AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION

Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure No 6 (2006-07)

CONTENTS

CHARTS

TABLES

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. 6 provides a detailed account of ASIO's activities during 2006-07 covering:

- the security environment and 2006-07 overview;
- expenditure;
- the structure of the Organisation;
- direction and strategic planning;
- legislative changes;
- security of ASIO and ASIO security assessments;
- human resource management;
- staff performance management and evaluation;
- accommodation; and
- public relations and reporting.

The Security Environment and 2006-07 Overview

Countering the threat of terrorism continued to be the major focus of ASIO's effort during 2006-07, though counter-espionage and counter-proliferation were also priorities. Australia and its worldwide interests remained a target of radical Islamists, and the flow of intelligence on terrorist threats continued to increase. ASIO issued 1,994 Threat Assessments and produced a range of other intelligence reporting.

ASIO continued to enhance its capability for counter-terrorism in particular, but also for counter-espionage, counter-proliferation and border security. ASIO also invested in key technologies to enable more effective intelligence collection and analysis.

Expenditure

In 2006-07, ASIO received a significant increase in revenue from Government primarily arising from the Taylor *Review of ASIO Resourcing* (the Taylor Review). ASIO's budget increased from $66m in 2001-02 to $227m in 2006-07. This resulted in small operational surpluses for 2004-05 to 2006-07 – a contrast to operating deficits in 2001-02 to 2003-04.

Structure of the Organisation

In July 2006, ASIO moved to a nine division structure reflecting the first implementation phase of a five-year plan to grow ASIO to around 1,860 staff by 2010–11.

In March 2007, further adjustments were made to strengthen strategic management oversight of critical work areas, and as a consequence, an expanded organisational structure was created to take effect from 1 July 2007. As part of this expanded organisational structure, ASIO established several new Branches to support the growing need for specialist training; development and investigation of intelligence leads; and counter-terrorism investigations in NSW.

Direction and Strategic Planning

To support ASIO's corporate governance framework, two corporate committees were introduced in 2006-07 – the Organisational Development Committee and the Research and Development Committee. These new committees provide strategic oversight and direction to ASIO capabilities and provide strategic guidance on ASIO's growth.

In early 2007, ASIO released its *Corporate Plan 2007-11*. This five year plan identifies ASIO's business focus, provides measurements of performance and identifies how the Organisation achieves its outcomes.

ASIO's resource allocation across its four reporting outputs was consistent with allocations in 2005-06.

Legislative Changes in 2006-07

There were a number of legislative changes in 2006-07 that impacted both directly and indirectly on the administration of ASIO. In particular, the *Telecommunications (Interception) Amendment Act 2006* offered ASIO an ability to request 'B-Party' telecommunications service warrants to intercept third party communications with persons of interest, where the requisite threshold can be met.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* was the first step in the reform of Australia's anti-money laundering and counter-terrorism financing regulatory regime, and provided ASIO with ongoing access to the information held by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

Security of ASIO and ASIO Security Assessments

Prospective permanent ASIO staff are subject to stringent background checking to assess their suitability for a TOP SECRET positive vetted security clearance. ASIO staff security clearances are revalidated and re-evaluated on an ongoing basis throughout the employment of the staff member to ensure they remain suitable for access to national security classified material.

ASIO is responsible, under Part IV of the *Australian Security Intelligence Act 1979*, with furnishing security assessments to Commonwealth agencies for persons seeking access to national security classified information, visas to enter or remain in Australia, and for access to controlled areas or materials. In 2006-07 ASIO conducted 20,856 personnel security assessments, 53,387 visa security assessments and 134,981 counter-terrorism security assessments. Of these, ASIO issued one qualified personnel security assessment and seven adverse visa security assessments. ASIO devotes considerable resources to meeting its benchmarks for processing security assessments, and places priority on refugee, humanitarian and other compassionate cases. While ASIO endeavours to process these applications in a timely manner, processing times are affected by a range of factors, particularly the complexity of the case.

Human Resource Management

ASIO achieved a net growth in staff of 246 in 2006-07 and is on track to meet its target of 1860 staff by 2010-11.

During 2006-07, ASIO ran a series of recruitment advertising campaigns focusing on ASIO's ability to offer a 'career with meaning', aimed at attracting quality applicants from diverse backgrounds.

An external evaluation of ASIO's training and development strategies concluded there is a strong and genuine commitment to learning and development in ASIO. Recommendations from the evaluation align with, and enhance, existing initiatives such as the establishment of the Training Branch on 1 July 2007.

ASIO has a range of strategies and programs designed to deliver sound human resource management across the Organisation. Workplace diversity has been increasing as the Organisation grows. There were no formal complaints or grievances lodged during 2006-07.

Staff Performance Management and Evaluation

ASIO's performance management framework encourages and facilitates open, two-way communication between staff and management to evaluate staff performance and monitor individual needs to ensure that both the goals of the individual and Organisation are met.

Accommodation

The growth in staff continues to put pressure on ASIO's accommodation nationally. The Government has provided $460m additional funding for a new building housing ASIO's Central Office. ASIO's growth has also affected State and Territory offices; funding has been allocated in the 2006-07 and 2007-08 Budgets to address the accommodation needs of these offices.

Public Relations and Reporting

In addition to direct engagements with individuals, community representatives and businesses, ASIO's primary means of communicating with the public are ASIO's annual *Report to Parliament*, statements and speeches by the Director-General of Security (which are available on ASIO's website), participation in Parliamentary committee processes, and ASIO's website. ASIO seeks to provide information on the Organisation and on its activities and challenges, while at the same time balancing the need for operational and information security.

Introduction and Security Environment in 2006-07

ASIO's Role

ASIO is Australia's security service. Its roles and responsibilities are mandated by the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). The ASIO Act specifies ASIO's remit as 'security', which it defines as: the protection of Australia and Australians from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence systems, and foreign interference. The ASIO Act mandates that ASIO's responsibility for security extends geographically beyond Australia, and includes Australia's security obligations to other countries.

ASIO is also 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 Defence Signals Directorate (DSD).

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 the Attorney-General's guidelines;
- assesses intelligence and provides advice on security matters;
- investigates and responds to threats to security;
- maintains a national counter-terrorist capability;
- provides protective security advice; and
- provides security assessments, including for visa entry checks, 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 question persons in relation to terrorism matters. ASIO also has specialist capabilities that can be deployed to assist in intelligence operations and incident response.

ASIO differs from other members of the Australian Intelligence Community (AIC) in important respects:

- ASIO is the only AIC agency whose primary function is security intelligence – which is concerned with specific types of threats as defined in the ASIO Act;
- ASIO is the only AIC agency that both collects and assesses intelligence; other members of the AIC perform one, or the other, of these functions; and
- ASIO is the only AIC agency authorised in the course of its normal duties to undertake investigations into, and collect intelligence on, the activities of Australian citizens.

Particularly because Australia and Australians are central to ASIO's work, the Organisation operates under a stringent oversight and accountability framework, the centrepiece of which is the ASIO Act. ASIO's specific legislative operating parameters ensure there is an appropriate balance between individual rights and the public's collective right to security.

SECURITY ENVIRONMENT AND 2006-07 OVERVIEW

Counter-terrorism

Countering the threat of terrorism directed against Australians and Australian interests, both in Australia and abroad, continued to be the major focus for ASIO during 2006-07.

On 1 July 2006, a 17 minute audio statement attributed to Usama bin Laden was released.

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

The statement underlined the ongoing and dangerous terrorist threat to Australia and its interests worldwide.

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

The flow of threat-related intelligence to ASIO continued to increase in 2006–07 and resulted in the Organisation issuing 1,994 Threat Assessments.

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

Throughout 2006–07, ASIO contributed to preparations for the Asia-Pacific Economic Cooperation (APEC) forum aimed at delivering a safe and successful event.

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

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

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

Violent protests

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

Counter proliferation

As part of the 2005–06 Budget, ASIO received funding to boost resources devoted to countering the proliferation of weapons of mass destruction. During 2006-07, ASIO continued to work with other Australian and international agencies on this important work.

Counter-espionage and foreign interference

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

Border security

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

ASIO has been building its capability to contribute to Australia's border security effort. In late 2005, ASIO implemented a 24x7 border security unit which continued to grow in 2006-07. In addition, ASIO has worked closely with the other Australian border security agencies, particularly the Department of Immigration and Citizenship and the Australian Customs Service, to improve visa security assessment processing times and to ensure that people of security interest are not able to enter Australia. That task continues to increase in complexity as people of security interest become more adept at concealing their identities, activities or intentions.

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

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

The other side of the security equation is the denial of the opportunity for Australian citizens to travel to other countries with a view to engaging in activities that would be inimical to the security of Australia or to any other country. In 2006-07, ASIO issued a small number of security assessments that resulted in action by the Department of Foreign Affairs and Trade to cancel or deny them issue of a new or replacement Australian passport.

Capability enhancements

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

Technology and support to operations

In recognition of the important role of technology and technical capabilities, refinements to the organisational structure boosted the senior management arrangements in the Technical Capabilities Division and created a new Information Division.

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

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

The challenge ahead

ASIO's focus must remain firmly fixed on the prevention of harm to Australians and Australian interests, wherever threats emerge, while managing effectively the continued growth of the Organisation to meet current and future challenges. The security of APEC, the 2007 Federal Election, and World Youth Day and the Beijing Olympics in 2008, will require ASIO's close attention in the 2007-08 reporting period.

EXPENDITURE

OVERVIEW

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

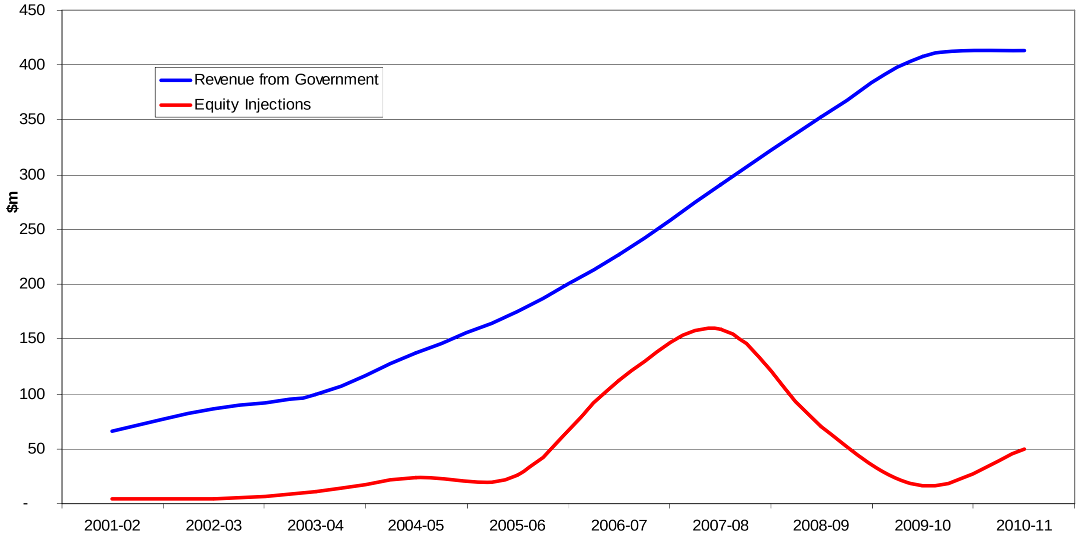
ASIO's outcome, which supports the Government's policy aim of 'A secure Australia in a secure region' is: 'A secure Australia for people and property, for government business and national infrastructure, and for special events of national and international significance.'

