



**Australian Government**

**Australian Security  
Intelligence Organisation**

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

# REVIEW OF ADMINISTRATION AND EXPENDITURE

No.5; 2007

**ASIO**



UNCLASSIFIED

AUSTRALIAN SECURITY  
INTELLIGENCE ORGANISATION

---

Submission to the  
Parliamentary Joint Committee on Intelligence and Security

REVIEW OF ADMINISTRATION AND  
EXPENDITURE No.5

*28 February 2007*

UNCLASSIFIED



# Contents

---

	Page
1 Executive Overview .....	1
2 Budget .....	9
3 Organisational Structure .....	12
4 Strategic Planning and Management .....	16
5 Legislative Changes in 2006 .....	19
6 Intelligence Capabilities: Collection .....	23
7 Intelligence Capabilities: Technical Capabilities .....	30
8 Intelligence Capabilities: Technical Operations .....	31
9 Intelligence Capabilities: Surveillance .....	32
10 Intelligence Capabilities: Telecommunications Interception.....	34
11 Intelligence Capabilities: Intelligence Analysis .....	37
12 Intelligence Capabilities: Support for Litigation.....	40
13 Intelligence Capabilities: Counter-Espionage and Foreign Interference .....	41
14 Human Resource Management: Recruitment.....	45
15 Human Resource Management: Training .....	49
16 Human Resource Management: Workplace Diversity, Retention & Complaints.....	52
17 Staff Performance Management and Evaluation .....	56
18 Accommodation .....	58
19 Security .....	62
20 Public Relations and Reporting .....	65



# 1 Executive Overview

---

## OVERVIEW

In 2004 ASIO provided an unclassified submission and a private classified briefing to the then Parliamentary Joint Committee on ASIO, ASIS and DSD's *Review of Administration and Expenditure for ASIO, ASIS and DSD Number 3*. In 2006 ASIO again provided an unclassified submission and a private classified briefing to the Parliamentary Joint Committee on Intelligence and Security's *Review of Administration and Expenditure: Australian Intelligence Organisations Number 4 – Recruitment and Training*.

ASIO values the Committee's oversight in connection with the Organisation's administration and expenditure and is committed to engaging with the Committee on these matters. ASIO is pleased to present a classified submission and an unclassified version of the submission to the Committee. ASIO also will provide a private classified briefing. The provision of a classified and an unclassified version of the submission is intended to assist the Committee in the conduct of its review as well as its presentation to the Parliament of a report which will be available publicly.

## ASIO's ROLE

ASIO is Australia's security service. ASIO's mission is to provide advice to protect Australia and its people from threats to security as defined in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

In practice, ASIO is primarily a counter-terrorism and counter-espionage agency. Its responsibilities are defined in legislation thematically, not geographically. It is not purely a domestic service. While the great majority of ASIO's work is within Australia, significant elements relate to overseas—for example, Australians overseas of security interest, overseas connections of groups/individuals in Australia and our threat assessment responsibilities relating to Australian interests worldwide.

The National Counter-Terrorism Plan states that Australia relies upon a strong intelligence-led prevention and preparedness regime to support its counter-terrorism strategy. Intelligence capacity is an Australian Government responsibility. In policing and emergency management, the States and Territories have resources which can be drawn on when needed to bolster the Australian Government response. There is limited corresponding capacity in the States and Territories in intelligence.

Within this framework, ASIO has a wide set of roles and functions. It is both a collector and an assessor of intelligence – the only agency within the Australian Intelligence Community to undertake both roles. Its collection activity, and a large part of its analytical activity, is directed at investigating people and groups who are suspected of engaging in activities likely to result in harm to Australia or its interests, both here and overseas. It has a specific national threat assessment role as well as sole responsibility for foreign intelligence collection under warrant in Australia and a long-standing protective security role. ASIO also has an advisory role in respect of security

## UNCLASSIFIED

clearances, counter-terrorism checks, temporary and permanent entry to Australia, citizenship, the denial or cancellation of passports on security grounds and the release of documents under the *Archives Act 1983*. It has a formal 'lead-house' role on telecommunications interception among the security/law enforcement community.

