completed, compared with 118 during 2006–07.

A major review of the (classified) *ASIO Security Instructions* (ASI) was completed in 2007–08. The ASI, which all staff are required to read and apply to their daily work, is now a more user-friendly, comprehensive, ‘living’ document that reflects the contemporary security environment.

ASIO is responsible, under Part IV of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), with furnishing security assessments to Commonwealth agencies for persons seeking access to national security classified information, visas to enter or remain in Australia, Australian citizenship, and for access to controlled areas or materials.

In 2007–08, ASIO completed 21,386 personnel security assessments, which continued a long-term trend of growth in the overall personnel security assessment workload. Two qualified personnel assessments were issued during the year to assist the respective departments in managing potential risks. Adverse or qualified personnel security assessments may be appealed to the Administrative Appeals Tribunal. There were no appeals in 2007–08.

## *Human resource management*

At 30 June 2008, ASIO’s total staffing was 1,492. Net growth 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.

ASIO implemented new and refreshed human resource policies in 2007–08 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 in adjusting to ASIO’s specialised work environment.

## *Staff performance management and evaluation*

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.

## *Accommodation*

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 the period and a secure site office was established to accommodate the project team.

ASIO's capability enhancement 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.

### *Public relations and reporting*

Each year, ASIO produces an unclassified annual *Report to Parliament* as well as a highly classified *Annual Report*. Beyond the *Report to Parliament*, the primary means by which ASIO provides information to the public are through public statements and addresses by the Director-General of Security, public statements through parliamentary accountability processes, its website, and responses to media inquiries through ASIO's Media Liaison Officer.



# INTRODUCTION AND SECURITY ENVIRONMENT IN 2007–08

---

## ASIO'S ROLE

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 ASIO Act. ASIO's primary function is to collect, analyse and disseminate security intelligence. In this context, 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. It 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 the 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 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 the 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) and 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.

## **SECURITY ENVIRONMENT AND 2007–08 OVERVIEW**

### *Counter-terrorism*

Terrorism – particularly by violent jihadists – remained the most significant security threat to Australia during 2007–08. 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.

Globally, in 2007–08, terrorist attacks or incidents affecting Australian citizens 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.

The terrorist threat evolved further during the reporting period. 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.

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. 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.

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

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 some of these individuals, and some were consequently convicted of terrorism offences.

The ability to identify new terrorist capability, tactics, techniques and procedures is an important component of ASIO's counter-terrorism efforts. In 2007–08, ASIO enhanced its ability to provide chemical, biological, radiological, nuclear, and explosive terrorist (CBRNET) weaponry advice. ASIO's worked closely with experts across the Australian Intelligence Community, the Australian Federal Police (AFP), and other parts of Government with responsibility for health, radiological and chemical matters. Although far less prevalent than explosives, terrorist pursuit of chemical, biological, and radiological (CBR) weaponry continues.

### *Violent protests*

Most protest activity in Australia is peaceful and lawful and therefore not of concern to ASIO. However, a small number of individuals consider the promotion and use of violent protest tactics is justified in order to influence government policy or achieve other political ends. The activities of these individuals can fall within the definition of politically motivated violence within the ASIO Act and, therefore, be of interest to ASIO.

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

### *Counter-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).

### *Counter-espionage and foreign interference*

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 this capability through to 2010–11.

In 2007–08, ASIO continued to undertake inquiries and investigations to identify foreign interference – such as clandestine activities by a foreign power to influence governmental processes in Australia, or inappropriate interference in the affairs of expatriates in Australia.

### *Border security*

ASIO plays a key role in Australia's border security arrangements. The prevention of harm to Australian interests relies, in part, on preventing entry to Australia by people assessed to be a threat to security.

In 2007–08 ASIO continued to work closely with the other Australian border security agencies, particularly the Department of Immigration and Citizenship (DIAC) and the Australian Customs Service, to improve visa security assessment processing times and to

ensure that people of security concern are not able to enter Australia. That task continues to increase in complexity as people of security interest become more adept at concealing their identities, activities or intentions.

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

In 2007–08, ASIO completed 72,688 visa security assessments and issued adverse assessments in relation to two individuals seeking entry to Australia. This advice was based on rigorous assessments of the potential threat to Australia's security of allowing these individuals entry.

In 2007–08, ASIO issued two security assessments that resulted in action by the Department of Foreign Affairs and Trade (DFAT) to cancel or deny the issue of a new or replacement Australian passport.

### *Capability enhancements*

2007–08 marked the mid-point of a program – implemented as a result of the 2005 review of ASIO resourcing conducted by Mr Allan Taylor AM – to build capability across ASIO's functions.

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

In 2007–08 ASIO's workforce increased to 1,492. Recruitment remains on track to reach the 2010–11 target of 1,860 staff.

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

ASIO invested \$6.4m in staff learning and development during 2007–08, established a Training Branch under Corporate Management Division and introduced a *Learning and Development Strategy* to provide specialised training in areas such as operations, administration and leadership.

ASIO commenced a major upgrade of its human resource information systems, introducing greater automation of payroll processes and bringing on-line a range of other technology solutions to assist human resource management.

ASIO's budget increased from \$234.8m in 2006–07 to \$291m, and is expected to grow to \$417m in 2010–11.

### *Technology and support to operations*

ASIO continued to expand its Information Technology (IT) facilities in line with its overall strategy of capability enhancements. In 2007–08, ASIO upgraded a number of IT facilities, rolled out new support software, achieved greater connectivity, and made enhancements to audio-visual and video-conferencing capabilities.

An IT Traineeship Scheme was introduced in 2007–08 as part of a 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 to encourage collaboration and capture and share knowledge across ASIO in a way that was not previously possible.

### *The challenge ahead*

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

# EXPENDITURE

## OVERVIEW

ASIO's budget is set out in the Portfolio Budget Statements with the audited outcome published in ASIO's annual unclassified *Report to Parliament*. Portfolio Budget Statements are prepared annually, consistent with the Commonwealth's budgeting requirements. When required, ASIO also prepares Portfolio Additional Estimates Statements – including in 2007–08 – which reflect the updated budget position for the year taking into account funding for new measures approved by the Government since the Budget.

ASIO's outcome, which supports the government's policy aim of a 'secure Australia in a secure region', is:

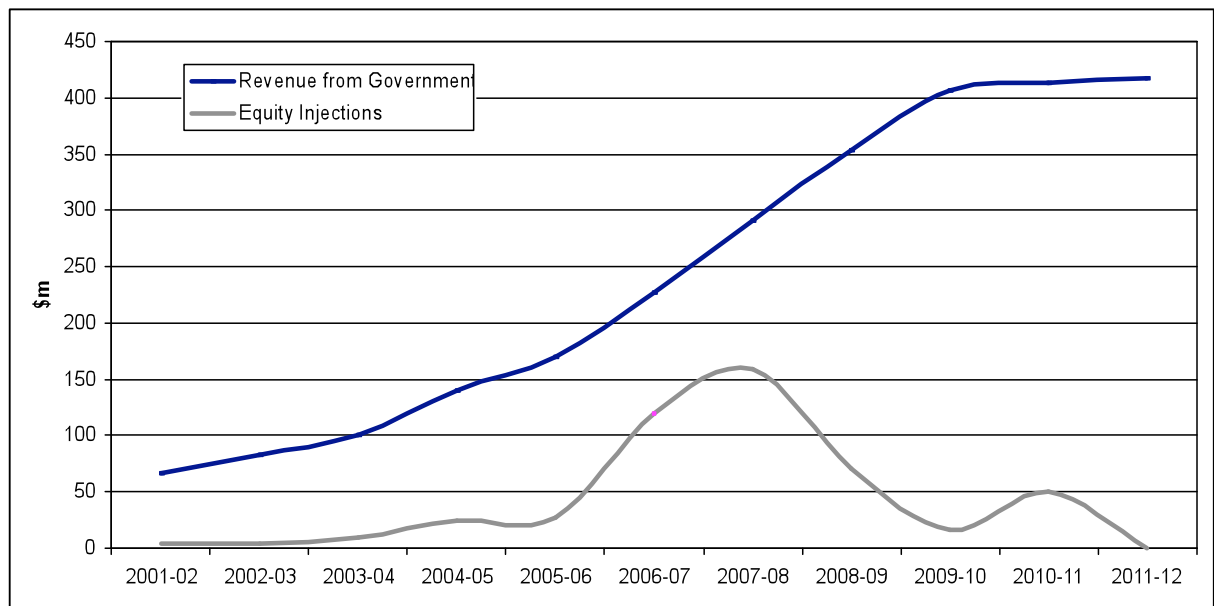
'a secure Australia for people and property, Government business and national infrastructure, and for special events of national and international significance'.

## DEVELOPMENTS/TRENDS

ASIO's revenue from Government increased to \$291m in 2007–08. Forward estimates for 2008–09, 2009–10, 2010–11 and 2011–12 are \$353m, \$407m, \$413m and \$417m respectively.

ASIO's planned equity injections peaked at \$159m in 2007–08. Forward estimates for 2008–09, 2009–10, and 2010–11 are \$71m, \$16m and \$50m respectively, with no equity injection planned in 2011–12.

**Fig 1: Revenue from Government: 2001–02 to 2011–12**



The significant increase in ASIO’s budget from 2006–07 predominantly arises from the Review of ASIO Resourcing (the Taylor Review). The Taylor Review – endorsed by the Government in October 2005 – made recommendations for the further growth of ASIO to cope with existing operational demands and to enhance its ability to analyse the ‘unknowns’ relating to Australia’s security and threat environment. The increase in funding is to allow ASIO to purchase equipment to support growth in the technical operations/surveillance area, to recruit and train new staff, for necessary enhancements to ASIO’s IT infrastructure and for expansion of its international liaison program. The Taylor Review also acknowledged there were necessary additional consequential accommodation requirements to support growth in ASIO’s State and Territory offices.