RECENT DEVELOPMENTS/TRENDS

ASIO's revenue from Government has increased from $66m in 2001-02 to $227m in 2006-07. Forward estimates for 2007-08, 2008-09, 2009-10 and 2010-11 are $291m, $353m, $407m and $413m respectively.

ASIO's equity injections have increased over the same time period, from $4m in 2001-02 to $113m in 2006-07. Forward estimates for 2007-08, 2008-09, 2009-10 and 2010-11 are $159m, $71m, $16m and $50m respectively.

Chart 3.1: ASIO revenue from Government, 2001-02 to 2010-11



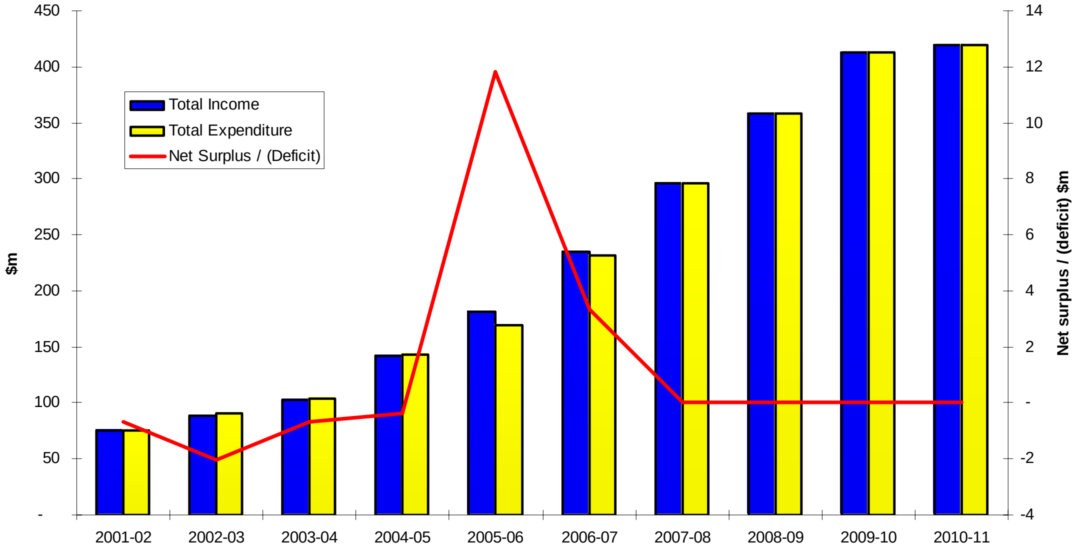
The significant increase in ASIO's budget from 2006-07 predominantly arises from the *Review of ASIO Resourcing* (the Taylor Review). The Taylor Review, endorsed by Government on 16 October 2005, made recommendations for the further growth of ASIO to cope with existing operational demands and to enhance 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 information technology infrastructure and for expansion of the 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.

ASIO'S FINANCIAL PERFORMANCE

ASIO recorded operating deficits in 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 with the deficits, ASIO has recorded operating surpluses for 2004-05 to 2006-07, with breakeven results budgeted for 2007-08 through to 2010-11. The improved financial performance reflects the easing of budgetary pressures on the Organisation through additional funding by Government in 2004-05.

As shown in the following chart, the 2006-07 financial year saw a small operating surplus of $3.4m. The variance from the $7.0m surplus estimated in the 2006-07 PBS is within 2%, and occurred due to slight under-expenditure against employees.

Chart 3.2: ASIO's financial performance, 2001-02 to 2010-11



FINANCIAL MANAGEMENT AND INTERNAL CONTROLS

ASIO prepares annual financial statements in accordance with section 49 of the *Financial Management and Accountability Act 1997* (the 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.

On a monthly basis the Chief Finance Officer reports to the ASIO Corporate Executive (the main ASIO forum for managing strategic corporate priorities resource issues) on the financial performance of the Organisation.

ASIO has a robust and reliable Financial Management Information System (FMIS) and a comprehensive suite of monthly and ad-hoc management reports which Senior Management utilise in ensuring appropriate financial management and accountability across the organisation.

The rise in ASIO's budget has positioned the Organisation well to deliver the significant growth identified 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.

CHALLENGES

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.

One of the major challenges in the short term is the growth in employee numbers. This has a twofold impact:

- expenses flowing from workplace agreements increase faster than the appropriation indexation provided by Government; and
- in order to allow employees the best possible tools to do their job, the investment needed in information technology infrastructure increases exponentially.

Both recruitment planning and information technology investment are regularly reviewed to ensure expenditure continues to support ASIO's direction and priorities.

STRUCTURE OF THE ORGANISATION

In July 2006, ASIO moved to a nine division structure reflecting the first implementation phase of a five-year plan to grow ASIO to around 1,860 staff by 2010–11.

In March 2007, further adjustments were made to strengthen strategic management oversight of critical work areas, and as a consequence, an expanded organisational structure was created to take effect from 1 July 2007. The expanded organisational structure consists of 12 ongoing divisions and one non-ongoing Senior Executive Service (SES) Band 2 position, supported by 36 Managers (SES Band 1), up from 28.

Features of the new divisional structure include:

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

Changes within the existing divisions include:

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

Chart 4.1: ASIO's organisational structure at 1 July 2006

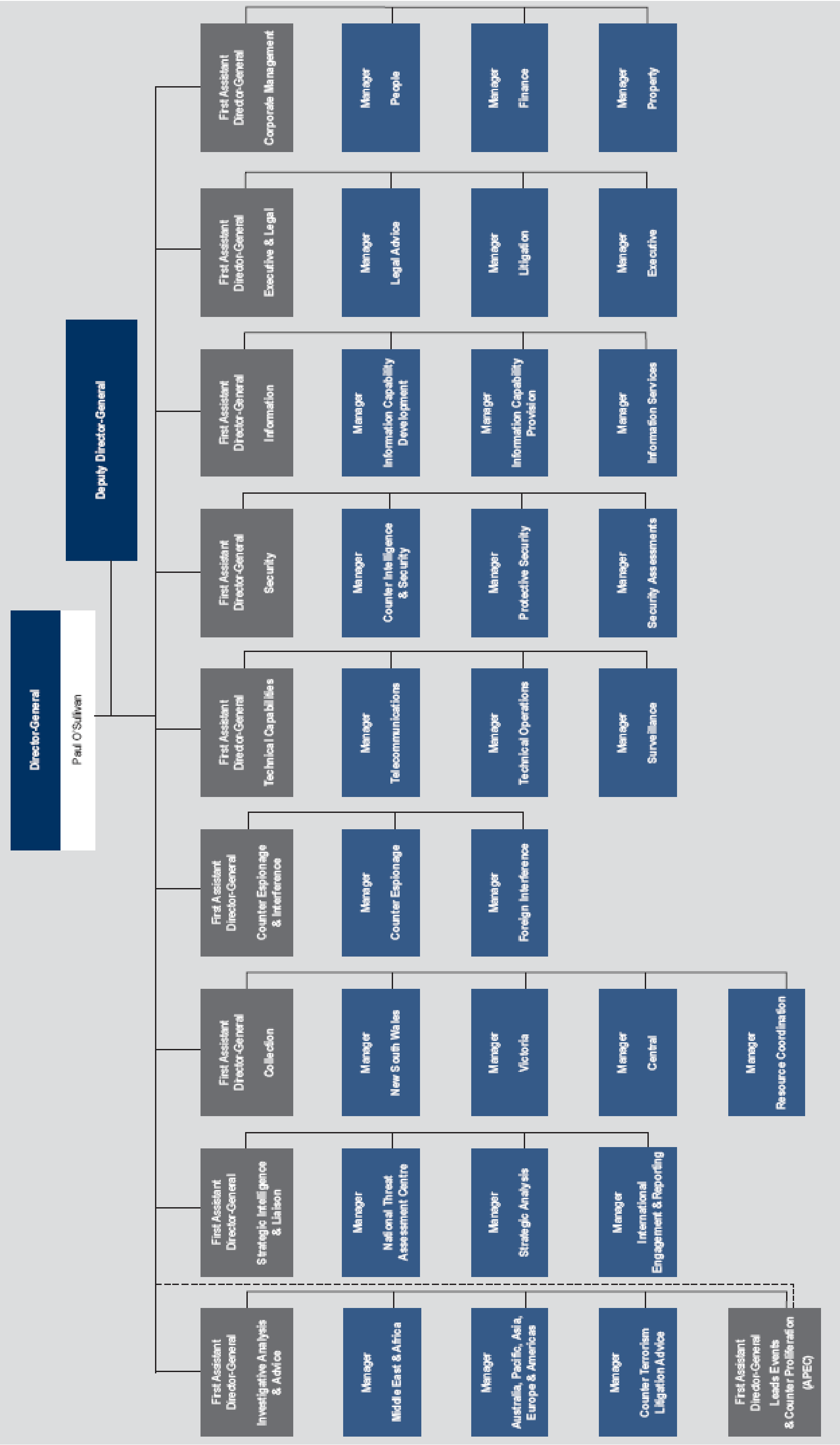
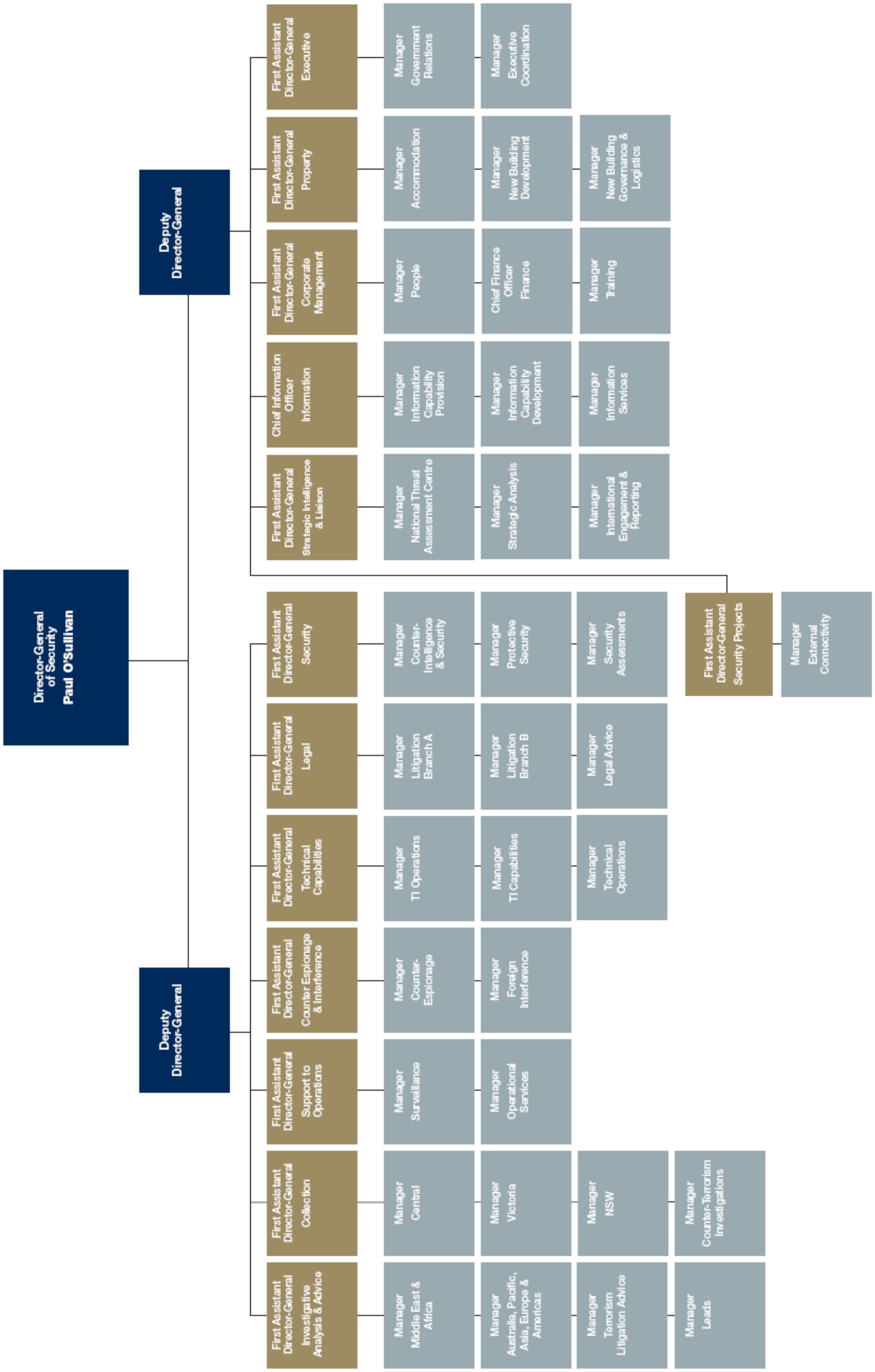