Government expects ASIO to: fulfill its statutory responsibilities by maintaining a strong intelligence capability; contribute to the broader government effort on counter-terrorism initiatives; contribute to national schemes for security checking that are comprehensive, coordinated and consistently administered; be a critical and authoritative voice in security assessments; and maintain a 'one-stop-shop' for high-quality threat assessments.

Successful security intelligence work requires a detailed and persistent approach to investigation and analysis, and the flexibility and agility to react to new leads and threats as they arise. ASIO assesses the information available to it, makes judgments about its credibility and reliability, resolves any ambiguities and provides advice that is as specific as possible.

The value of ASIO's advice and the contribution it makes to the protection of Australia and Australians is dependent on the quality of the information available, the effectiveness of the tools it uses to collect and analyse it, and the caliber of the people engaged in this important work. While there can be no guarantee that ASIO will always have prior intelligence to prevent harm, there is a clear expectation that there will be no preventable 'intelligence failures' that result in the death or injury of Australians or other significant harm to our interests.

After the end of the Cold War in the early 1990s, ASIO's focus had been shifting increasingly to the threat of Islamic extremism and its manifestations through acts of terrorism around the world. Prior to the attacks in the United States on 11 September 2001, ASIO had developed a good understanding of the complexity of the problem, although the ongoing impact and the sheer scale of the work involved in countering the threat had yet to become apparent. We now know that Australia and Australians are terrorist targets, that an attack in Australia is feasible and could well occur, and that Australians have been the focus of aborted, disrupted or actual terrorist attacks since 2000.

In response to the changes in the perception and the reality of the terrorist threat wrought by the September 2001 attacks, ASIO underwent modest growth from 2002 as a result of a series of New Policy Proposals. Particular aspects of ASIO's work that have changed significantly since 2000–01 include:

- increased volume and pace of information flowing to ASIO;
- the move to 24x7 operations for the threat assessment, global monitoring and border security functions;
- increased engagement with international and Australian partners;
- increased engagement with law enforcement agencies, including increased support for prosecutions;
- closer engagement with the private sector;
- new legislative powers;



## UNCLASSIFIED

- increased public profile and Parliamentary scrutiny;
- increasingly sophisticated targets; and
- rapid technological change, including that available to individuals of security interest.

Following the Taylor Review of ASIO Resourcing in 2005 the Government committed additional resources to ASIO that will see the Organisation grow to 1,860 staff and operating with enhanced capabilities across a range of functions by 2010–11. Staffing is currently at around 1,300.

The growth of ASIO from 584 staff at 30 June 2001 to 1,860 staff by 30 June 2011 is a challenging exercise on a number of fronts, including recruitment, training, accommodation and infrastructure. ASIO is not the only agency seeking to recruit high-calibre staff in a tight employment market. ASIO's recruitment efforts are, however, spread across a range of job families and skill sets. Recruitment is being undertaken strategically to ensure an appropriate balance between core business and enabling functions. Similarly, ASIO is seeking to achieve appropriate synergies between the growth in its staff numbers and the expansion and enhancement of the Organisation's IT infrastructure and accommodation arrangements. This is to ensure that ASIO maintains its focus and effectiveness on its core business while undergoing this period of growth.

### RECENT DEVELOPMENTS/TRENDS

Further details about recent developments and trends in ASIO's administration and expenditure as the Organisation undergoes a period of planned and systematic growth are set out in the following sections. A brief summary is provided below.

#### *Budget*

ASIO's revenue from Government has increased from \$66m in 2001–02 to \$227m in 2006–07 and is expected to grow to \$392m by 2009–10. ASIO's equity injections have also increased from \$4m in 2001–02 to \$113m in 2006–07.

ASIO had recorded operating deficits in the period from 2001–02 to 2003–04 although in 2004–05 it recorded an operating surplus of \$526k, reflecting the easing of budgetary pressures through additional funding. ASIO's operating surplus in 2005–06 was \$11.8m, largely due to the higher than anticipated capitalisation of expenditure on capital works. This expenditure relates to consultancies required to deliver information technology, technical and property projects.