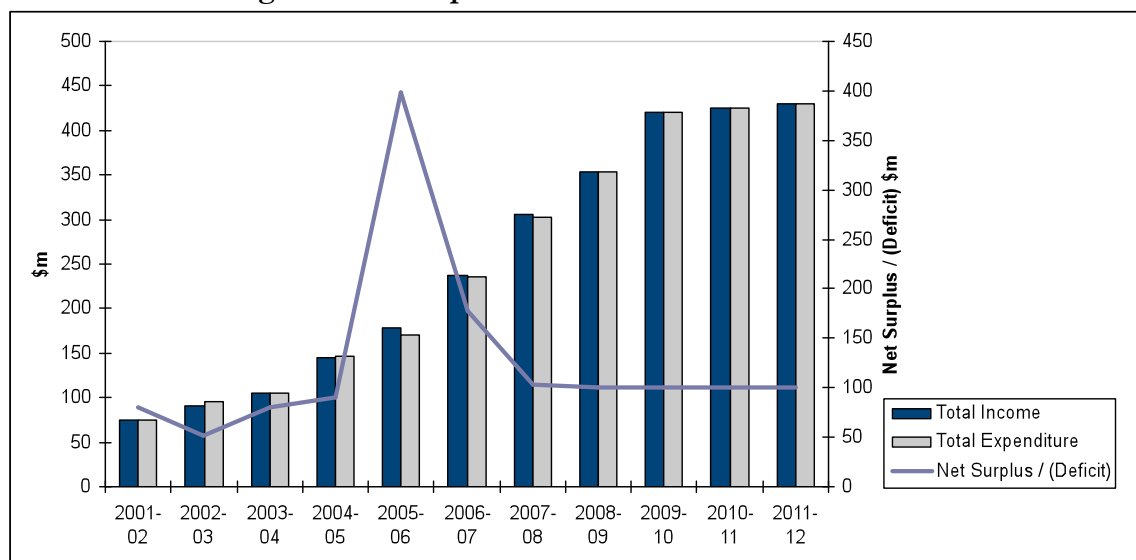
While revenue from Government continues to increase over the forward years, in part to support increased staff numbers, equity injections will decrease as a consequence of the upfront investment in both capability and additional accommodation requirements.

## ASIO’S FINANCIAL PERFORMANCE

ASIO recorded operating deficits from 2001–02 to 2003–04. The ongoing demand for analytical and collection resources and the recruitment and training of new staff were major contributors to the reported losses. In contrast to the deficits, ASIO recorded operating surpluses from 2004–05 to 2007–08, with break-even results budgeted for 2008–09 through to 2011–12. The improved financial performance reflects the easing of budgetary pressures on the Organisation through additional funding from Government in 2004–05.

As shown in the following chart, the 2007–08 financial year saw a small operating surplus of \$0.3m, consistent with the break-even result estimated in the 2008–09 Portfolio Budget Statement.

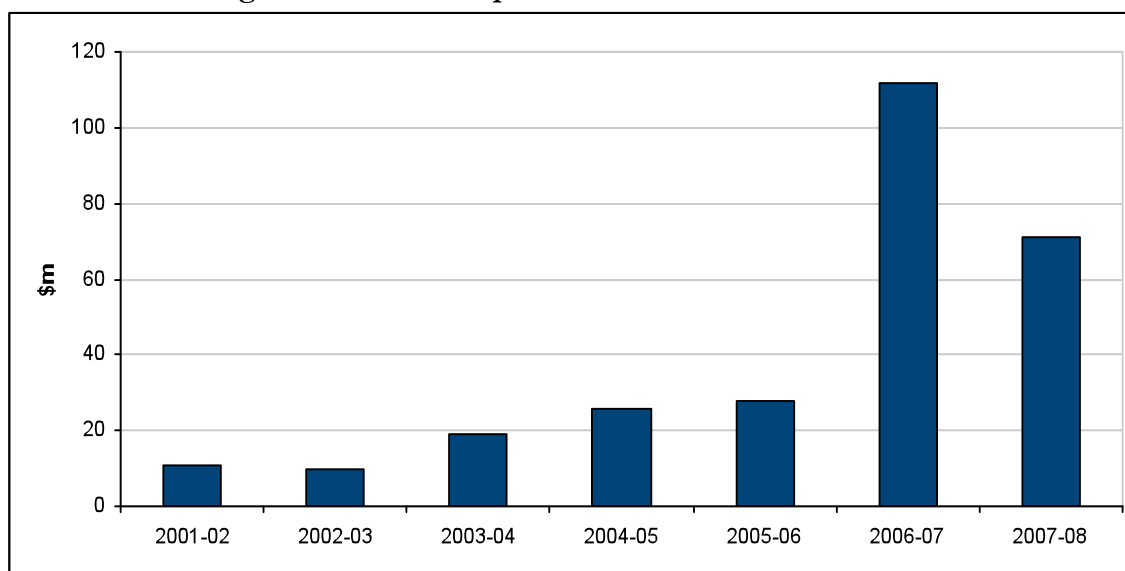
**Fig 2: Financial performance: 2001–02 to 2011–12**



## ASIO'S RESOURCE ALLOCATION

Total full time equivalent staffing numbers increased from 618 in 2001–02 to 1,374 in 2007–08 (with an end point of 1,860 in 2010–11); The proportion of expenditure on employees has, however, slowly decreased over time, to 46% for 2007–08. This is partly a reflection of increased expenditure in IT capabilities and the additional costs involved in providing accommodation and support services for an expanding workforce.

**Fig 3: Purchase of capital items 2001–02 to 2007–08**



The noticeable increase in capital expenditure from 2006–07 has been to provide infrastructure to support ASIO's capability enhancement.

## FINANCIAL MANAGEMENT AND INTERNAL CONTROLS

ASIO prepares annual financial statements in accordance with provisions of section 49 of the *Financial Management and Accountability Act 1997* (FMA Act) and the Finance Minister's Orders. ASIO's financial statements are audited by the Australian National Audit Office (ANAO). As part of that process the ANAO conducts an annual examination of the internal systems and key financial controls of the Organisation. ASIO has not received any adverse audit qualifications from the ANAO as part of its independent audit reporting to Parliament.

Under ASIO's corporate governance and accountability framework, ASIO conducts a range of internal audits and evaluations, overseen by the Audit and Evaluation Committee which is chaired by a Deputy Director-General and includes a senior representative from the ANAO. Each year the Audit and Evaluation Committee approves a strategic internal audit plan which includes a range of mandatory audits undertaken to satisfy the requirements of various state legislation and memoranda of understanding.

The Chief Finance Officer reports monthly to the ASIO Corporate Executive (the main ASIO forum for managing strategic corporate resource issues) on both the present and future financial performance of the Organisation.



Financial performance reporting is underpinned by a robust and reliable financial management information system and a comprehensive suite of management reports, supported by an engaged senior management, ensuring appropriate financial management and accountability across the Organisation.

The increase in ASIO's budget has positioned the organisation well to deliver the significant growth identified as necessary by the Taylor Review. A comprehensive budget management framework is in place to support the delivery of agreed outputs and outcomes, arising from both the Taylor Review and other government initiatives such as the Next Generation Border Security program (see p. 32).

As with other government agencies, ASIO constantly needs to develop and introduce on-going efficiencies to ensure it can continue to meet expectations whilst managing the organisation within agreed financial parameters.

2008–09 will see concerted effort in ensuring resource allocation decisions are aligned with the Taylor Review outcomes, whilst also ensuring sufficient financial flexibility to meet emerging priorities.

# STRUCTURE OF THE ORGANISATION

---

On 1 July 2007 ASIO's organisational structure was expanded to strengthen strategic management oversight of critical work areas. The enhanced structure consisted of 12 ongoing Divisions and one non-ongoing SES Band 2 position, supported by 36 SES Band 1 Managers, up from 28.

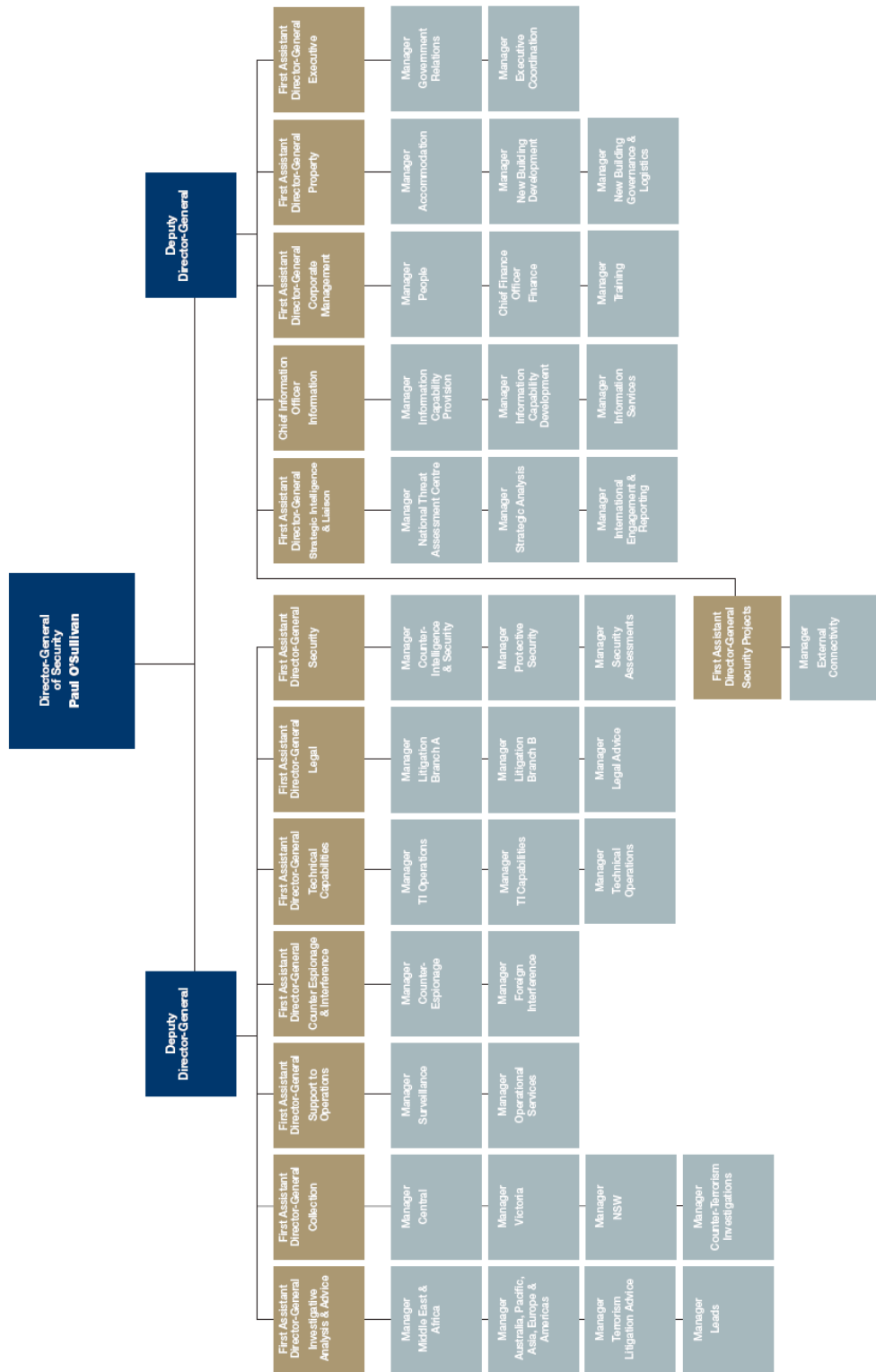
During 2007–08 further adjustments were made, to take effect from 1 July 2008. Executive Division was expanded from two to three branches – Government Relations, Corporate Governance and Corporate Strategy – strengthening further ASIO's strategic planning, priority setting, and governance framework. Executive Division plays a central role in strengthening engagement with key partners and supporting ASIO's contribution to government policy initiatives and reviews.