Director-General
Paul O'Sullivan
Deputy Director-General
First Assistant Director-General Corporate Management
Manager People
Manager Finance
Manager Property
First Assistant Director-General Executive & Legal
Manager Legal Advice
Manager Litigation
Manager Executive
First Assistant Director-General Information
Manager Information Capability Development
Manager Information Capability Provision
Manager Information Services
First Assistant Director-General Security
Manager Counter Intelligence & Security
Manager Protective Security
Manager Security Assessments
First Assistant Director-General Technical Capabilities
Manager Telecommunications
Manager Technical Operations
Manager Surveillance
First Assistant Director-General Counter Espionage & Interference
Manager Counter Espionage
Manager Foreign Interference
First Assistant Director-General Collection
Manager New South Wales
Manager Victoria
Manager Central
Manager Resource Coordination
First Assistant Director-General Strategic Intelligence & Liaison
Manager National Threat Assessment Centre
Manager Strategic Analysis
Manager International Engagement & Reporting
First Assistant Director-General Investigative Analysis & Advice
Manager Middle East & Africa
Manager Australia, Pacific, Asia, Europe & Americas
Manager Counter Terrorism Litigation Advice
First Assistant Director-General Leads Events & Counter Proliferation (APEC)

Chart 4.2: ASIO's organisational structure at 1 July 2007


Director-General of Security Paul O'Sullivan
Deputy Director-General
First Assistant Director-General Executive
Manager Government Relations
Manager Executive Coordination
First Assistant Director-General Property
Manager Accommodation
Manager New Building Development
Manager New Building Governance & Logistics
First Assistant Director-General Corporate Management
Manager People
Chief Finance Officer Finance
Manager Training
Chief Information Officer Information
Manager Information Capability Provision
Manager Information Capability Development
Manager Information Services
First Assistant Director-General Strategic Intelligence & Liaison
Manager National Threat Assessment Centre
Manager Strategic Analysis
Manager International Engagement & Reporting
First Assistant Director-General Security Projects
Manager External Connectivity
Deputy Director-General
First Assistant Director-General Security
Manager Counter-Intelligence & Security
Manager Protective Security
Manager Security Assessments
First Assistant Director-General Legal
Manager Litigation Branch A
Manager Litigation Branch B
Manager Legal Advice
First Assistant Director-General Technical Capabilities
Manager TI Operations
Manager TI Capabilities
Manager Technical Operations
First Assistant Director-General Counter Espionage & Interference
Manager Counter-Espionage
Manager Foreign Interference
First Assistant Director-General Support to Operations
Manager Surveillance
Manager Operational Services
First Assistant Director-General Collection
Manager Central
Manager Victoria
Manager NSW
Manager Counter-Terrorism Investigations
First Assistant Director-General Investigative Analysis & Advice
Manager Middle East & Africa
Manager Australia, Pacific, Asia, Europe & Americas
Manager Terrorism Litigation Advice
Manager Leads

DIRECTION AND STRATEGIC PLANNING

CORPORATE GOVERNANCE

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

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

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

- The DGM is held twice weekly and comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. It manages the day-to-day business of ASIO, including areas of ongoing corporate priority and urgent or emerging issues requiring consideration by the Executive.
- The CE meets twice monthly and comprises the Director-General, Deputy Directors-General, First Assistant Directors-General and two managers on rotation, with the Staff Association President attending as an observer. It sets ASIO's strategic direction and oversees resource management, providing the main forum for managing strategic corporate priorities and resource issues. It also conducts detailed quarterly reviews of the performance of the Organisation. The results of these reviews feed into ASIO's *Annual Report*.

The DGM and CE manage a number of corporate committees that formally report to them. With the addition of the Organisational Development Committee and the Research and Development Committee, in 2006–07, the number of committees grew from six to eight, reflecting the Organisation's focus on effectively managing growth and capability enhancement.

- The Intelligence Coordination Committee, chaired by a Deputy Director-General, includes senior managers involved in the intelligence process. The committee sets security intelligence investigative priorities and allocates broad resources to these on a risk management basis. It also performs quarterly reviews against strategic objectives and approves arrangements for ensuring the legality and propriety of ASIO's intelligence collection, analysis and advice.
- The Audit and Evaluation Committee, chaired by a Deputy Director-General, includes a senior executive from the Australian National Audit Office. The committee facilitates the internal audit of ASIO in accordance with the Internal Audit Charter, by setting priorities for audit, fraud control and evaluation planning. It also considers the findings of the internal audits and evaluations and ensures management-endorsed recommendations are implemented.

- The Organisational Development Committee, chaired by the head of Corporate Management Division, includes the Staff Association President. This new committee provides strategic guidance on ASIO's growth with particular regard to growing the capabilities of ASIO's staff, shaping an appropriate culture and managing change.
- The Staff Placements Committee is comprised of the two Deputy Directors-General, who make strategic decisions on staff commencements and placements. (In 2005-06 this committee was chaired by the head of the Corporate Management Division).
- The Security Committee, chaired by the head of Security Division, includes the Staff Association President. It reviews and addresses key issues relevant to the security of ASIO people, property and performance. The committee also provides a consultative forum to develop security policies and practices.
- The Research and Development Committee, chaired by the head of Technical Capabilities Division, includes a representative from the Defence Science and Technology Organisation. This new committee provides strategic oversight and direction to technical collection and analysis capability.
- The Information Management Committee, chaired by the head of Information Division, provides strategic oversight and direction to ASIO's information and communication technology work program.
- The ASIO Consultative Council, co-chaired by the head of the Corporate Management Division and the Staff Association President, comprises representatives from management and the Staff Association. The committee makes recommendations to the Director-General on personnel policies and practices. It is an advisory and deliberative body, enabling management and staff discussion and resolution of issues of mutual interest and concern.

CORPORATE PLANNING

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

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

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

The new plan was released in early 2007 and is available on ASIO's website.

ORGANISATIONAL PERFORMANCE MANAGEMENT

ASIO's organisational performance management framework is comprehensive and multi-faceted:

- a process of regular performance reviews informs senior management of trends and pressure points and provides an objective basis for managing risk;
- ASIO conducts an annual survey of key clients from Commonwealth departments and agencies and from State and Territory police services and the private sector. The results are reported in general terms in the annual *Report to Parliament*;
- the CE reviews the performance of key areas of activity through regular reporting on budget and finance, growth, information technology, security, property management and accommodation, and the general 'health' of ASIO; and
- the twice-weekly DGM oversees performance of a range of critical issues including**:**
  - staff recruitment;
  - critical business areas including security assessments, and border security; and
  - some litigation/legal matters.

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, technical and human, to support complex investigations in both its collection and analysis capacity. The priority attached to, and expense involved in, maintaining and applying capability is reflected in resource allocation against Output 3, as shown in Table 5.1. Resource allocation across the Outputs was consistent with previous years.

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 the Department of Immigration and Citizenship 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 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's *Fraud Control Plan 2006–08* sets out ASIO's responsibilities for the conduct of audit and evaluation to prevent and defeat fraudulent activity.