#### *Organisational Structure*

On 1 July 2006 ASIO implemented a nine-division structure to replace the previous five-division model. While not all positions in the new structure will be filled until 2010–11, the decision was taken that it was preferable to have a first-cut of the 'final' framework in place early and to work towards populating it through a planned program of recruitment. The alternative of making constant incremental changes to the structure as the Organisation grew was seen as potentially disruptive and

## UNCLASSIFIED

unnecessary given the certainty afforded by the Government's endorsement of the recommendations of the Taylor Review.

While in the first years of growth arising from the Taylor Review, additional resources have been allocated to the intelligence collection and analysis functions, greater emphasis has been placed on building the enabling functions for the Organisation to support the growth (for example, staff in areas such as IT, recruitment, training and facilities management). This was to ensure that new staff in the operational areas could be brought into the Organisation in the most efficient manner and have quality support mechanisms in place to enable them to become effective in the shortest possible time.

ASIO will continue to focus on building its capabilities across the full range of functions it performs.

### *Strategic Planning and Management*

As part of the implementation of the nine-division structure, ASIO revised its corporate governance framework. ASIO's corporate governance arrangements support the management of risk, the flexible allocation of resources to meet changing business needs, regular critical review of performance across all functions as well as providing for transparency and accountability.

There is a regular schedule of meetings of ASIO's senior executive and a system of committees spanning ASIO's functions. Meeting and reporting arrangements ensure the Director-General, Deputy Director-General and the division heads remain informed about matters and are able to provide high quality guidance and leadership across the Organisation.

### *Legislative Changes in 2006*

There were a number of legislative amendments in 2006 that impacted both directly and indirectly on ASIO. Overall, the legislative changes that have occurred since 2002 have sought to refine and enhance ASIO's powers and its ability to perform its functions effectively in the current security environment.

### *Intelligence Capabilities: Collection*

ASIO's intelligence collection resources have been growing, although the bulk of the growth arising from the Taylor Review will occur in future years, particularly in 2007-08.

ASIO collects intelligence by using a number of methods, including the use of human sources, special powers operations conducted under warrant, cooperation with a range of Australian and international agencies. In addition to information obtained through covert means extensive use is made of open source information.

The current security environment requires a continual balancing of the urgency, complexity and volume of information and makes heavy demands on resources. In recognition of the magnitude and complexity of the task of managing this risk, in early 2006 the management structure of the Collection Division was adjusted so that there are now three Senior Executive Service officers based outside Canberra.

## UNCLASSIFIED

Training of Intelligence Officers is time intensive and not something that can be easily replicated outside the intelligence community. While language skills can add to the repertoire and capabilities of ASIO's Intelligence Officers, of greater importance is the need for Intelligence Officers to be culturally aware and sensitive, to understand the parameters of their role and to have strong analytical and interpersonal skills. ASIO also employs specialised Linguists to undertake translation and interpreting work.

Refinements to the legislation governing ASIO's use of special powers generally has increased ASIO's operational flexibility and responsiveness while retaining a rigorous regime for approvals and accountability. ASIO has not invoked its detention powers since they were introduced in 2003 but has utilised 15 questioning warrants, involving 14 people (3 in 2003–04, 11 in 2004–05 and 1 in 2005–06).

### *Intelligence Capabilities: Technical Capabilities*

ASIO's Technical Capabilities Division works in close co-operation with the Collection and Counter-Espionage and Interference Divisions. It is responsible for the technical aspects of ASIO's special powers operations and the development and maintenance of capabilities to meet special powers requirements. It also manages ASIO's physical surveillance resources. The Division covers three intelligence capabilities – Technical Operations, Surveillance and Telecommunications Interception.

### *Intelligence Capabilities: Technical Operations*

In recent years most of ASIO's technical operations have focused on the execution of special powers operations in support of counter-terrorism investigations and, to a lesser extent, foreign intelligence collection activities.

ASIO needs to continue to invest in maintaining and improving its technical capabilities if it is to remain at the leading edge of technology.

### *Intelligence Capabilities: Surveillance*

ASIO maintains a specialist surveillance capability to support the collection of intelligence. As with ASIO's other investigative activities, surveillance is now conducted in a more complex environment against a diverse range of subjects. ASIO's surveillance capability has been growing since 2003 and will continue to grow until full capacity is achieved in 2009. Balancing operational requirements against the training and development needs of new staff will remain a challenge.