Reflecting the increased workload and complexities emerging in this important area, Counter-Espionage and Interference Division was expanded to incorporate an additional Branch – Foreign Intelligence Support.

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 temporary position of First Assistant Director-General Security Projects was discontinued. The important work of this area will be carried forward by External Connectivity Branch, which will be absorbed within Security Division.

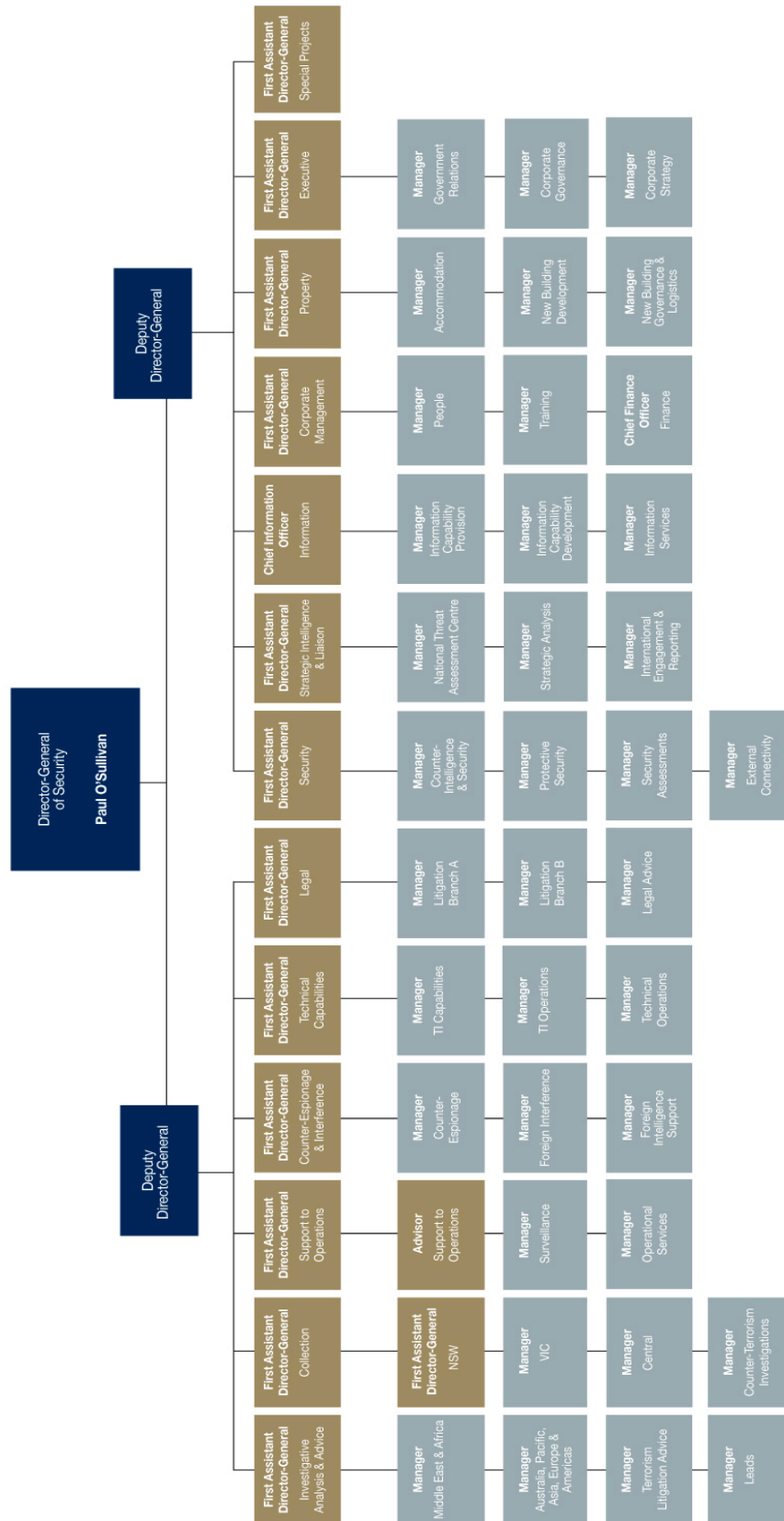
A new temporary position, First Assistant Director-General Special Projects, oversees a range of critical and high-level initiatives, and implementation of review outcomes.

**Fig 4: Organisational structure at 1 July 2007**



# ASIO – SES Structure

Fig 5: Organisational structure at 30 June 2008



# DIRECTION AND STRATEGIC PLANNING

---

## 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 place 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-General's Meeting (DGM) and the twice monthly Corporate Executive (CE) meeting.

The DGM 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 high-level attention.

The CE 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 DGM and the CE oversee eight ongoing corporate committees, as well as one non-ongoing committee (for 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 ANAO. 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.

**Fig 6: ASIO's corporate governance arrangements**



## **CORPORATE PLANNING**

ASIO's Corporate Plan 2007–2011 sets the broad framework for how ASIO does its business, measures its performance and achieves its outcomes. It sets out the critical success factors driving ASIO, maps out where ASIO needs to be in 2012 and provides a guide to meeting the expectations of the Government, Parliament and Australian community.

## **ORGANISATIONAL PERFORMANCE MANAGEMENT**

ASIO's organisational performance management framework is comprehensive and multi-faceted. Regular performance reviews inform senior management of trends and pressure points and provide an objective basis for managing risk.

ASIO conducts an annual survey of key clients, seeking feedback on the quality and effectiveness of ASIO's engagement, reporting and product. In 2007–08 clients were also asked for any specific initiatives and/or improvements that could be made to strengthen further and expand their engagement with ASIO.

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

## STRATEGIC ALLOCATION OF RESOURCES

As Australia's security intelligence service, ASIO provides a unique and valuable service to the Government and the people of Australia. Its business is fundamentally one of collecting and analysing information, and reporting it to others so that they may act to protect Australia, Australians and Australian interests. So that it is well-placed to provide the best-quality advice – now and into the future – ASIO must continue to develop its capabilities, (both technical and human, and collection and analysis). Resource allocation across the Outputs is classified and was consistent with previous years.

**Fig 7: Resource allocation, 2002–03 to 2006–07**

Output	2003–04	2004–05	2005–06	2006–07	2007–08
Output Group 1: Security Intelligence	\$103.023m	\$142.449m	\$181.099m	\$234.764m	\$304.109m

Counter-terrorism security checking and protective security advice is undertaken on a cost-recovery basis and the allocation of resources is driven by customers. Work for DIAC on unauthorised arrivals is also customer-funded and driven.

Between February and May each year, the CE approves the internal budget in order to allocate divisional base budgets. In addition to base budgets, ASIO also allocates funds to internal projects – these are considered by the CE in this same period, with not all being approved.

The allocation of New Policy Proposal (NPP) funding is exercised strictly in accordance with NPP implementation plans developed internally by the relevant functional areas for each initiative and approved by the CE or the DGM. Divisional base budgets, internal projects and NPPs are monitored and driven by the CE on a monthly basis.

## AUDIT, EVALUATION AND FRAUD CONTROL

ASIO has a proactive program of audit and fraud control which includes a dedicated Audit and Evaluation Committee that reports to the Director-General of Security. In addition to financial and asset fraud auditing and control, ASIO audits use of assumed identities that support intelligence operations.

During 2007–08, an internal review of the Audit and Evaluation Committee was conducted in accordance with the 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 was finalised after the reporting period, and was also not proven.

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 have 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.

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 & 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 have been 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 were provided to the IGIS.

# LEGISLATIVE CHANGES IN 2007–08

---

## LEGISLATIVE DEVELOPMENTS

ASIO continued to liaise with Commonwealth departments and agencies on policy development and proposed legislative amendments relevant to ASIO's functions. ASIO also continued to foster close working relationships within government to ensure that the legislative framework supports ASIO's functions and capabilities.

The following legislative developments relevant to ASIO's technical capabilities occurred during 2007–08.

### *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. The Amendment Act 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 1979* (the TIA Act).

The Amendment Act 2007 makes a distinction between access to historical data (data already in existence at the time of the request) and prospective data (data collected as it is created and forwarded to the agency in near real time).

- With the 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 exists – that is, where access to telecommunications data is no longer connected with or necessary for the performance of ASIO's 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. The key changes made to the TIA Act by this amendment Act include:

- extending the network protection exceptions for specified agencies (including ASIO) until 12 December 2009. These provisions allow specified agencies to monitor all

- communications within their corporate networks, for the purpose of protecting and maintaining their networks and maintaining their professional standards; and
- clarifying the ability of ASIO to intercept multiple telecommunication devices on a single named person warrant.

### *The role of Legal Division*

Legal Division plays a central role in the use of ASIO's special powers. The Warrants Documentation Directorate is responsible for the management of the warrants process, and lawyers from the Division review every warrant request prior to its consideration by the Attorney-General.

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 the prosecution.

### *Training*

Legal Division regularly provides training to new officers and targeted training regarding the use of special powers and, more generally, the ASIO Act and other relevant legislation.

### *Use of ASIO's special powers*

Under the ASIO Act and the TIA Act, 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.

No questioning warrants were sought in 2007–08.

# SECURITY OF ASIO AND ASIO SECURITY ASSESSMENTS

---

## SECURITY ASSESSMENTS AND VETTING OF ASIO STAFF

### *Current Procedures*

All ASIO officers and others who work in the Organisation are cleared to a TOP SECRET positive vetted (TSPV) level if they are to have access to ASIO IT systems. Assessing individuals for their suitability to be granted such a clearance is done in accordance with the PSM and its (classified) supplement and is necessarily a lengthy process. ASIO has sought to minimise the impact of this process on the timely recruitment of applicants.

- ASIO developed a Diploma of Personnel Security (Vetting) for AIC agencies in cooperation with other AIC agencies and the Canberra Institute of Technology.
- An external review of recruitment and vetting practices was conducted to identify efficiencies and process improvements. Implementation of the recommendations contained in the (classified) report submitted by the review team commenced in 2008 and will continue to be implemented into 2008–09.