- ASIO's program of internal reviews, audits and evaluations are overseen by the Audit and Evaluation Committee.
- During 2006–07, 11 internal audits and one evaluation were completed.
- ASIO's fraud prevention strategies include a program on ethics and accountability which all staff are required to attend at least once every three years. The program includes a substantial component covering ASIO's approach to fraud control and its expectations of staff.

LEGISLATIVE CHANGES IN 2006-07

Legislative changes introduced during the Review period impacting on ASIO's administration included:

- the *Telecommunications (Interception) Amendment Act 2006*; and
- the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT ACT 2006

The *Telecommunications (Interception) Amendment Act 2006* (the TI Amendment Act) received Royal Assent on 3 May 2006 and amended the then *Telecommunications (Interception) Act 1979*. The Amendment Act clarified and enhanced ASIO's telecommunications interception capability by implementing certain recommendations of the *Blunn Report on the review of the regulation of access to communications under the Telecommunications (Interception) Act 1979*.

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

- an ability to request a 'B-Party' telecommunications service warrant which authorises interception of the communications of a person known to communicate with a person of interest. A 'B-Party' warrant may only be employed where ASIO has exhausted all other practicable means of identifying the service being used by the person of interest or it would not otherwise be possible to intercept the service being used by the person of interest;
- an authority to access stored communications such as SMS messages, email or other communications that have been previously sent over a telecommunications service; and
- an ability to request an equipment-based telecommunications service warrant that intercepts the telecommunications service or the telecommunications device used by a person of interest. For example, an equipment-based warrant might authorise communications to, or from a specified mobile telephone handset, while a service-based warrant might authorise communications to, or from a SIM card within a handset.

The role of Legal Division

Legal Division plays a central role in the use of ASIO's special powers. The Division is responsible for the management of the warrants process, and a senior lawyer reviews every warrant request prior to its consideration by the Director-General and Attorney-General.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING ACT 2006

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML CTF Act) received Royal Assent on 12 December 2006 and formed part of a legislative package that implemented the first tranche of reforms to Australia's anti-money laundering and counter-terrorism financing regulatory regime.

In particular, the AML CTF Act enables ASIO to access information held by the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australia's anti-money laundering regulator and specialist financial intelligence unit. The AML CTF Act limits ASIO officers' ability to disclose AUSTRAC information to the following circumstances:

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

ASIO, in concert with AUSTRAC, provides training to its officers in the appropriate handling of AUSTRAC information.

ASIO limits its officers' access to AUSTRAC information to those officers who have received training. All ASIO access to, and use of, AUSTRAC information must be approved in writing and must comply with ASIO's Memorandum of Understanding with AUSTRAC. The IGIS audits ASIO access to AUSTRAC records, and in 2006-07 found no breaches of acceptable practice.

SECURITY OF ASIO AND ASIO SECURITY ASSESSMENTS

SECURITY OF ASIO

ASIO staff must be cleared to a TOP SECRET positive vetted (TSPV) level if they are to have access to our information technology systems. Suitability to hold a TSPV clearance is determined through rigorous background checks, security checks and psychological assessments both prior to, and in the course of employment at ASIO.

While employed at ASIO, staff members are provided with security education, including:

- at induction;
- formal training programs;
- security workshops;
- (classified) *ASIO Security Instructions*;
- published policies;
- security awareness briefings;
- articles published in ASIO's in-house magazine; and
- information contained on the ASIO Intranet.

Revalidation and Re-evaluation program

ASIO staff members are also required under the *Protective Security Manual* (PSM) to undergo a revalidation program to ensure that they remain suitable to access national security classified material.

In 2006-07 ASIO completed 1,865 revalidations of security clearances, and 118 re-evaluations of security clearances.

SECURITY ASSESSMENTS

ASIO is responsible under Part IV of the ASIO Act for furnishing security assessments to Commonwealth agencies relevant to their roles and functions. ASIO can issue security assessments for:

- access to security classified material (*personnel security assessments*);
- access to places or activities controlled on security grounds (e.g. maritime and aviation security identity cards, Australian Nuclear Science and Technology Organisation (ANSTO) and ammonium nitrate programs, counter-proliferation programs) (often referred to as *counter-terrorism security assessments*);
- entry into Australia or to remain in Australia *(visa security assessments)*;
- citizenship of Australia; and

- the cancellation of Australian passports or the seizure of foreign passports held by persons of security concern (often called *passport cancellations*).

In making a security assessment ASIO draws on classified and unclassified information 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 its security assessment to grounds related to 'security' as it is defined in the ASIO Act. Other factors where there is no security nexus (such as health or criminal history) 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 that 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 or access.

Requesting agencies then make a determination on whether the applicant should be granted the proposed access. The agency's determination is based on ASIO's security assessment as well as the agency's own assessment of the individual's general suitability. 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, etc. In some circumstances (such as personnel security assessments) the requesting agency has some discretion in determining the nature of administrative action arising from an adverse or qualified security assessment. However, in other cases, (such as 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 where 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 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 poses to security.

The complexity of investigation undertaken by ASIO into any application varies depending upon the information available to DIAC and ASIO, the visa type, and the background of the applicant. Some assessments are relatively straightforward and can be completed quickly; others require additional investigative resources, checking of information with external agencies, or interviews of the applicants or their associates. Other factors that can influence the timeframe for an assessment include the total caseload of referrals to ASIO at any given time, the availability of resources to undertake checks or investigation, and the complexity of or rapid changes in the security environment.

Visa security checking processes are generally managed in order of referral from DIAC, taking into account any agreed priority caseloads. ASIO actively responds to security risks and DIAC priorities (with particular emphasis on the refugee, humanitarian and protection caseloads and genuine compassionate or compelling cases)

The majority of visa security assessments were completed within accepted timeframes, although processing times for permanent resident applications fell short of expectations.

Chart 7.1: Visa security assessment process

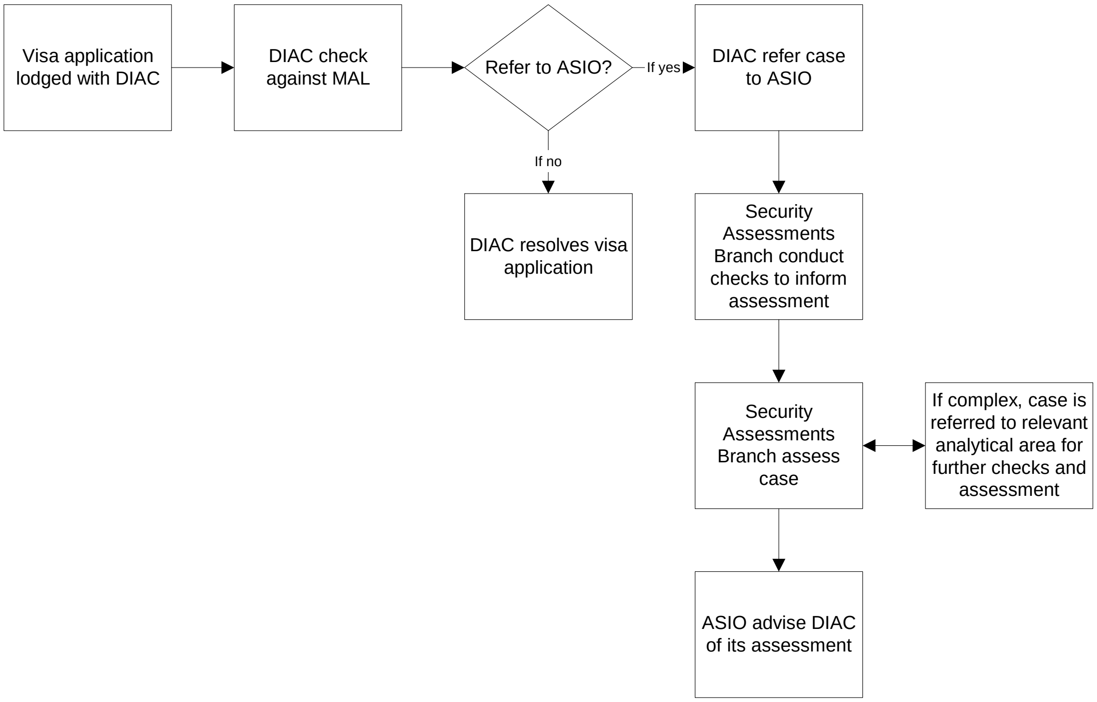

Visa application lodged with DIAC
DIAC check against MAL
Refer to ASIO?
If yes
DIAC refer case to ASIO
If no
DIAC resolves visa application
Security Assessments Branch conduct checks to inform assessment
Security Assessments Branch assess case
If complex, case is referred to relevant analytical area for further checks and assessment
ASIO advise DIAC of its assessment

Chart 7.2: Visa security assessments, 2000-01 to 2006-07

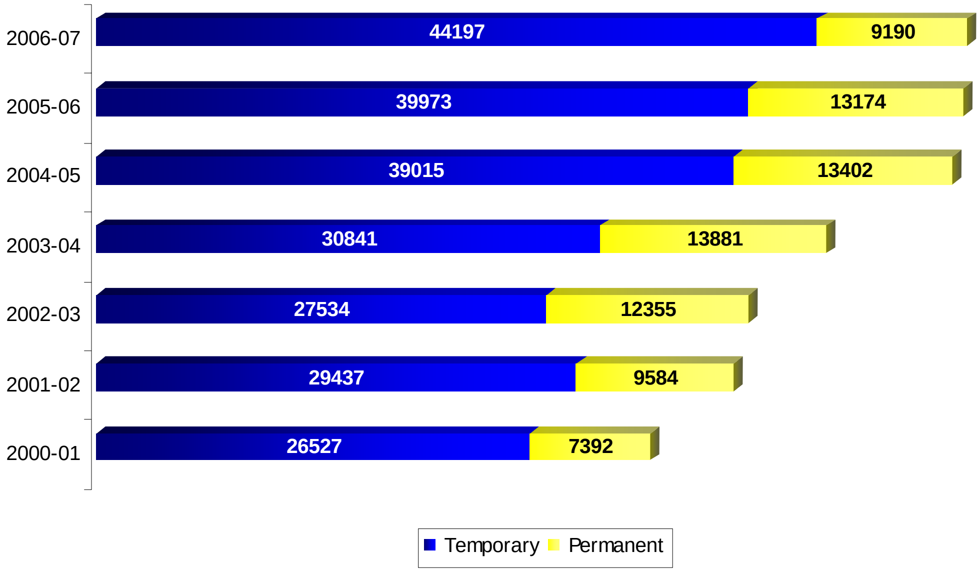
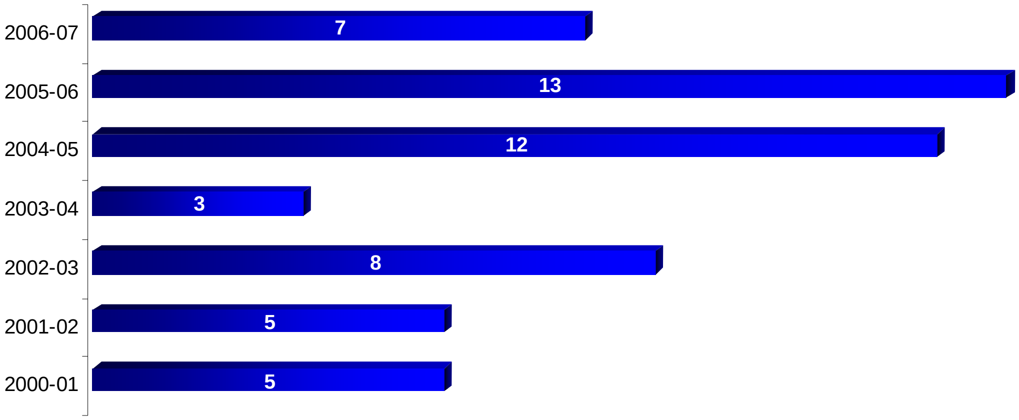