### *Intelligence Capabilities: Telecommunications Interception*

ASIO invests significantly in the development and maintenance of its telecommunications interception systems and to meet its responsibilities as the 'Lead Agency' for security and law enforcements agencies on interception matters.

### *Intelligence Capabilities: Intelligence Analysis*

The nine-division structure has provided for greater specialisation across the various areas of intelligence analysis, including investigative analysis and strategic analysis.

## UNCLASSIFIED

The primary focus remains on counter-terrorism but as additional resources come on line it has been possible to boost the effort against other sources of threat.

Growth areas have included: providing intelligence support to prosecutions; greater effort on counter-proliferation work; responding to leads generated by the National Security Hotline and other sources; and the provision of security intelligence support for special events of national significance. These growth areas, together with increases in the volume of information flowing into ASIO, have driven the development of new techniques and capabilities to underpin the analysis function and the ability of ASIO to provide high quality and timely advice.

### *Intelligence Capabilities: Support for Litigation*

The creation of an Executive and Legal Division has provided a framework for an enhanced in-house legal capability through two new branches – one focused on the provision of in-house legal advice and the other on litigation. In addition, a new Counter-Terrorism Litigation Advice Branch within the Investigative Analysis and Advice Division provides a specialised capability directed at supporting prosecutions wherever possible, while at the same time protecting ASIO's ability to operate effectively.

### *Intelligence Capabilities: Counter-Espionage and Foreign Interference*

ASIO's work in this area is conducted within a separate divisional management structure to other security intelligence investigations in recognition of the particular requirements of this subject. It has been important to stage the growth in this area carefully so as to maintain a balance between experienced and new staff and to allow for effective mentoring and training.

### *Human Resource Management: Recruitment*

ASIO achieved net staff growth of 155 in 2005–06, and is confident of meeting the target of annualised net average growth of 170 in 2006–07. Recruitment into some job families remains challenging in a tight and competitive employment market, however, ASIO continues to develop and refine its attraction strategies to ensure it remains competitive as an employer.

ASIO has bolstered the recruitment area, streamlined processes and enhanced recruitment systems, through:

- using a 'job family' approach to recruitment campaigns to improve recruitment efficiency and to enhance recruitment planning;
- continued selected use of recruitment agencies for response management and sourcing of applicants;
- the upgrading of recruitment data management, including development of an online recruitment capability;
- a strong presence at Australian Intelligence Community university career presentations;
- the development of a Recruitment Task Force to provide further capability during peak periods; and

## UNCLASSIFIED

- using innovative advertising concepts for some job families, targeting relevant industry publications, internet advertising including career websites and Google, and use of personal case studies as a marketing strategy.

### *Human Resource Management: Training*

The training and development of new staff remains a high priority. In 2006 ASIO's Audit and Evaluation Committee commissioned an external evaluation of ASIO's non-intelligence training programs. Recommendations from that review will be considered and implemented from early 2007 to ensure relevance and effectiveness. Other training programs, including the Intelligence Officer traineeship are subject to ongoing review and refinement in the light of experience.

### *Human Resource Management: Workplace Diversity, Retention, Complaints*

ASIO has a range of strategies and programs designed to deliver good human resource management across the Organisation. Workplace diversity has been increasing as the Organisation grows and seeks to reflect broadly Australian society. ASIO's separation rate has been decreasing steadily since 2002 and remains at around 6%. The number of formal staff complaints has shown a steady decrease since 2003–04.

### *Human Resource Management: Staff Performance Management and Evaluation*

ASIO's performance management framework receives strong and visible support from the senior executive and this has contributed to 98% of staff having a current agreement in place. This is an improvement on previous years and is 13% higher than the average participation rate in the Australian Public Service.

### *Accommodation*

The growth in staffing numbers has put pressure on ASIO's accommodation nationally. Funding for the construction of a new building housing ASIO's Central Office and the Office of National Assessments is subject to normal budget processes and will be offset against the funding already provided for the superseded extension to ASIO's existing Central Office building. Consultations will occur with the Public Works Committee, National Capital Authority and Department of Environment and Heritage. Some of ASIO's State and Territory Offices also require new accommodation.