### *Timelines*

ASIO endeavours to complete the TSPV security assessment process within a 16 week period. In practice, vetting timeframes can range from as little as eight weeks through to in excess of six months, particularly for applicants who have complex backgrounds, or when there are matters that need to be resolved. Other causes of delays in the vetting process include:

- applicants who do not provide information in a timely manner or who do not make themselves available to attend interviews due to work and/or personal commitments;
- logistics and resource implications in vetting applicants outside of Canberra;
- delays in information from relevant Commonwealth and state agencies and other institutions;
- the geographic location, availability and cooperation of applicants' referees;
- complexities associated with mitigating identified security-related vulnerabilities; and
- the relative priority for vetting particular applicants.

### *Revalidation and re-evaluation program*

ASIO staff are also required under the PSM to undergo a revalidation/re-evaluation program to ensure that they remain suitable to access national security classified material.

The revalidation/re-evaluation program continues throughout the life of the clearance. Clearance holders must be re-assessed as remaining honest, loyal, trustworthy, mature and tolerant through a process of psychological testing, police and financial checks, multiple referee appraisals and workplace assessments.

In 2007–08 ASIO completed 125 re-evaluations of security clearances, compared with 118 in 2006–07.

## **E-SECURITY ARRANGEMENTS AND ENHANCEMENTS**

ASIO provided input to a whole-of-government review of Australia’s e-security policies, programs, and capabilities in 2007–08. The review, led by the Attorney-General’s Department, was ongoing at the conclusion of the reporting period. ASIO’s contribution emphasised the importance of a balanced approach to e-security through implementation of appropriate administrative and personnel policies and procedures, protective security measures, and effective e-security awareness activities.

In light of the potential e-security threat to ASIO’s systems, ASIO’s IT Security sections implemented several measures to mitigate risks to ASIO systems, including those externally connected. These include:

- targeted ICT security education programs for ASIO staff, ICT staff and ICT contractors;
- enhanced audit and investigation capability across ASIO ICT systems, including real-time monitoring and response;
- an active program of ICT systems review for security vulnerabilities, and provision of remediation recommendations;
- development and review of new and existing internal ICT Security Policies; and
- provision of ICT security advice, including advice in response to general enquiries and design, development, and implementation advice to ICT projects.

ASIO continued to collaborate with other agencies to strengthen Australia’s e-security.

## **SECURITY ASSESSMENTS**

ASIO is responsible, under Part IV of the ASIO Act, for furnishing security assessments to Commonwealth agencies, including for:

- access to security classified material (*personnel security assessments*);
- access to places or activities controlled on security grounds (eg. maritime and aviation security identity cards, Australian Nuclear Science and Technology Organisation, ammonium nitrate programs, counter-proliferation programs) (often referred to as *counter-terrorism checks*);
- entry into Australia or to remain in Australia (*visa security assessments*);
- applications for Australian citizenship; and
- the cancellation of Australian passports or the seizure of foreign passports (often called *passport cancellations*).

In making a security assessment ASIO draws on relevant classified and unclassified intelligence and considers the person's activities, associates, attitudes, background and character, and the credibility and reliability of any information available to ASIO. The assessment process may also include an ASIO interview of the applicant to provide them with an opportunity to resolve issues of concern.

ASIO is required to limit the factors underpinning security assessments to grounds related to 'security' as it is defined in the ASIO Act. (Other factors, such as health or criminal history – where there is no security nexus – are not within ASIO's remit.)

On completion of an assessment ASIO provides one of the following types of advice to the requesting agency:

- a *non-prejudicial* assessment, which does not recommend against the proposed action;
- a *qualified* assessment, which does not recommend against the proposed action but includes information ASIO considers may be relevant to the agency's decision to help minimise an identified potential risk; or
- an *adverse* assessment that recommends against the proposed action.

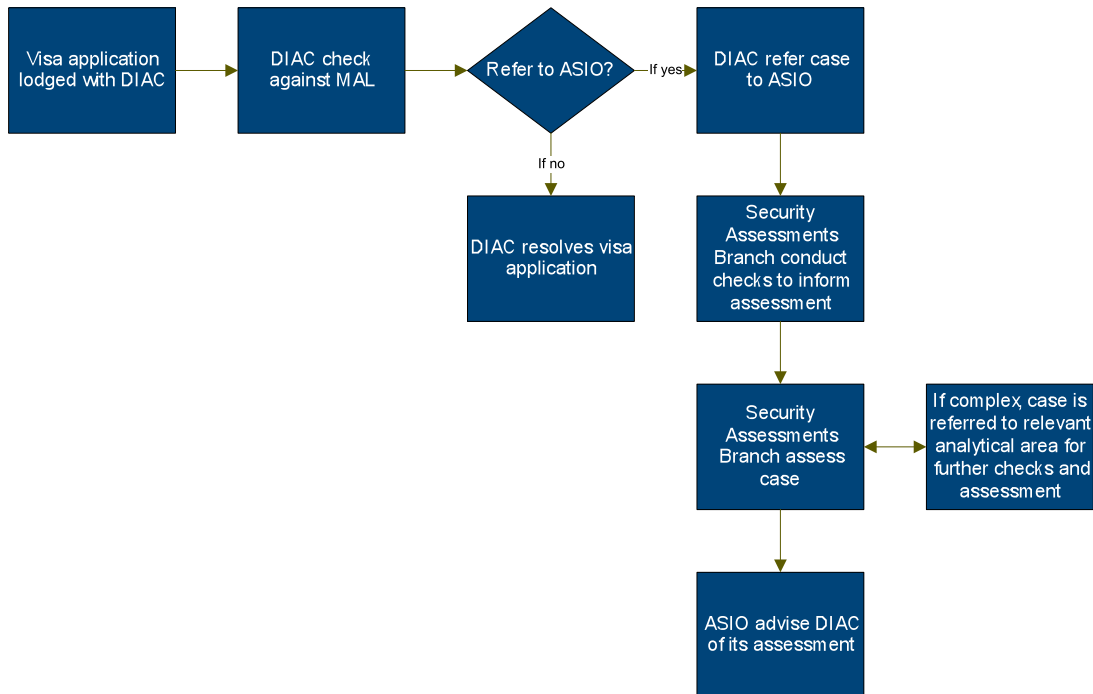
Requesting agencies then make a determination, based on ASIO's security assessment as well as the agency's own assessment. Any administrative action taken in response to an ASIO assessment is the responsibility of the requesting agency – ASIO is not responsible for granting or denying security clearances, visas, or the like. In some circumstances (such as personnel security assessments) the requesting agency has some discretion in determining the nature of the administrative action arising from an adverse or qualified security assessment. However, in other cases (such as most security assessments for visa purposes) the requesting agency is obliged to act upon ASIO's security assessment.

Qualified or adverse ASIO security assessments may be appealed to the Administrative Appeals Tribunal, if the applicant is an Australian citizen or permanent resident, or holds a special category visa or special purpose visa. Visa applicants are, however, entitled to file an application in the Federal Court and seek judicial review in respect to an adverse security assessment.

## Visa security assessments

Any person applying for a visa to travel to – or remain in – Australia may have their application referred by 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).

**Fig 8: Visa security assessment process**



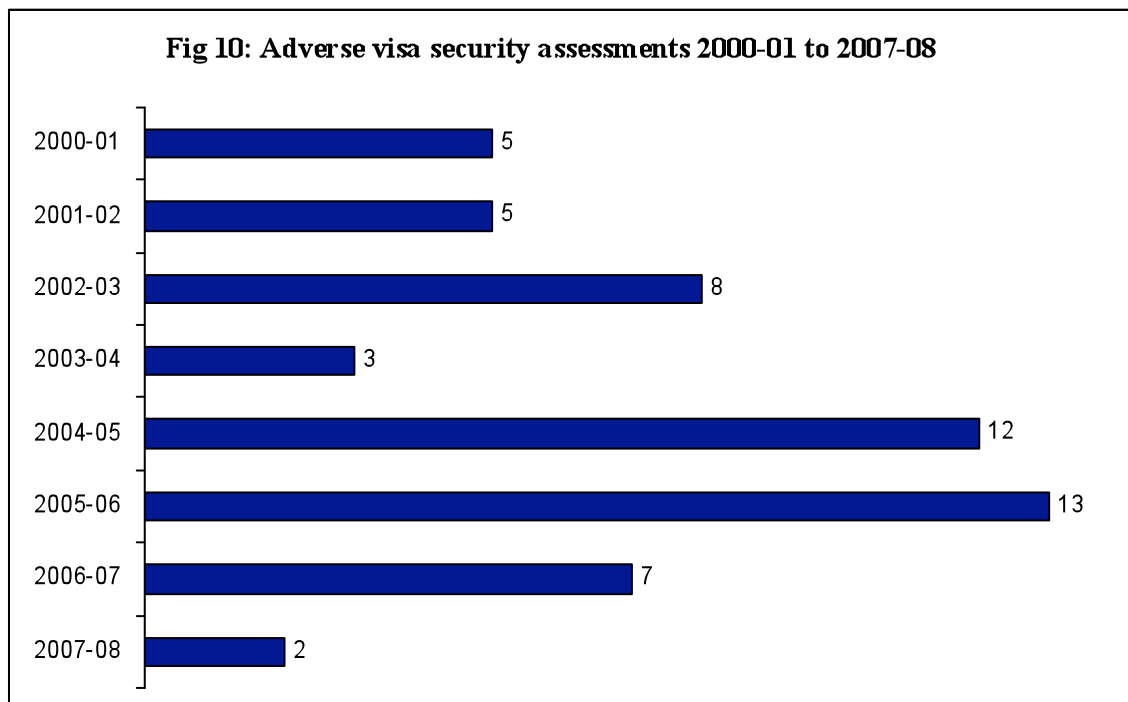
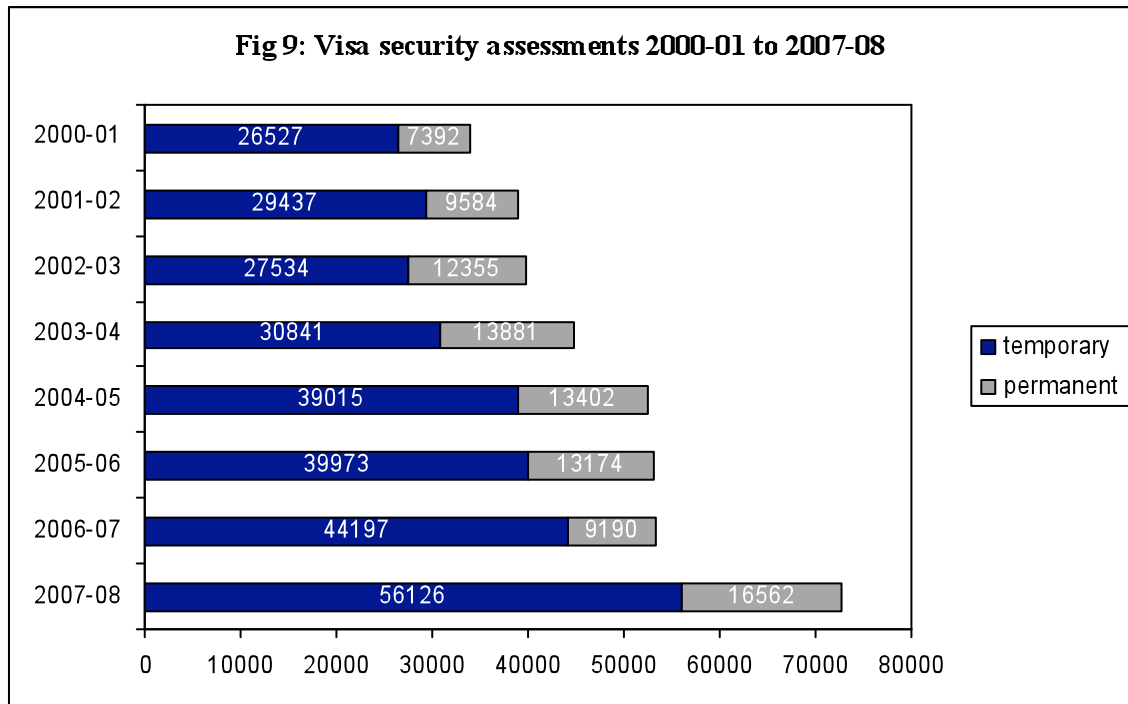
Visa security checks are generally managed in order of referral from DIAC, taking into account any agreed priority caseloads, with particular emphasis on the refugee, humanitarian and protection caseloads and genuine compassionate or compelling cases. The prevailing security environment and the increasing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