Chart 7.3: Adverse visa security assessments, 2000-01 to 2006-07



Personnel security assessments

ASIO's personnel security assessments are undertaken at the request of other agencies as part of their own 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 gives cause for security concern. ASIO does not assess general suitability for the access proposed, nor 'issue' security clearances; these remain the responsibility of the requesting agency which will conduct interviews and referee checks to satisfy itself of the applicant's suitability.

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

The length of time taken to complete a security assessment will be dependent upon the complexity of the case. Average turn-around times will, however, be dependent upon numbers of client requests, complexity of case load, staffing and competing priority special events.

On completion of an assessment, ASIO provides advice that it does not recommend against a security clearance or otherwise issues an adverse or qualified assessment. In instances where ASIO has issued a qualified or adverse assessment, candidates are notified and have a right of appeal to the Administrative Appeals Tribunal.

Chart 7.4: Personnel security assessment process

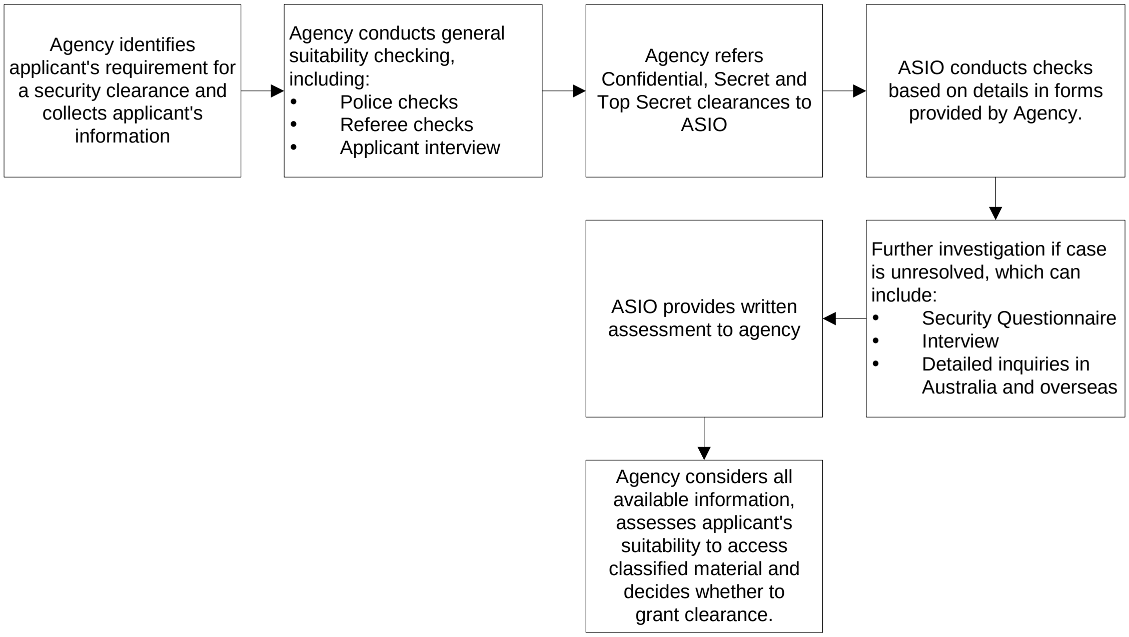

Agency identifies applicant's requirement for a security clearance and collects applicant's information
Agency conducts general suitability checking, including:
• Police checks
• Referee checks
• Applicant interview
Agency refers Confidential, Secret and Top Secret clearances to ASIO
ASIO conducts checks based on details in forms provided by Agency.
Further investigation if case is unresolved, which can include:
• Security Questionnaire
• Interview
• Detailed inquiries in Australia and overseas
ASIO provides written assessment to agency
Agency considers all available information, assesses applicant's suitability to access classified material and decides whether to grant clearance.

Chart 7.5: Personnel security assessments, 2000-01 to 2006-07

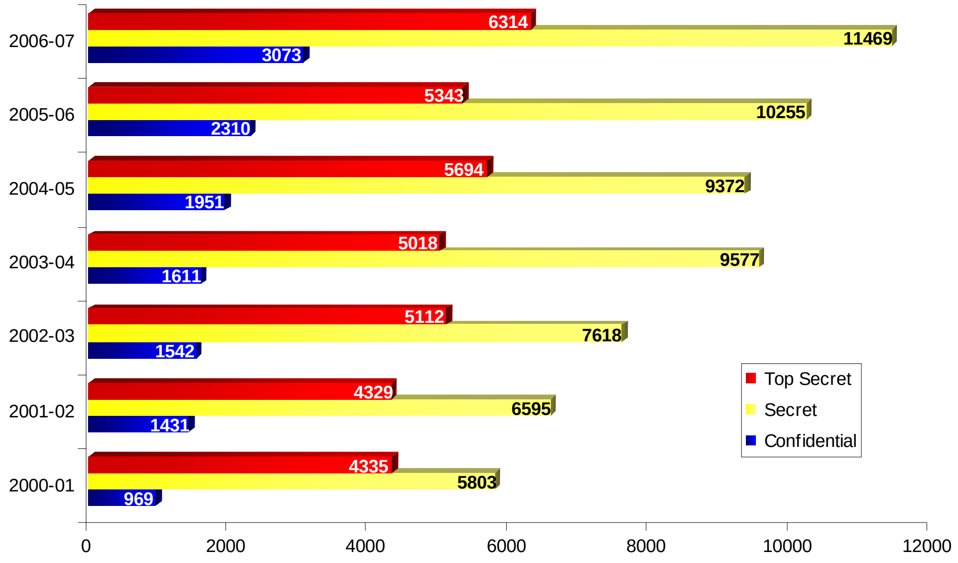
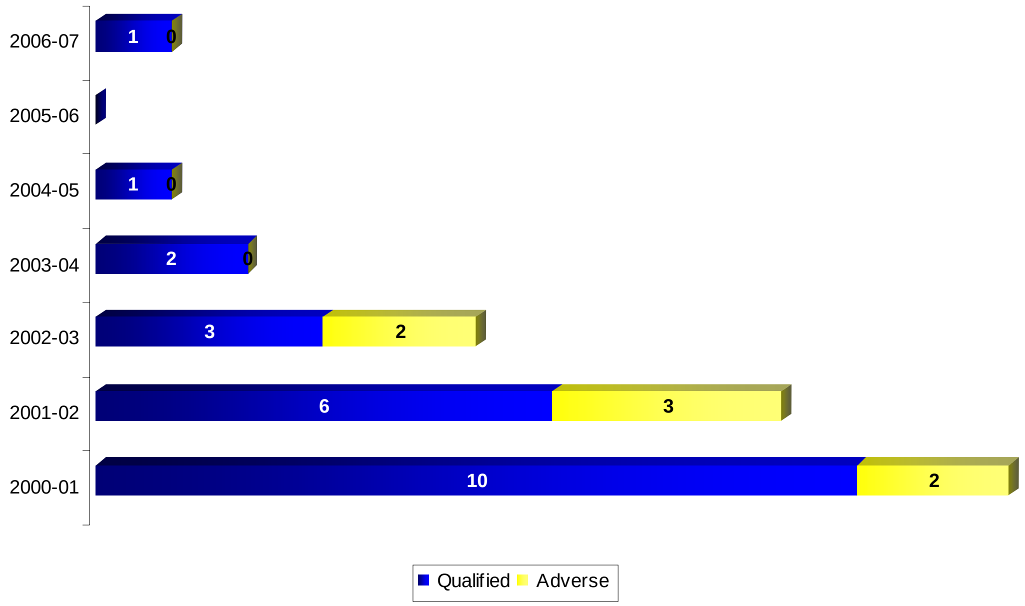


Chart 7.6: Qualified or adverse personnel security assessments, 2000-01 to 2006-07



Counter-Terrorism Security Assessments

Counter-terrorism security checking comprises checks in relation to:

- Aviation Security Identity Cards;
- Maritime Security Identity Cards;
- ammonium nitrate licensing;
- ANSTO staff;
- flight crew; and
- special events such as the Asia-Pacific Economic Cooperation (APEC).

Counter-terrorism security checks are limited to inquiring whether an individual has any known links to terrorism. They are completed more quickly than access assessments; ASIO endeavours to complete 99% within 10 days, and met this benchmark in 2006-07.