### *Security*

ASIO has a strong security framework and culture comprising structures, policies and training, and it closely monitors emerging issues to maintain best security practice.

Before joining ASIO, prospective staff members are subject to stringent background and suitability checking. The revalidation program ensures that staff members remain suitable to have access to national security classified material. There has been a steady decline in the percentage of security breaches incurred by ASIO staff since the introduction of a revised policy in July 2005 which provided benchmarks for all staff to meet, in relation to security breaches, as part of their performance agreements.

## UNCLASSIFIED

### *Public Relations and Reporting*

ASIO provides the public with as much information as possible within the constraints of security. ASIO continues to be the only agency in the Australian Intelligence Community, and one of very few similar agencies around the world, that produces an unclassified annual report. Information about ASIO also is available publicly through a range of other sources. The increase in the number of public statements by the Director-General (which are available on ASIO's website) further increases ASIO's public profile.

## 2 Budget

---

### OVERVIEW

ASIO's budget is set out in the Portfolio Budget Statements (PBS) with the audited outcome published in its annual report. 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.

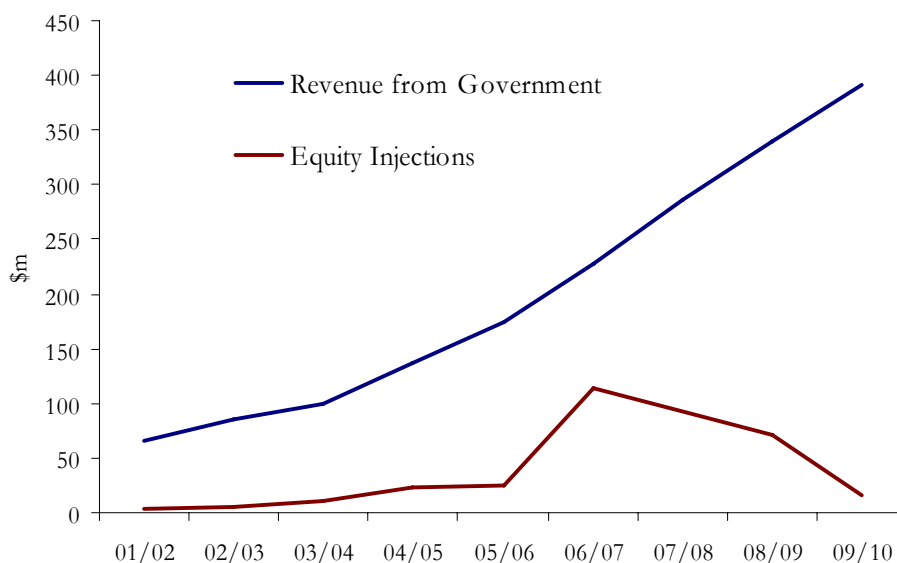
In support of the Government policy aim of *'A secure Australia in a secure region'*, ASIO's budget is directed towards achieving its Outcome of *'A secure Australia for people and property, for government business and national infrastructure, and for special events of national and international significance'*.

### 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 and 2009–10 show an increase to \$286m, \$338m and \$392m respectively (see Chart 2.1).

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 and 2009–10 show a decrease to \$93m, \$71m and \$16m respectively (see Chart 2.1).