ASIO and DIAC work closely at the operational, policy and management levels to identify initiatives that improve processes for managing increasing caseloads and service standards.

ASIO reduced substantially the time required to complete visa security assessments in 2007–08. This reflected ASIO’s ongoing improvement of processes, careful 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 electronic processes for certain temporary visa referrals through the establishment of electronic connectivity between DIAC and ASIO. This connectivity, known as the Security Referral Service (SRS) delivers significant improvements in the security assessment process, enhancing the auditing and tracking of cases and improving processing times.



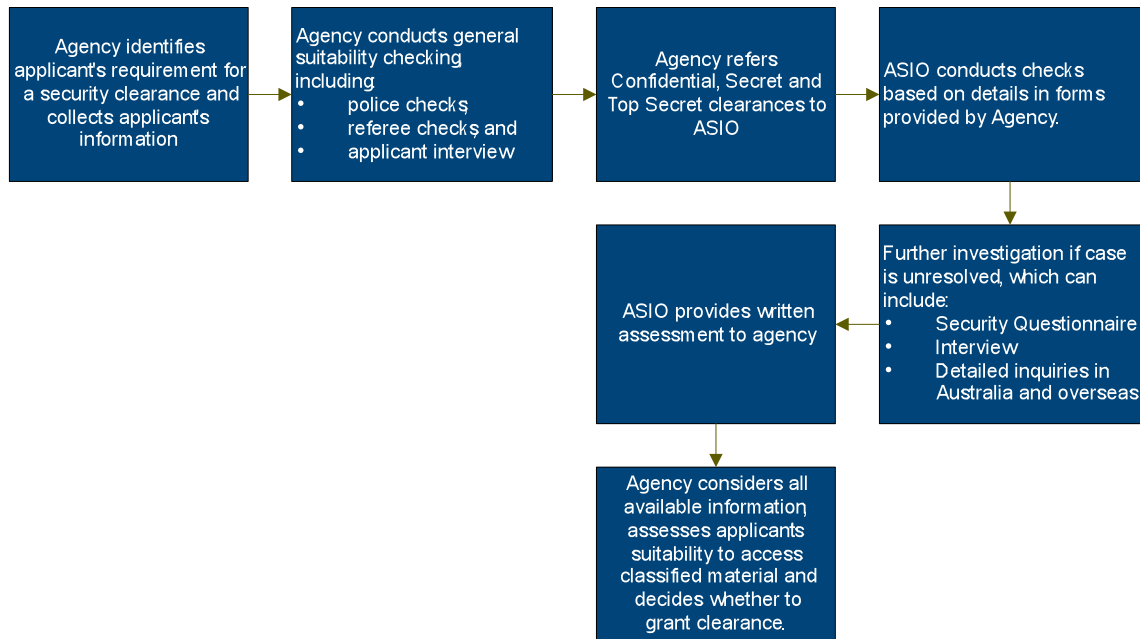
In 2007–08 ASIO issued adverse assessments on two visa applicants who were assessed by ASIO to pose a direct or indirect risk to security.



## Personnel security assessments

ASIO undertakes personnel security assessments at the request of other agencies as part of the vetting process to determine whether an individual is suitable to have access to national security classified material. ASIO's role in the process is to determine whether anything in the candidate's background or activities is cause for security concern.

**Fig 11: Personnel security assessment process**



ASIO does not assess general suitability for the access proposed, nor does it issue security clearances for other agencies. This remains the responsibility of the requesting agency. ASIO's assessment is considered by the requesting agency, in conjunction with information gathered from other avenues such as interviews and referee checks, in determining the applicant's suitability and approving the issue of a security clearance.

The majority of ASIO's security assessments are resolved based on material provided by the requesting agency. If there are issues of potential security concern, ASIO may conduct interviews or make other inquiries.

As part of ASIO's ongoing efforts to improve service, it is establishing direct connectivity arrangements with primary clients, including the Defence Security Authority. These refinements will enhance administrative processes and reporting arrangements.

Fig 12: Personnel security assessments 2000–01 to 2007–08

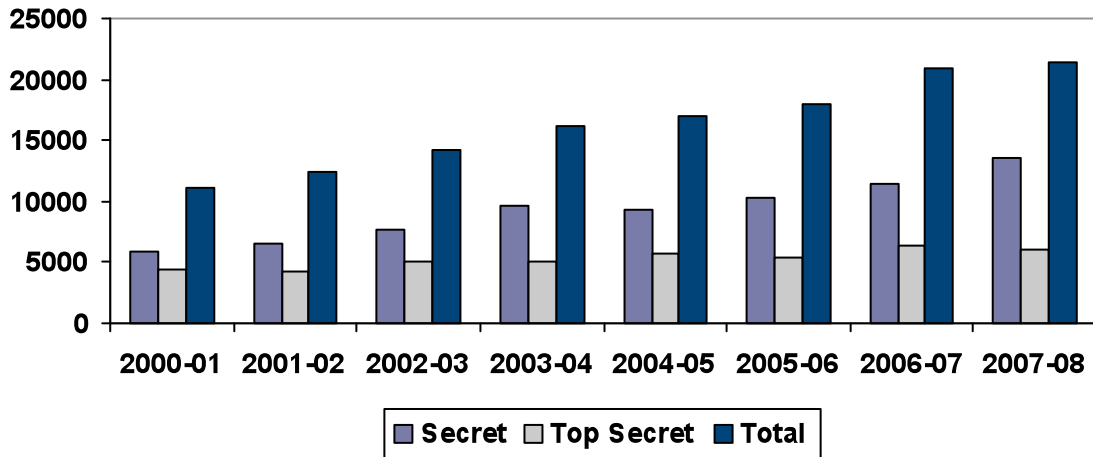


Fig 13: Qualified or adverse assessments 2000–01 to 2007–08

	2000-01	2001-02	2002-03	2003-04	2004-05	2005-06	2006-07	2007-08
Qualified	10	6	3	2	1	0	1	2
Adverse	2	3	2	0	0	0	0	0
Total	12	9	5	2	1	0	1	2

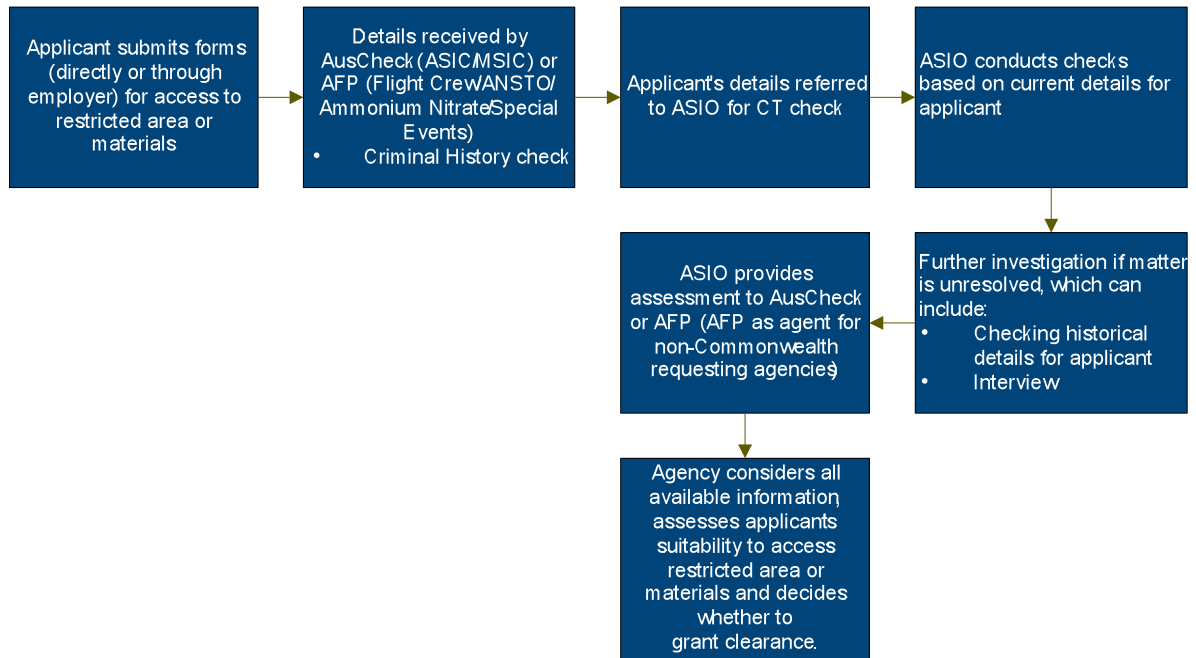
### *Counter-terrorism security assessments*

ASIO’s counter-terrorism security checks are carried out at the request of government authorities who are responsible for accreditations, predominantly the 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).