Chart 7.7: Counter-terrorism security assessment process

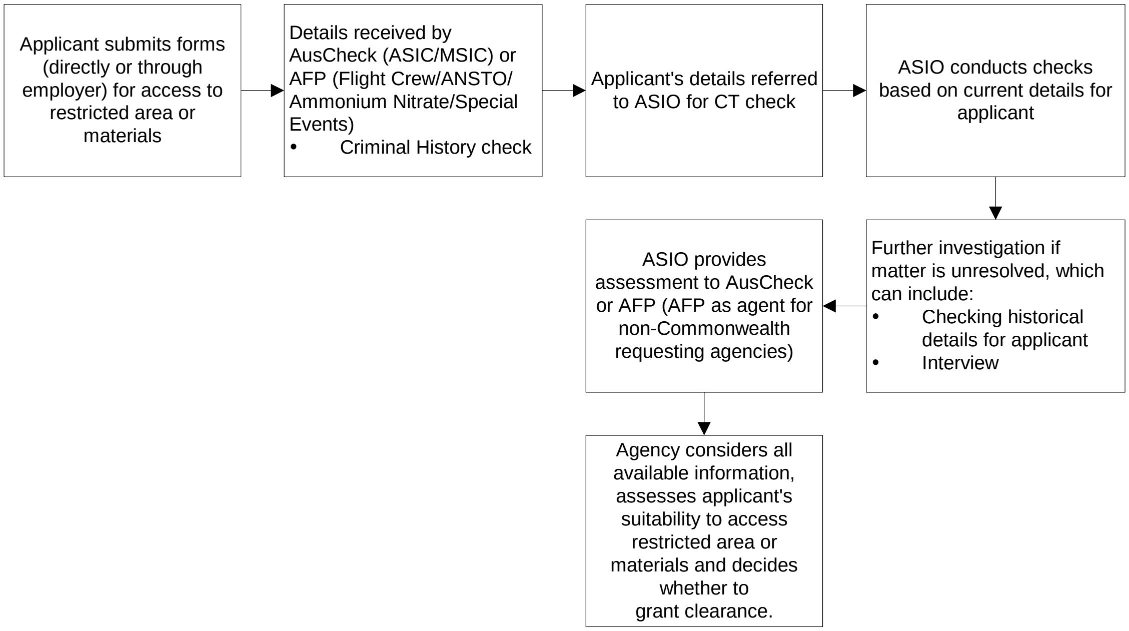

Applicant submits forms (directly or through employer) for access to restricted area or materials
Details received by AusCheck (ASIC/MSIC) or AFP (Flight Crew/ANSTO/ Ammonium Nitrate/Special Events)
• Criminal History check
Applicant's details referred to ASIO for CT check
ASIO conducts checks based on current details for applicant
Further investigation if matter is unresolved, which can include:
• Checking historical details for applicant
• Interview
ASIO provides assessment to AusCheck or AFP (AFP as agent for non-Commonwealth requesting agencies)
Agency considers all available information, assesses applicant's suitability to access restricted area or materials and decides whether to grant clearance.

Table 7.1: Counter-terrorism security assessments, 2003-04 to 2006-07

Type of check	2003-04	2004-05	2005-06	2006-07
Aviation	58147	38466	62285	36338
Maritime Security Identity Cards	-	-	9448	81780
Ammonium Nitrate	-	1634	7428	6419
ANSTO	-	-	-	1027
Commonwealth Games	-	-	56149	-
G20 Finance Ministers' Meeting	-	-	-	1580
APEC	-	-	-	7837
Total	58147	40100	135310	134981

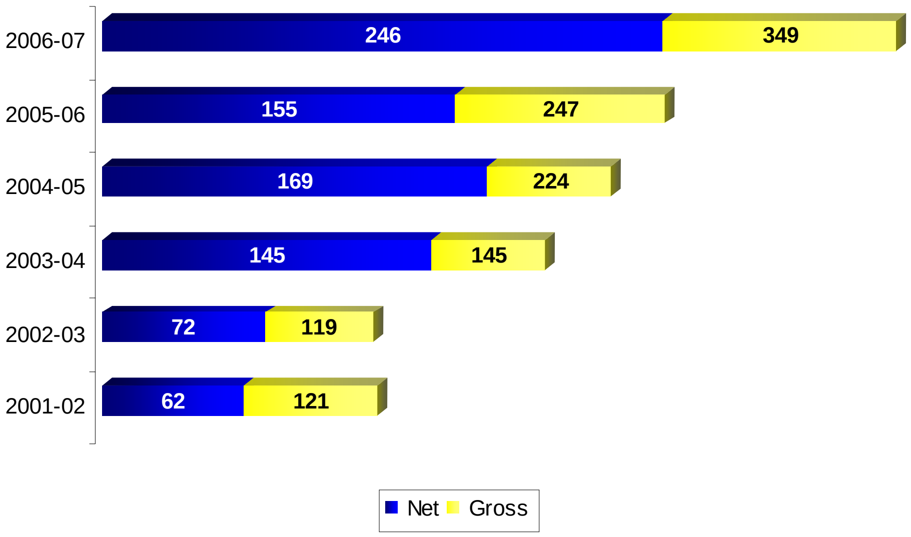
HUMAN RESOURCE MANAGEMENT

RECRUITMENT

The year saw the continuation of ASIO's high level of recruitment activity to meet its growth targets. A total of 349 new staff joined ASIO in 2006-07 compared to 247 in 2005–06. This was the most staff ever recruited into the Organisation during a financial year, and allowed a net growth of 246, 76 over the net growth target of 170. The majority of these additional staff were absorbed into developing ASIO's enabling functions. For example, ASIO bolstered its recruitment area further and have continued to enhance and streamline its processes and recruitment systems to allow it to continue to meet its recruitment targets. This places ASIO in a strong position to increase recruitment of operational staff from 2007-08.

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

Chart 8.1: Recruitment figures, 2001-02 to 2006-07



Recruitment strategies

The tight labour market and the requirement for ASIO to attract and retain high-calibre staff requires frequent reconsideration of its recruitment strategies. In 2006-07 ASIO further developed recruitment strategies to meet its recruitment targets without compromising standards. These included:

- the extension of prioritised 'job family' campaigns to most ASIO vacancies in 2006–07. This approach minimised the number of separate recruitment processes and facilitated coordinated selection processes. It also enabled better forward planning to ensure effective deployment of recruitment resources;
- the use of recruitment agencies to assist in sourcing applicants for some roles, coordinate assessment centres, and conduct on-line testing;
- the employment of vetting agencies to support some stages of the vetting processes;
- the development of an ASIO recruitment Internet tool progressed in 2006–07, with a view to implementation in late 2007, to improve efficiency in receiving and processing applications, and allowing applicants to receive timely and regular updates on the progress of their applications;
- ASIO's enhanced presence on the Internet, and increased participation at Australian Intelligence Community (AIC) Roadshows, University Careers Fairs and Defence Resettlement seminars; and
- further research and development of an organisational 'brand' to position ASIO as a unique and dynamic organisation offering 'careers with meaning' in a wide range of disciplines.

Recruitment advertising

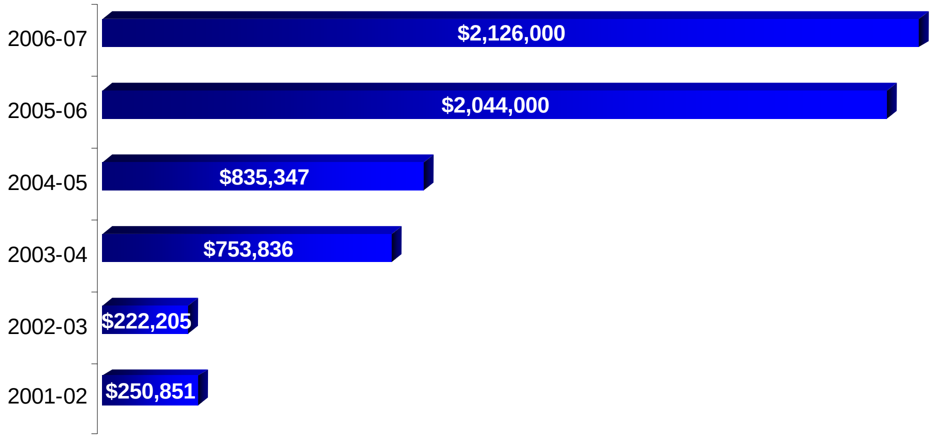
ASIO continued to engage recruitment and advertising agencies to enhance its attraction strategies and ensure it remains a competitive employer. ASIO ran a series of innovative recruitment advertising campaigns in 2006–07 aimed at attracting quality applicants from diverse backgrounds to fill a range of vacancies.

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

Other advertising initiatives included targeted campaigns in relevant industry publications (e.g. legal and engineering magazines) and Internet advertising (e.g. career websites and Google).

ASIO's overall recruitment advertising costs for 2006–07 were $2.126m compared to $2.044m in 2005–06 in line with the increase in staff recruitment and the need for innovative strategies to attract high quality recruits.

Chart 8.2: Advertising costs for recruitment, 2001-02 to 2006-07

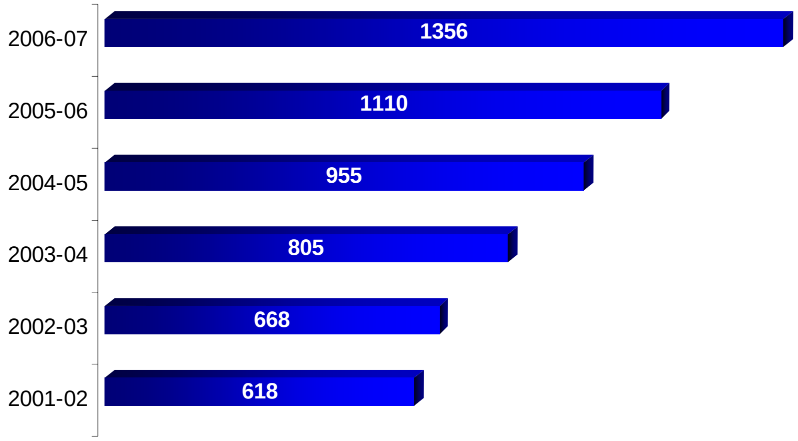


Staffing levels

ASIO has been increasing its staffing levels since 2002. The implementation of the recommendations from the Taylor *Review of ASIO Resourcing* saw the development of a structured program to manage this growth through to 2010-11.

As at 30 June 2007 ASIO had 1,356 staff, an increase of 22% from the previous year.

Chart 8.3: ASIO staffing levels, 2001-02 to 2006-07



Training and Staff Development

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

In 2006–07, ASIO invested $4.9m (about 2% of its budget) in training and development, an increase of $1.3m from the previous year. This reflects the additional resources required for the training and development of a growing workforce, and ASIO's commitment to ensuring staff are adequately trained to meet the challenges faced by the Organisation.

Evaluation of training and development strategies

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

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

The evaluation concluded that there is a strong and genuine commitment to learning and development in ASIO, and our learning and development strategies could be enhanced through:

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

A number of these recommendations align with, and enhance existing initiatives, and the implementation of recommendations had commenced by the end of the period – Training Branch was established on 1 July 2007.