**Chart 2.1: ASIO's Revenue from Government 2001–02 to 2009–10**



## UNCLASSIFIED

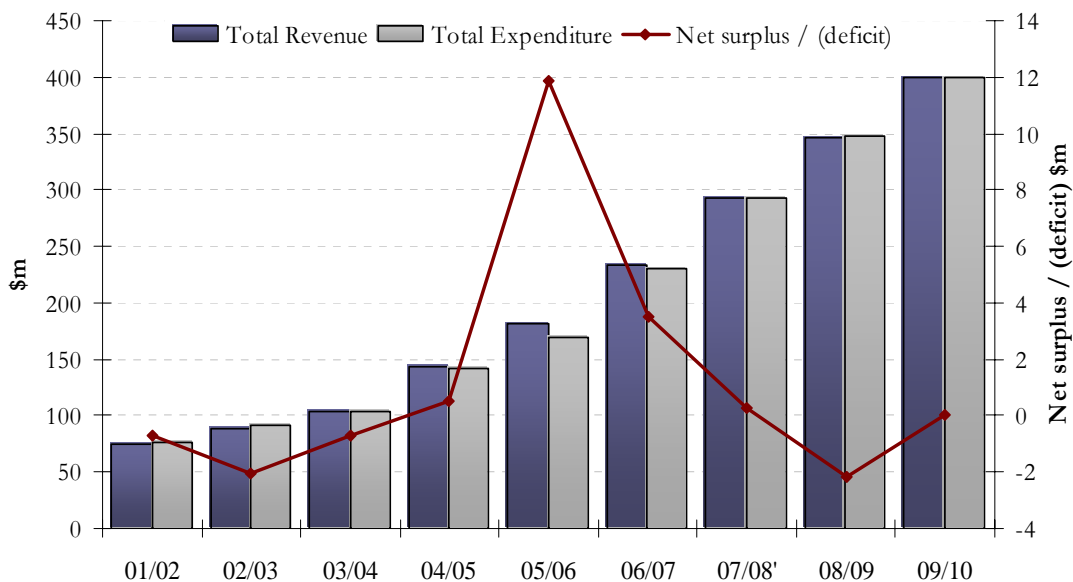
The significant increase in ASIO's budget in 2006–07 predominantly arises from the Taylor Review. The increase in funding was for staffing and for ASIO to purchase equipment to support growth in the technical operations/surveillance area, for necessary enhancements to its information technology infrastructure 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 Central Office and State/Territory offices.

### *ASIO's Financial Performance*

In relation to the period being reviewed, 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, ASIO recorded an operating surplus of \$526k in 2004–05. This surplus reflected the easing of budgetary pressures on the Organisation through additional funding by Government in 2004–05.

As shown in Chart 2.2, the 2005–06 financial year saw an operating surplus of \$11.8m. The result was approximately \$3m higher than forecast in the PBS due largely to higher than anticipated capitalisation of expenditure on capital works. This expenditure relates to consultancies required to deliver information technology, technical and property projects.

**Chart 2.2: Financial Performance 2001–02 to 2009–10**





## UNCLASSIFIED

### *Financial Management and Internal Controls*

ASIO prepares annual financial statements (which are publicly available) 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 the Deputy Director-General and includes a 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 Director-General, the Deputy Director-General and the Corporate Executive on the financial performance of the Organisation. These reports are audited by ANAO.

ASIO has a robust and reliable Financial Management Information System (FMIS) and a comprehensive suite of management reports which the CE considers monthly. The internal financial management reports have evolved since they were developed in 1999 and provide both Senior Managers and Project Managers with detailed financial information on project and budget delivery.

The rise in ASIO's budget has positioned the Organisation well to deliver the significant growth identified by the Taylor Review. Over the past financial year this growth has enabled ASIO to establish a solid budget and project management framework, including a financial reporting platform to support and monitor project delivery, and provide early identification of potential budgetary issues before they become problematic.

### FUTURE FOCUS

A challenge for ASIO in managing its budget into the future is the cost of employee-related expenses from negotiated workplace agreements. These agreements are an essential element of remaining an attractive employer able to recruit and retain the high-calibre staff that we require.

## 3 Organisational Structure

---

### OVERVIEW

Following the Government's endorsement of ASIO's proposed resourcing plan (developed as part of the Taylor Review), ASIO implemented a revised organisational structure based on nine divisions which came into effect from 1 July 2006 (Chart 3.1 refers).

The nine-division structure provides logical groupings of functions and responsibilities. It also provides defined points of focus for meeting Government expectations of ASIO's performance across all areas. It facilitates more effective line management and staff development by ensuring reasonable spans of management responsibilities at all levels and across all divisions.

Key changes compared to the previous structure (Chart 3.2 refers) include:

- the creation of a division to address threats from espionage and foreign interference that complements the focus on terrorism and other extremist activity;
- new branch structures to respond to ASIO's increased involvement in legal matters:
  - one branch with direct alignment to the intelligence business deals with the complex issue of utilising intelligence in legal proceedings;
  - another branch forms part of an expanded team of in-house lawyers;
- the creation of a Security Assessments Branch within the Security Division which brings together all areas providing assessments of individuals relating to border security, counter-terrorism or access to classified information;
- the creation of a Surveillance Branch to reflect the growth in size and complexity of ASIO's physical surveillance capacity; and
- the creation of an Information Division to provide more effective knowledge management, robust delivery of critical enabling infrastructure and information systems and better IT capability to enhance security intelligence outcomes.