The counter-terrorism security checking program comprises checks in relation to:

- ASICs;
- MSICs;
- ammonium nitrate licensing;
- Australian Nuclear Science and Technology Organisation (ANSTO) staff;
- flight crew; and
- special events such as Asia-Pacific Economic Cooperation (APEC) forum and World Youth Day 2008.

**Fig 14: Counter-terrorism security assessment process**



ASIO completed 89,290 counter-terrorism security assessments in 2007–08, 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;
- 4,502 security assessments for persons requiring licences to access ammonium nitrate;
- 1,251 security assessments for staff and visitors to the ANSTO facility at Lucas Heights, Sydney; and
- 13,453 security assessments for persons requiring accreditation for special events such as the APEC forum and World Youth Day.

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

There has been a 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 a 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.

**Fig 15: Counter-terrorism assessments by type**

<b>Type of check</b>	<b>2003-04</b>	<b>2004-05</b>	<b>2005-06</b>	<b>2006-07</b>	<b>2007-08</b>
ASIC and MSIC	58147	38466	71733	118118	70084
Ammonium Nitrate	-	1634	7428	6419	4502
ANSTO	-	-	-	1027	1251
Commonwealth Games	-	-	56149	-	-
G20 Finance Ministers' Meeting	-	-	-	1580	-
APEC	-	-	-	7837	9349
World Youth Day 2008	-	-	-	-	4104
<b>Total</b>	<b>58147</b>	<b>40100</b>	<b>135310</b>	<b>134981</b>	<b>89290</b>

# HUMAN RESOURCE MANAGEMENT

---

## RECRUITMENT

A buoyant employment market in 2007–08 meant that it was the most challenging year in recent times for the recruitment of new staff and the retention of existing staff. While ASIO recruited 285 new staff this resulted in a net growth of 136, against a target of 170, to reach a staffing level of 1,492 by 30 June 2008. ASIO's focus continued to be on building the intelligence-focused areas while maintaining capability in the enabling functions. In particular, the recruitment of Intelligence Officers and Intelligence Analysts remained challenging.

Legal functions received a much needed boost to meet the demands of a continuing heavy litigation load.

Other job families in the intelligence-focused areas generally saw modest increases while job families within the enabling functions also saw modest increases or remained static.

### *Advertising and marketing*

ASIO has engaged the services of TMP Worldwide to assist with candidate management for the larger campaigns. In 2007–08 ASIO extended this relationship into marketing and advertising with a view to refreshing and reinvigorating its advertising campaigns. TMP developed the advertising strategy and concepts for the Surveillance Officer, Intelligence Analyst and Intelligence Officer campaigns. The revised strategy included the use of radio, an increase in information available online through ASIO's website, and a sharpened focus on selected national print media and other cost effective options, including job boards, news sites, postcards, and digital displays. These campaigns resulted in strong fields of applicants and the resulting recruitment processes during 2007–08 have contributed directly to the increased number of commencements of these job families in the early part of 2008–09.

This multi-faceted strategy was also successful in attracting applicants from a wider cross-section of the Australian community, including from individuals who had not previously considered a career with ASIO. ASIO has continued to work with TMP to develop a longer term advertising strategy with a view to positioning ASIO as an employer of choice for high calibre applicants over the next three to five years at least.

The overall cost of ASIO's advertising in 2007–08 was \$2.192m, up slightly from \$2.126m in 2006–07. As ASIO develops further its advertising strategy into 2008–09 and beyond it expects to reduce expenditure on advertising by relying less on expensive print media and more on online and other electronic forms of advertising.



**Fig. 16: Advertisements from ASIO's 2007–08 Intelligence Analyst campaign**

ASIO is also seeking to sharpen and strengthen its focus on recruitment from universities and other tertiary institutions that offer courses consistent with ASIO's requirements across a range of job families.

## RETENTION

ASIO is committed to retaining high calibre staff members and has a number of strategies that it employs to facilitate this outcome.

### *New Employee Support Officer scheme*

In 2007–08 ASIO introduced a new initiative to assist new starters in settling in to the Organisation. A New Employee Support Officer (NESO) is a support person outside the new employee's immediate work area who can provide informal support and guidance immediately after commencement. NESOs are approved volunteers who have been with the Organisation for at least one year and who have a broad appreciation of its work. NESOs initiate contact with their new starter in the first week with a view to meeting informally soon after. NESOs are able to provide advice and guidance on minor administrative matters or, in some cases, have been able to flag more significant settling-in issues with a view to engaging line managers or other support mechanisms to ease the transition.

### *Mature age employees*

ASIO is investigating a number of initiatives aimed at retaining critical capabilities, including the retention of mature staff members who are approaching retirement age. Possibilities include phased retirement, part-time work, project work or other tasks that can draw on their expertise and skills.

## *Updated human resource policy framework*

In 2007–08 ASIO commenced a program of reviewing and updating all its human resource (HR) policies and delegations. The rapid growth of the Organisation, from 805 staff members at 30 June 2004 to its 30 June 2008 total of 1,492 staff members, has meant that a number of human resource policies and practices that were appropriate for a smaller organisation are not necessarily as applicable in an organisation that has now doubled in size and is still growing.

The first stage of this project involves updating the language in the policy documents to reflect current terminology and designations, improving the format to enhance readability, and placing them on the Organisation's online communication tools to make them more readily accessible. Around 50 policies required review, and six had been reviewed and accepted by management by 30 June 2008. The review of the remaining policies is scheduled for completion in early 2009.

The second stage of this project will involve a more strategic review of key policies, including against the background of negotiations for the next workplace agreement, to ensure that ASIO's HR policies contribute to its wider attraction and retention strategies and remain relevant to the needs of a larger organisation.

## *Separation rates*

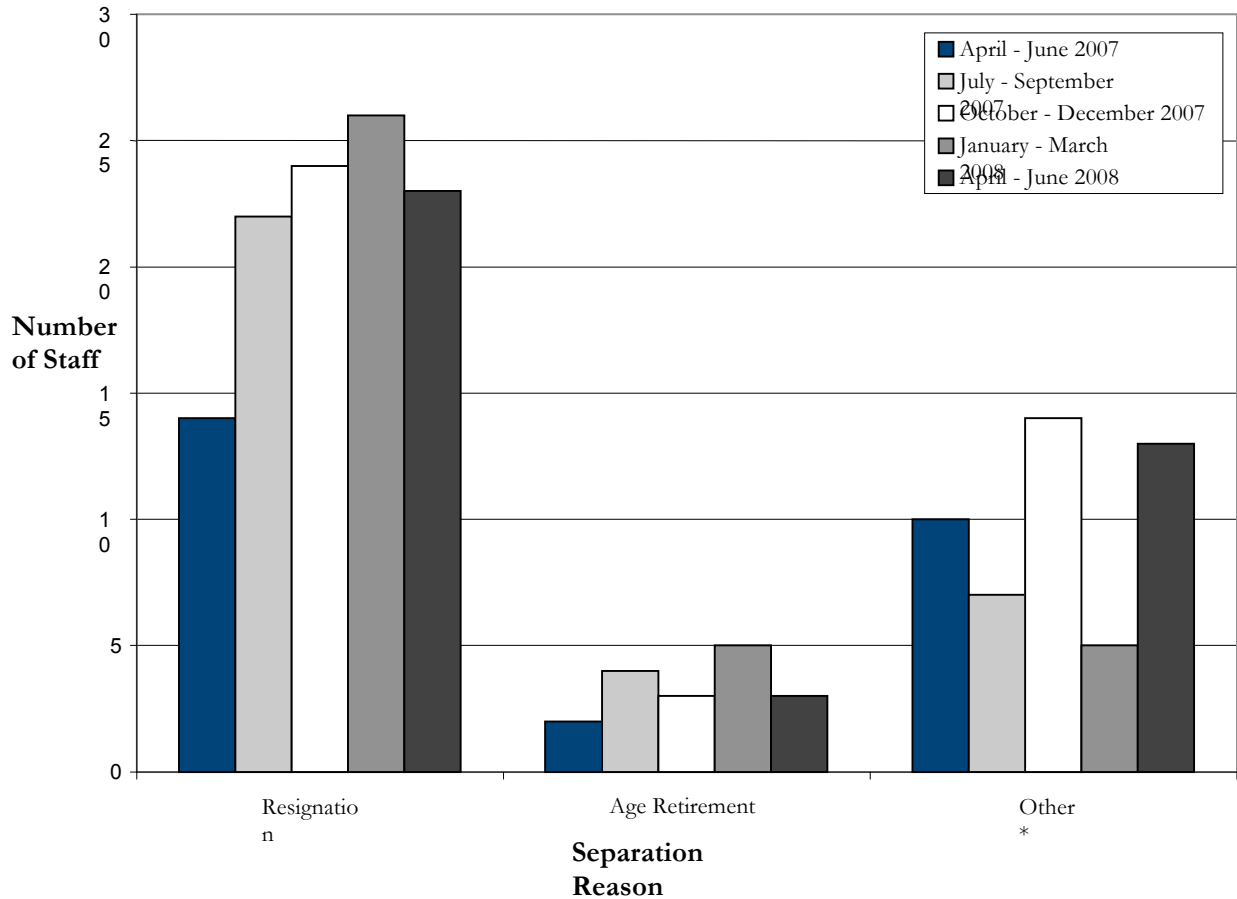
In 2007–08 there were a total of 149 separations. The average length of service for those who resigned was 3.79 years and the median was 3.15 years.

The separation rate at 30 June 2008 for the previous 12 months was 7.6%. This was a 0.7% increase from the rate at 31 March 2008 (for the period 1 April 2007 to 31 March 2008) of 6.9%. The rate compares favourably to the Australian Public Service (APS) separation rate of 8.2% as of 30 June 2008 (*State of the Service Report 2007–08*).

Age retirements were steady over 2007–08, and while resignations decreased in the June quarter compared to the January and March quarters, they were higher compared to the same period in 2007.



**Fig 17: Separations by percentage of total staff and reason**



\* Including end of attachments and contract expiries.

ASIO’s human resource area conducts voluntary exit interviews, with around half of all separating staff choosing to participate. Reasons cited by separating staff include promotion/career opportunities, work/life balance issues, job satisfaction issues, retirement and a range of personal reasons. The exit interview process did not reveal any systemic concerns requiring management response.

## **TRAINING AND STAFF DEVELOPMENT**

The training and development of ASIO staff is particularly important in a growing workforce and remained a high priority for both newly recruited staff and those who have been with the Organisation for some time.

### *Developments/ trends*

During 2007–08 the implementation of the recommendations from ASIO’s 2006–07 evaluation of training and development strategies continued. A Training Branch was established on 1 July 2007. ASIO has endorsed a Learning and Development Strategy which

underpins all training course development and delivery, tying programs to business user needs. This:

- provides mechanisms for the identification of corporate training priorities and the allocation of resources to support these priorities;
- allows for the evaluation of the effectiveness of training activity; and
- supports managers and staff, through performance management arrangements, in identifying, prioritising and delivering on training needs.