Leadership and management skills

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

The *Learning and Development Strategy for Leadership* includes the delivery of structured coursework that addresses a variety of leadership and management competencies. (see Table 8.1)

Table 8.1: Leadership and management learning activities, 2006-07

Activity	Description	Number of attendees
Management to Leadership	A five day course designed to help managers achieve high quality outcomes through effective leadership of their teams.	49
Diploma of Business (Frontline Management)	Provides essential skills and knowledge to effectively manage staff, resources and projects.	34
Career Development Assessments Centres	Designed to assess a Senior Officer's skills and capabilities against the SES capabilities.	5
Senior Officer Orientation Workshop	Provides insight into the accountability and responsibility expectations placed on Senior Officers within ASIO.	69

In 2006-07, leadership and management learning and development also involved:

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

Corporate training

All officers below the SES level are provided learning opportunities under the (classified) *ASIO Officer Capability Strategy*. This strategy ensures that appropriate training and career development occurs across the Organisation, and throughout the various stages of an ASIO officer's career.

Corporate training activities include:

- administrative training – contract management, project management, staff selection skills, presentation skills, trainer training, interviewing, effective reading and writing, finance and budgeting;
- IT training – basic and advanced training in the use of ASIO's computer systems;
- ethics and accountability – all members of staff are required to attend at least once every three years;
- the Studies Assistance Program – supporting tertiary study, including language study, by members of staff; and
- the Director-General's Study Bursaries – supporting members of staff who achieve outstanding results in their studies while maintaining high levels of work performance.

ASIO also conducts an internal Seminar Series that consists of monthly presentations on topics of general professional interest to staff. It seeks to foster a sense of teamwork and a shared culture, through broadening knowledge of work areas across the Organisation. Seminars in 2006-07 included:

- exposure to new technologies in intelligence analysis;
- working with overseas partner agencies;
- ASIO's response to APEC;
- understanding warrant processes;
- the importance of effective security assessments;
- roles and responsibilities of managers; and
- a presentation by Ms Pru Goward on her experiences and observations as the former Sex Discrimination Commissioner and Commissioner Responsible for Age Discrimination.

Intelligence Training

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

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

Australian Intelligence Community Training

ASIO supports continued efforts to broaden understanding by AIC staff of the whole-of-government approach to intelligence needs and partnerships. This includes providing presenters and participants to AIC-wide induction and Senior Officer development programs. (see Table 8.2)

Table 8.2: ASIO participation in AIC courses, 2006-07

Course	ASIO presenters	ASIO participants
Working with the AIC	14	0
AIC Senior Officer Course	5	37
AIC Induction Course	103	168

Language training

ASIO continued to invest in the development of language skills.

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

Secondments

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

- Australian Federal Police;
- Australian Secret Intelligence Service (ASIS);
- Australian Transaction Reports and Analysis Centre;
- Defence Imagery and Geospatial Organisation;
- Defence Intelligence Organisation;
- Defence Science and Technology Organisation;
- Defence Signals Directorate (DSD);
- Department of Defence;
- Department of Finance and Administration;
- Department of Foreign Affairs and Trade;
- Department of Transport and Regional Services; and
- Office of National Assessments (ONA).

Complementing this cooperation and engagement, in 2006–07 ASIO seconded officers to DSD, ASIS, the Department of the Prime Minister and Cabinet and ONA.

Workplace Diversity

ASIO requires a workforce that reflects the diversity of the broader Australian community and has implemented strategies accordingly. These include the:

- (classified) *Workplace Diversity Program 2005-09*, which encourages the recognition and appreciation of individuals and their contribution to the corporate mission and objectives; and
- (classified) *Disability Action Plan* and ongoing monitoring and quarterly reporting of age, length of service and gender to the Corporate Executive.

Workforce diversity is monitored through the collection and reporting of relevant statistics to the Senior Management team. Table 8.4 shows the representation of designated groups within ASIO at 30 June 2007.

Table 8.3: Representation by rank at 30 June 2007

Group	Total Staff[1]	Available EEO Data[2]	Females	People from a non-English speaking background[3]	Aboriginal & Torres Strait Islander	People with a disability
SES (excl DG)	35	34	9	0	0	0
Senior Officers[4]	305	283	100	33	0	4
AO5[5]	388	379	187	74	2	3
AO1-4[6]	538	496	303	78	1	7
ITO1-2[7]	87	83	18	17	1	1
ENG1-2[8]	3	3	0	0	0	0
Total	1356	1278	617	202	4	15

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

[2] Provision of EEO data is voluntary

[3] Based on EEO data provided by staff

[4] Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the engineer and information technology classifications

[5] ASIO Officer grade 5 group translates to APS Level 6 and includes Intelligence Officers

[6] Translates to span the APS 1 to 5 classification level. Intelligence Officer Trainees are included in this group (equivalent to APS Level 5)

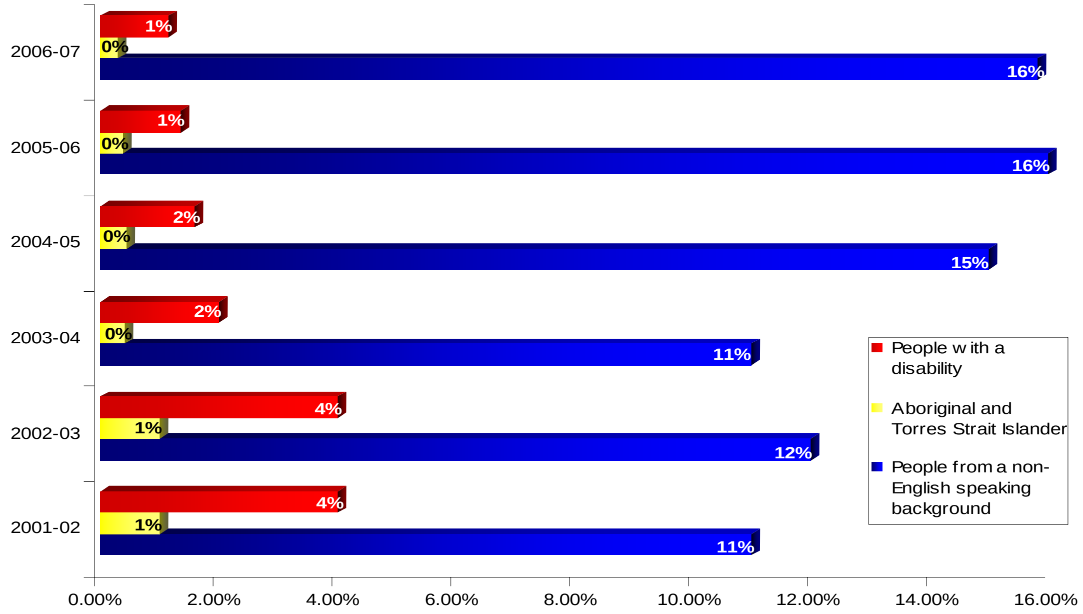
[7] Information Technology Officers grades 1 and 2

[8] Engineers grades 1 and 2

Ethnic diversity

Since 2001-02 there has been a steady increase in the proportion of ethnically diverse staff, but a decrease in the proportion of Aboriginal or Torres Strait Islander staff and those with a disability (See Chart 8.4). This decrease is attributable to the net growth of the Organisation – in 2006-07, 4 ASIO staff were Aboriginal or Torres Strait Islander and 15 had a disability, up from 4 and 14 respectively in 2005-06.

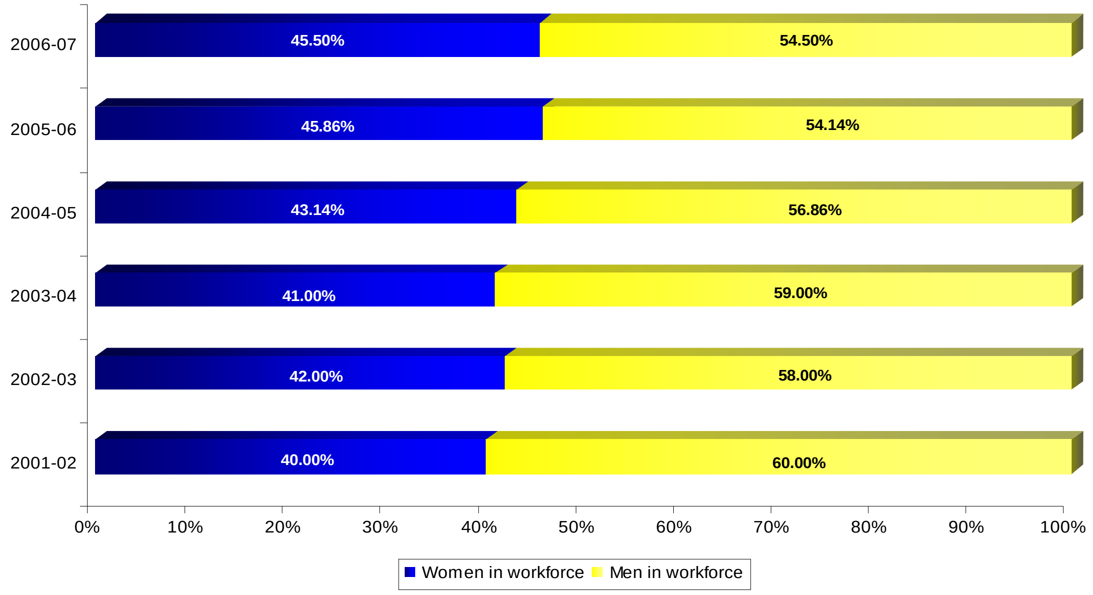
Chart 8.4: Ethnic diversity, 2001-02 to 2006-07