Other areas have retained existing structures or have been strengthened:

- the National Threat Assessment Centre retains its focus to provide comprehensive advice on threats to Australian interests;
- The Collection Division branches have been adjusted to reflect the national coverage provided by this division focused on the critical issues of developing effective human sources and managing operations to gain intelligence on terrorism, other politically motivated violence, and proliferation; and
- Security Division retains the effective concept of a 'one-stop-shop' for security advice, continuing the connection between advice to government and advice to business.

Chart 3.1: Organisational Structure as at 1 July 2006

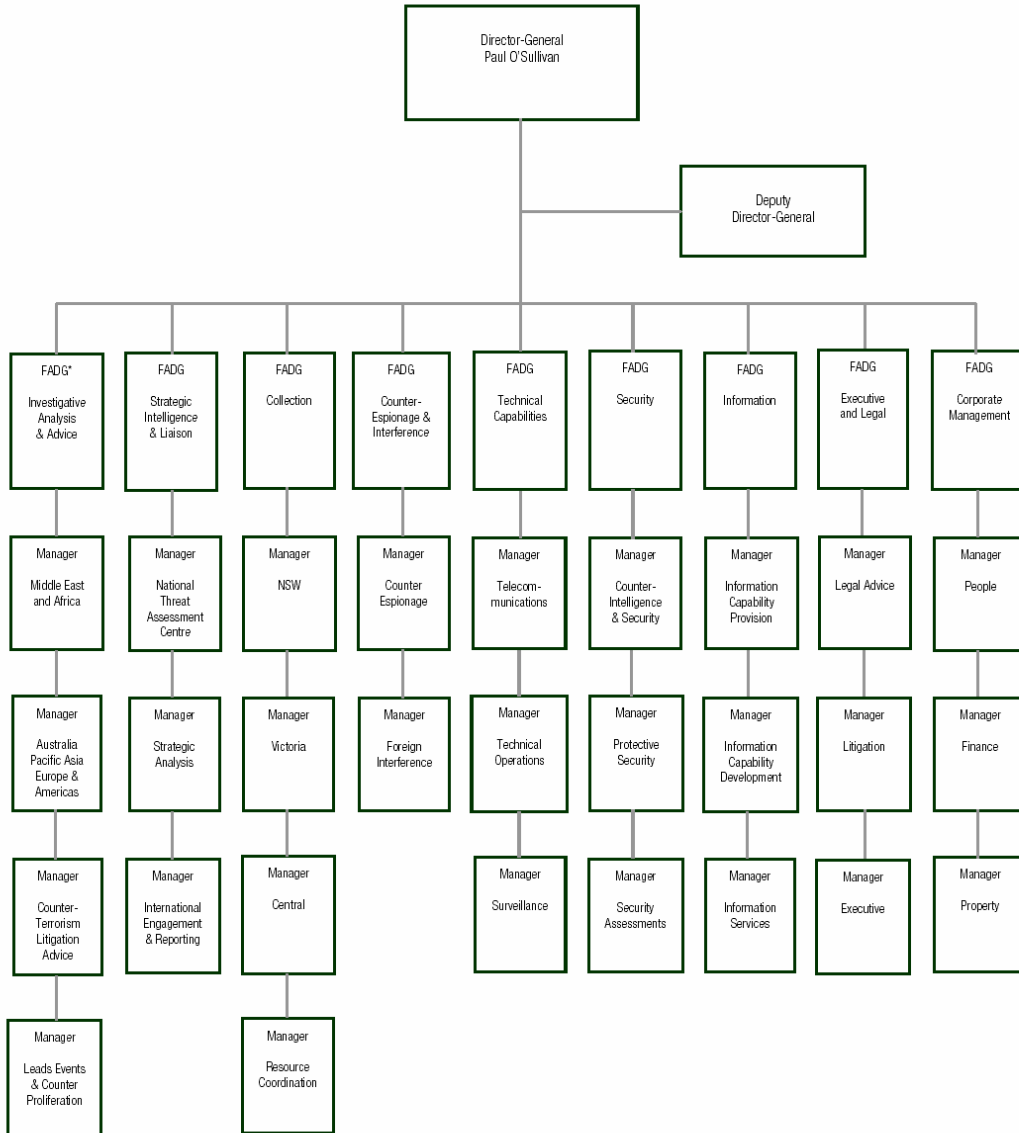