The Learning & Development Strategy provides the mechanisms to identify the knowledge and skills staff need to fulfil ASIO's vision and mission and the methods through which this knowledge and skill should be developed, maintained, evaluated and reported on.

ASIO also introduced a new study initiative in 2007–2008, to help build ASIO's strategic capability and develop specific tertiary skills. ASIO afforded up to 13 high potential individuals the opportunity to undertake post-graduate opportunities for up to one year on a full-time basis. This initiative, which is fully funded by ASIO, is an investment in ASIO's future and will provide high calibre staff with an avenue to undertake advanced career and personal development activities.

The content and structure of the Intelligence Officer Traineeship also continues to be refined to ensure it remains effective and appropriate to the security environment, and also in light of the expanded trainee intake.

### *Corporate training programs*

ASIO provides targeted specialised training for officers engaged in specific roles across the Organisation. This training ensures ASIO's staff members are appropriately skilled and underpins ASIO's career development strategy. Corporate training activities include:

- comprehensive induction program for all new starters;
- administrative training – contract management, project management, staff selection skills, presentation skills, trainer training, interviewing skills, strategic thinking, communication, finance and budgeting;
- IT training – basic and advanced training in the use of ASIO's computer systems;
- ethics and accountability – all members of staff are required to attend at least once every three years;
- discipline-specific courses covering subjects such as Islamic history and culture, and the political and social drivers of terrorism;
- Studies Assistance Program – supporting tertiary study by members of staff; and
- the Director-General's Study Bursaries – supporting members of staff who achieve outstanding results in their studies while maintaining high levels of work performance.

### *Management and leadership skills*

ASIO continues to place a strong emphasis on the development of its Senior Executive Service (SES) and Senior Officers. A full range of leadership and management development activities continues to be offered. The orientation program developed in 2006 for newly

appointed or promoted Senior Officers has been reviewed and updated to ensure that new Senior Officers continue to have solid understanding of their responsibilities in the current context. Leadership and management learning and development also involved:

- three SES forums which focused on managing Organisational growth, corporate planning, whole-of-government activities and legal challenges. These programs are addressed by leading academics and practitioners in a range of fields; and
- two combined SES and Senior Officer forums, which considered a range of Organisational issues such as legal issues, Organisational priorities and plans, and upgrades to technical capabilities.

### *Performance management*

Enhancements to ASIO's Performance Management Framework in 2007–08 included greater automation of the process and the introduction of a four point rating system. These enhancements resulted in higher levels of compliance with around 93% of staff members having a current performance agreement in 2007–08.

The introduction of the four point rating scale has allowed line managers to address underperformance matters in a more informal manner by working with the staff member over a defined period before being required to enter a formal underperformance process.

### *Australian Intelligence Community training*

ASIO supports the continued efforts to broaden the understanding of whole-of-government approach to intelligence needs and partnerships. This includes providing presenters and participants to the Induction, Senior Officer Development Programs and Working in the AIC Programs.

### *Response to Street Review recommendations*

In response to the *Review of Interoperability between Australian Federal Police (AFP) and its National Security Partners* by Sir Laurence Street AC KCMG QC, a joint training committee with membership from the AFP, Commonwealth Director of Public Prosecutions, and ASIO has been established. This committee will oversee the development, implementation and delivery of ASIO training modules aimed at providing ASIO Intelligence Officers with an understanding of evidentiary and prosecutorial methodology and how it applies in the ASIO context, and the AFP and CDPP – their structure, roles and responsibilities.

There will also be modules designed for the AFP, including training in the handling and protection of classified and sensitive information and intelligence, and ASIO's structure, role, responsibilities and methodology.

The bulk of this training will be delivered in 2008–2009.

## *Language training*

ASIO continues to invest in language skills, including:

- full time training in languages relevant to ASIO's investigative work;
- comprehensive language training for ASIO Liaison Officers involving full time language course with DFAT, including one-on-one tutorials, small group learning and 'in-country' training; and
- training for ASIO's Linguists to refine and enhance their skills.

## *Workplace diversity*

ASIO's staffing profile compares favourably with that of the broader APS. Recruitment of new staff members over recent years has boosted the diversity of skills and experience within the Organisation. While some two thirds of ASIO's staff has currently been with the Organisation for less than five years, the injection of knowledge, skills and experience gained elsewhere in the public and private sectors has been of considerable benefit. At 30 June 2008, 88% of ASIO's total staffing of 1,492 was working on a full-time basis. This represented a full-time staff equivalent (FTE) of 1,374.

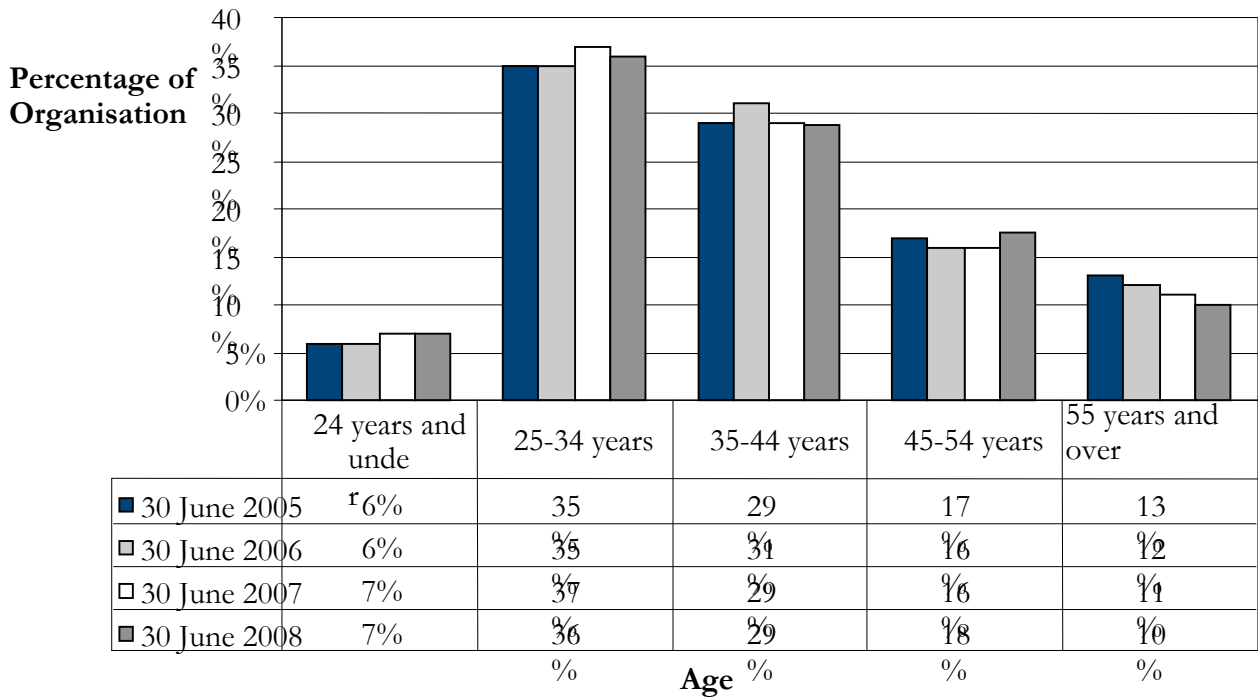
Approximately 8% (or 120) of ASIO's staff was employed on a part-time basis compared to around 12% in the broader APS in 2007–08. Most of these part-time staff members (84%, or 101) are women, with around half being in the 35–44 year age group.

The median age of ASIO's workforce has been decreasing steadily as a result of the growth of the Organisation to 37 years (compared to the APS median of 42 years in 2007–08), with the largest grouping continuing 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 42% in the APS.

While this demographic profile means that ASIO is not confronting some of the issues the APS faces in connection with a significant proportion of staff members approaching retirement age, it does present some challenges for managing the career expectations of many of its officers. In particular, expectations of promotion and advancement that may have been raised in an expanding organisation need to be managed in an organisation that is approaching, or is in, a steady state. Retaining the highest calibre staff in an environment with more limited advancement options will require innovative and attractive solutions beyond the inherent interest and challenge in the work provided by the Organisation.

The following graph compares age profiles of staff members in this reporting period with those from the last three years.

**Fig 18: Age of staff**

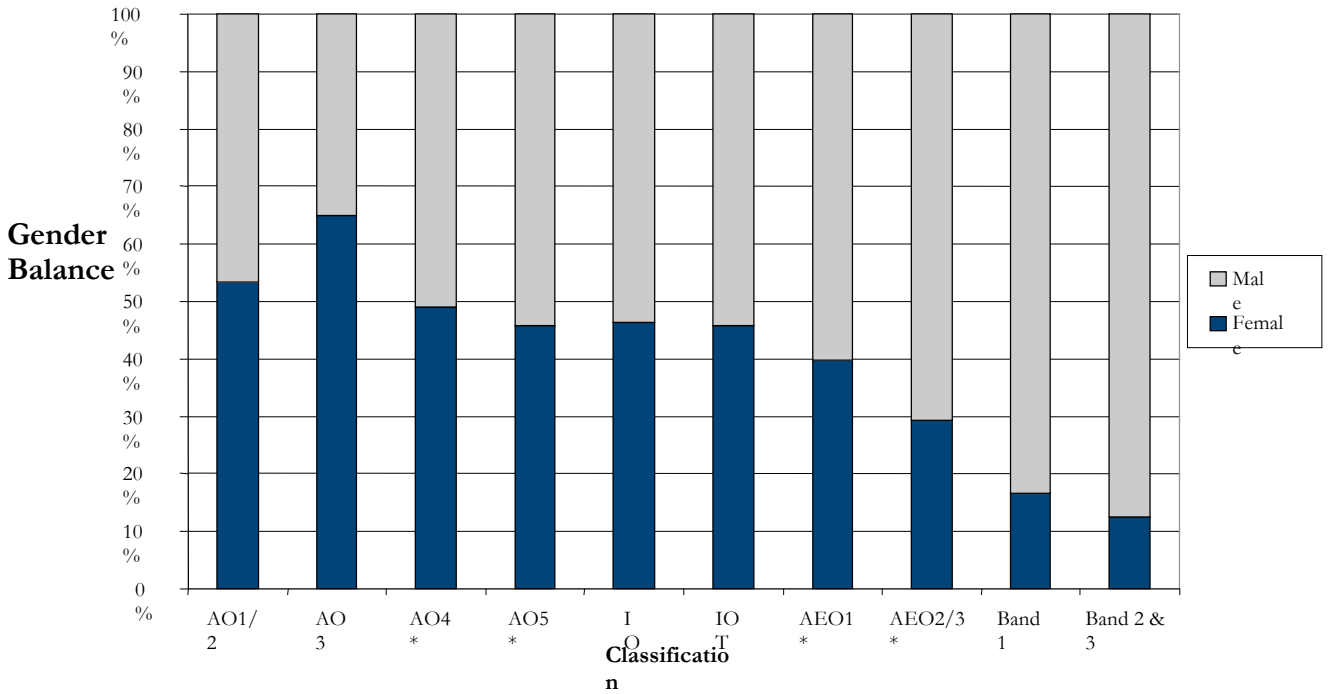


*Gender balance by classification*

While women now make up 45% of ASIO’s workforce – an improving trend – they remain under-represented in the Senior Officer (35%) and Senior Executive Service (18%) ranks compared to the APS norms of 45% and 37% respectively. This pattern is consistently lower than the APS figures of females constituting 45% of ongoing staff at the executive level and 37% at the SES level (*State of the Service Report 2007–08*).