Gender representation

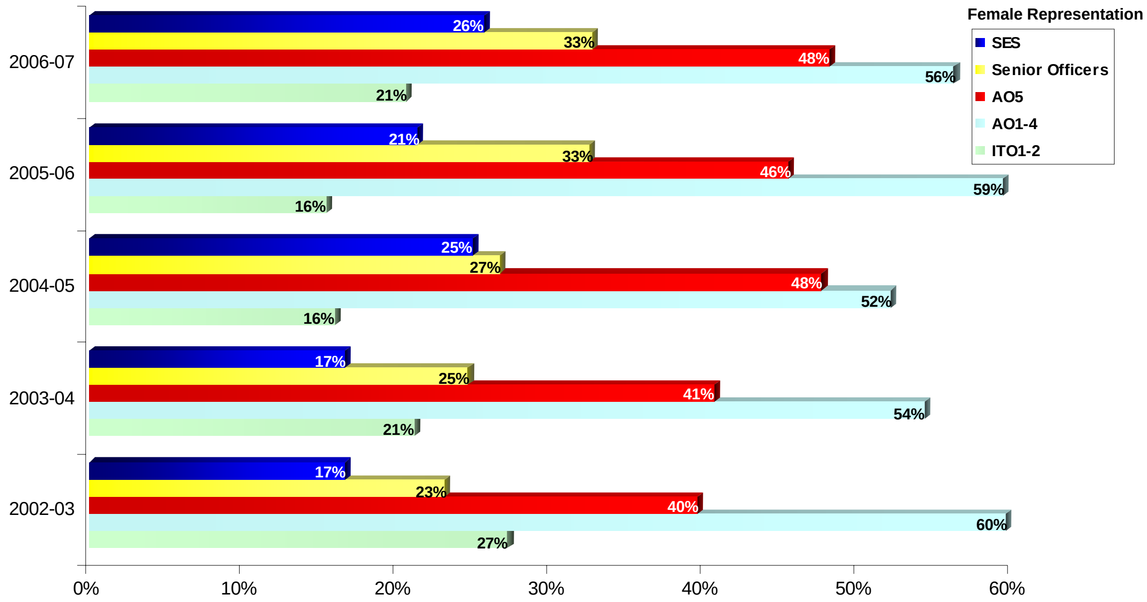
The representation by women in ASIO's workforce has risen steadily, from 40% in 2001-02 to 45.5% in 2006-07. (see Chart 8.5)

Chart 8.5: Gender representation, 2001-02 to 2006-07



Since 2002, there has been an upwards trend in the percentage of women occupying Senior Officer and SES positions within ASIO. (See Chart 8.6)

Chart 8.6: Gender representation by rank, 2002-03 to 2006-07



Staff complaints

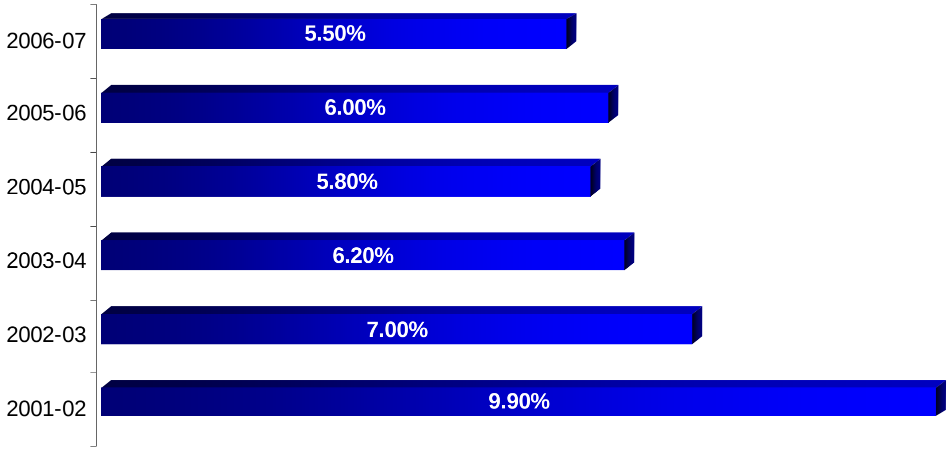
ASIO's Corporate Executive committee monitors staff complaints and grievance procedures.

In 2006-07 no formal complaints or grievances were lodged. This may be attributed to the focus ASIO has given to establishing Harassment Contact Officer (HCO) network which seeks to address issues proactively as they arise. During 2006-07, 13 matters were raised informally to the HCO network.

Separation Rates

ASIO's separation rate has decreased steadily since 2002, falling to 5.5% in 2006-07. In the context of voluntary separation interviews conducted over the past year, staff cited increased remuneration, promotion or career opportunities, work/life balance and greater job satisfaction as major reasons for their departure.

Chart 8.7: Separation rates, 2001-02 to 2006-07



STAFF PERFORMANCE MANAGEMENT AND EVALUATION

ASIO's staff performance management framework is an integrated system for staff evaluation which incorporates probation, performance appraisals and underperformance reviews. It is designed to link individual performance objectives to ASIO's business outcomes. Compliance with the Organisation's values and security principles are key assessable elements of the framework.

ASIO's current performance management system was introduced in 2002 and provides a comprehensive, integrated approach to all aspects of performance management within ASIO – probation, annual assessments and underperformance. It is designed to encourage and facilitate open, two-way communication between staff and management which jointly defines, evaluates and recognises performance to ensure that both the goals of the individual and Organisation are met.

Key features of the framework are:

- all staff members are required to participate in the scheme;
- definition of job-specific performance objectives/indicators which are aligned with corporate goals and priorities;
- assessment of performance against mandatory goals for all staff (security practices are integral to all professional and personal activities, and standards of work and behaviour are in accordance with ASIO's values);
- assessing line managers performance in encouraging their staff to participate in performance management and personal development; and
- identification of individual development requirements for current and future roles/careers.

By monitoring individual development needs, ASIO is able to identify emerging developmental needs to assist in the preparation of corporate strategies and budgets for subsequent financial years.

A continuing commitment to effective performance management is essential as ASIO undertakes significant workforce growth. Consequently ASIO has introduced a series of development activities to reinforce the importance of, and requirements associated with the framework. For example, a half-day session on probation, performance and underperformance management is a central component of the orientation course for Senior Officers. ASIO's Senior Executive Service and Senior Officers also undertake leadership/management development programs to obtain and refine human management skills.

ACCOMMODATION

The growth in staff numbers, flowing from the Government's decision in 2005 to increase ASIO capability, has put pressure on ASIO's accommodation nationally. A new Central Office building is required in Canberra. ASIO's offices in each State capital also will grow. The Central Office building in Russell, Canberra, is the only building that is declared publicly.

CENTRAL OFFICE, CANBERRA

On 12 April 2006, the Government agreed that ASIO and the Office of National Assessments (ONA) needed more space and a new Central Office building in Canberra was appropriate. On 16 August 2006, the Attorney-General and Minister for Finance and Administration announced that ASIO and ONA would move to a purpose-built building within Canberra's defence and security precinct.

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

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

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

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

STATE AND TERRITORY OFFICES

The Organisation's growth has put pressure on accommodation in our State and Territory offices. Funding was provided in the 2005–06 Additional Estimates, and in both the 2006–07 and 2007–08 Budgets, for the expansion of these offices. Significant progress has been made to deliver new and refurbished accommodation nationally.

The new and refurbished offices provide:

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

PUBLIC RELATIONS AND REPORTING

Although much of ASIO's work necessarily occurs outside the public view, ASIO relies upon the support of the Australian public to achieve its mission. While ASIO is unable, for reasons of operational security, to reveal the details of its operational activity in the public domain, ASIO nevertheless strives to provide the public with appropriate information on ASIO and its activities. As well as through its direct engagements with individuals, community representatives and businesses, ASIO provides information to the broader public through its own publications and statements, and through Parliamentary, Ministerial and legal processes, including:

- ASIO's annual *Report to Parliament*;
- ASIO's submissions to, and appearances, before Parliamentary committees;
- public statements and speeches by the Director-General of Security;
- ASIO's website; and
- the Business Liaison Unit (BLU).

The Inspector-General of Intelligence and Security (IGIS) also provides an annual report which may refer to aspects of ASIO's work.

REPORT TO PARLIAMENT

ASIO's annual report complies with the Requirements for Annual Reports issued by the Department of the Prime Minister and Cabinet. It also addresses specific requirements applying to the annual reports of Australia's intelligence and security agencies.

ASIO produces two versions of its annual report:

- a classified *Report to Parliament*; and
- an unclassified *Report to Parliament*.

The classified *Report to Parliament* contains an account of ASIO's performance across its functions during the previous 12 months. It includes details of operational outcomes, liaison activities, ASIO's reporting, and administrative activities, at a level that cannot be released publicly due to the sensitivity of the information. The distribution of the report is limited to the members of the National Security Committee of Cabinet, the Leader of the Opposition, and a small group of senior government officials.

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:

- Parliamentary Joint Committee on Intelligence and Security;
- Senate Standing Committee on Constitutional and Legal Affairs; and
- Senate Finance and Public Administration Committee.

Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) plays an important role in the oversight of ASIO. The PJCIS mandate includes reviewing the administration and expenditure of ASIO and the other AIC agencies, reviewing the listing of organisations as terrorist organisations under the *Criminal Code Act 1995*, and reviewing ASIO's questioning and detention powers.

The Director-General of Security or Deputy Director-General appeared before the PJCIS regarding the re-listing of:

- Abu Sayyaf, Jamiat ul-Ansar, Armed Islamic Group, and the Salafist Group for Call and Combat on 27 November 2006;
- Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn on 23 March 2007; and
- Hizballah's External Security Organisation on 18 June 2007.

The Deputy Director-General also appeared before the committee on 4 April 2007 at the inquiry into the terrorist organisation listing provisions of the *Criminal Code Act 1995*.

Senate Standing Committee on Constitutional and Legal 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 Estimates process and been questioned on aspects of its work. Senate Estimates hearings are open to the public and recorded in Hansard.

The Director-General of Security appeared before the committee on 31 October 2006 and 23 May 2007.

Senate Finance and Public Administration Committee

The Director-General of Security appeared before the Committee on 6 March 2007 in relation to the *Access Card – Inquiry into Human Services (Enhanced Service Delivery) Bill 2007*.

PUBLIC STATEMENTS

Public comments about the activities of ASIO may be provided by:

- the Attorney-General, as ASIO's Minister;
- the Director-General of Security; or
- ASIO's Media and Ministerial Liaison Officer (MMLO).

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 2006-07 the Director-General of Security delivered 18 public addresses, transcripts of which are available on ASIO's website.

ASIO's MMLO 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 website also provides links to related sites including the Attorney-General, Parliamentary Joint Committee on Intelligence and Security, the Inspector-General of Intelligence of Security and other members of the Australian Intelligence Community.

During 2006-07 ASIO upgraded its website.

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 better understand the security environment and the threats they face, and to provide them with a basis for security planning.

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

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

INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The Inspector-General of Intelligence and Security's (IGIS) role is to ensure that ASIO and the other members of the AIC act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights. The IGIS, whose powers are akin to those of a standing Royal Commission, has unlimited access to ASIO's operational, administrative, and all other records and may initiative enquiries into any aspect of ASIO's activities.

The IGIS provides a classified annual report to the Government, and an unclassified annual report that is tabled in Parliament. The report contains an overview of complaints against the intelligence agencies and the outcome of the IGIS's inquiries into them.

The IGIS may also provide other reports to the Government or to the public on the results of investigations undertaken at any time.