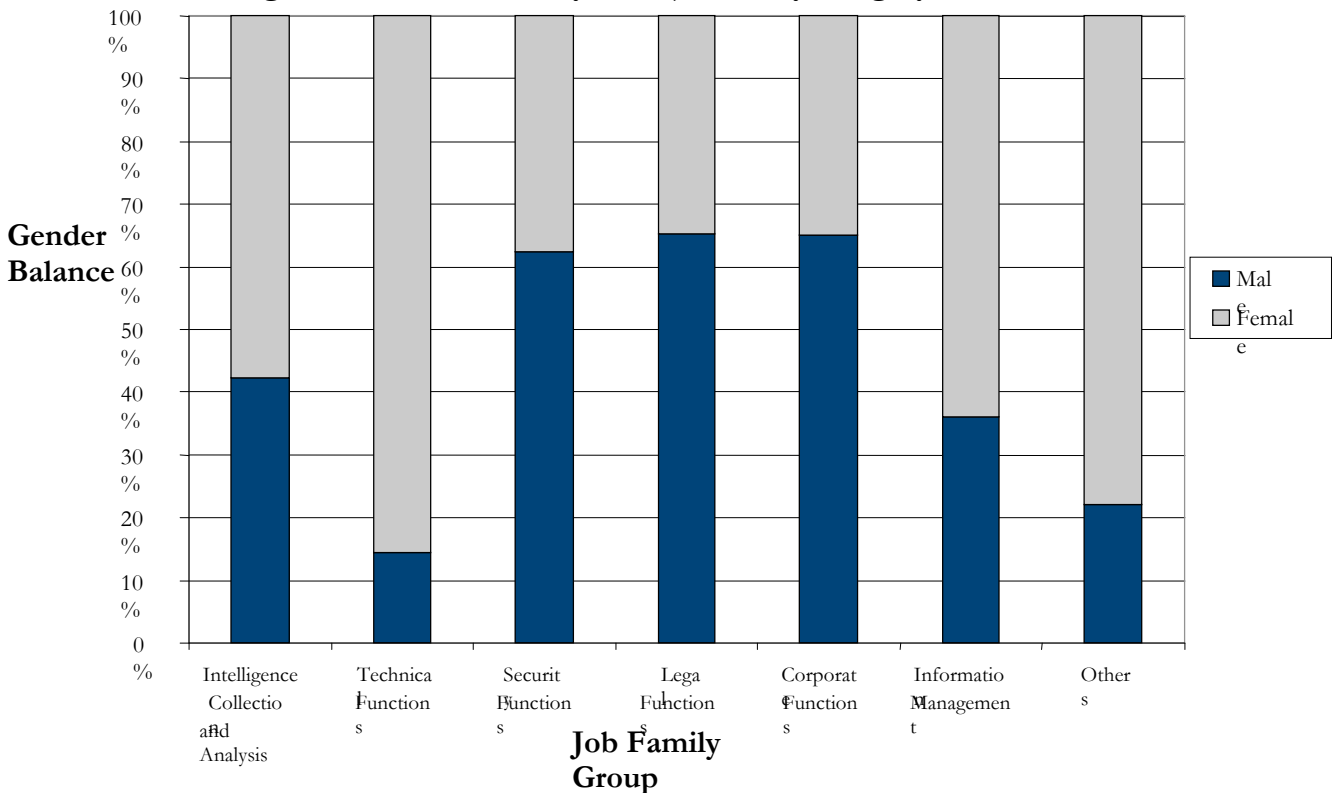
The following graph provides a breakdown of gender by classification.

**Fig 19: Gender Balance by classification**



\*Includes equivalent staff in the Engineering and Information Technology classifications.

**Fig 20: Gender balance by main job family category**



ASIO officers from non-English speaking backgrounds comprised 16.5% of ASIO staff at 30 June 2008. While ASIO has been able to attract and recruit a larger number of individuals from ethnically diverse backgrounds, and will continue to seek to attract more applicants from diverse backgrounds, a range of cultural and other factors mean that the ethnic diversity of ASIO's workforce remains below APS levels.

### *Staff complaints*

No formal grievances were lodged in 2007–08. A number of matters were raised informally with Harassment Contact Officers, Human Resource Management Section or the Organisation's Ombudsman, although all were resolved without the need for formal proceedings to be initiated.

ASIO is committed to the timely and accurate resolution of grievances within the workplace. ASIO has built and continues to support an organisational culture in which staff members are comfortable expressing concerns. ASIO recognises the right of staff members to appeal and to have certain decisions reviewed on request and that these appeals must be treated in a fair and discreet manner. In the situation where staff members wish to lodge a formal grievance ASIO has established formal committees for decisions to be reviewed and assessed, including mechanisms for timely feedback to staff member/s involved. Overall ASIO is committed to providing a work environment that allows grievances to be heard, to be reviewed and to be resolved.

ASIO has invested in its network of Harassment Contact Officers. In 2007–08, 11 Harassment Contact Officers participated in a two day training program delivered by a specialist external provider.

In addition, ASIO's human resource professionals regularly deliver presentations that address issues of inappropriate behaviour, discrimination, and workplace diversity.

# ACCOMMODATION

---

The growth in staff numbers flowing from the Government's decision in 2005 to increase ASIO capability continues to put pressure on ASIO's accommodation nationally. The construction of a new Central Office building in Canberra has been approved by the Government. ASIO's staff numbers in each State and Territory capital also will grow.

## **CENTRAL OFFICE, CANBERRA**

In the 2007–08 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 (Finance). It will be located on the site known as Section 49, Parkes, in close proximity to the Russell security 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 will 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 carefully developed to ensure the new building will take its place amongst Australia's national institutions in Canberra.

The new building will accommodate up to 1800 people and operate 24 hours a 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 place to work.

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 Finance project officers, along with the managing contractor, project architect and design consultants.

A managing contractor (Bovis Lend Lease) and project architect were appointed in September 2007 to conduct the planning phase of the project, which was completed in late 2008 with the approval of a schematic design and cost plan. Following this, the delivery phase will see the further development of the design and construction of the building to achieve an occupation date in late 2012.



## **STATE AND TERRITORY OFFICES**

The Organisation's growth continues to put pressure on accommodation in our State and Territory offices. Funding has been provided to expand these offices. Significant progress has been made in delivering new and refurbished accommodation nationally.

During 2007-2008 the Sydney relocation project commenced – staff began to occupy the new office in January 2009.

The new and refurbished offices will provide flexible, multi-functional environments that meet ASIO's operational needs and are adaptable to contingencies and emerging issues, and contemporary fit-out solutions that maintain the rigorous security standards that are a necessary requirement of the Organisation.

# PUBLIC RELATIONS AND REPORTING

---

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*;
- ASIO's submissions to, and appearance before, Parliamentary committees;
- public statements by the Director-General of Security;
- ASIO's website; and
- the Business Liaison Unit.

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 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's *Reports to Parliament* and its *Corporate Plan 2007–2011*.

## REPORT TO PARLIAMENT

The unclassified *Report to Parliament* excludes sensitive information in accordance with section 94 of the ASIO Act. The *Report to Parliament* nonetheless contains considerable detail of ASIO's activities, including information on the number of threat assessments and security assessments furnished during the year, discussion of the security environment, details of ASIO's human resource management, and ASIO's financial statements.

## PARLIAMENTARY COMMITTEES

ASIO's activities are overseen by Parliamentary committees including the:

- PJCIS;
- Senate Standing Committee on Constitutional and Legal Affairs; and
- Senate Finance and Public Administration Committee.

### *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*; and
- reviewing ASIO's questioning and detention powers.

At 30 June 2008, 19 terrorist groups were proscribed in Australia.

On 8 September 2007, the following proscribed terrorist groups were re-listed under Australian law:

- Lashkar-e-Tayyiba;
- 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 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.

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

### *Senate Standing Committee on Legal and Constitutional Affairs*

Since 1993 the Director-General of Security has appeared before the now Senate Standing Committee on Legal and Constitutional Affairs as part of the Senate Budget Estimates process. Senate Budget Estimate hearings are recorded in Hansard.

The Director-General of Security appeared before the committee on 19 February 2008 and 26 May 2008.

### *Other parliamentary oversight*

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

## **PUBLIC STATEMENTS**

Statements to Parliament about ASIO's activities are usually provided by the Attorney-General or where appropriate, the Minister representing the Attorney-General in the Senate. This includes answers during Parliamentary Question Time, and to Questions on Notice.

The Director-General of Security occasionally provides media interviews, and also makes speeches and addresses at business forums, conferences, and institutions. 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 business.

ASIO's MLO provides a first point of call for members of the media seeking comment from ASIO. ASIO maintains a publicly listed media enquiries line for this purpose.

## **WEBSITE – WWW.ASIO.GOV.AU**

ASIO's website provides the public with 24 hour access to information about ASIO, including:

- publications such as the annual *Report to Parliament and Corporate Plan 2007–11*;
- public statements by the Director-General of Security;
- historical information about ASIO;
- employment opportunities; and
- contact information.

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's *Reports to Parliament and Corporate Plan 2007–2011*.

The website also provides links to related sites including the Attorney-General, the PJCIS, the IGIS and other members of the AIC.

## **THE BUSINESS LIAISON UNIT**

ASIO's 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 distributes intelligence as unclassified Business Security Reports for specific industries (eg. 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 had 140 Business Security Reports available on its website at the end of the reporting period – compared with 55 in 2006–07. Reporting covered 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.

## **INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**

The role of the IGIS is to ensure that ASIO and the five other agencies which comprise the AIC 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 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)).