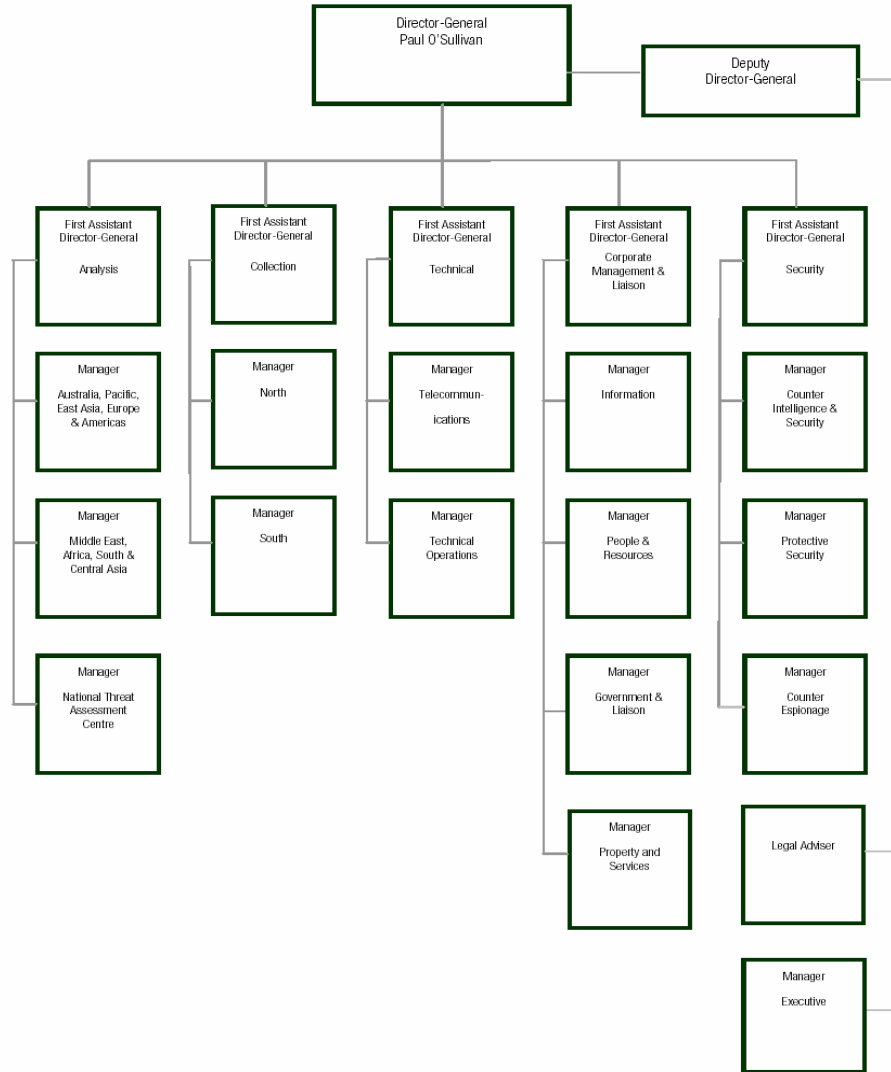


Chart 3.2: Organisational Structure as at 30 June 2006



*Planned Approach*

A critical focus has been the strategic management of growth through carefully planned and executed recruitment activities. ASIO’s recruitment program is reviewed regularly to ensure the structure is populated methodically with a constant focus on the growth target while continuing to develop and deliver critical security intelligence advice.

Positions will be filled progressively through to 2010–11 as a result of a planned rate of growth of around 170 net per year. ASIO has recognised the challenge of recruiting the right people at the right time – to grow while continuing to meet critical business priorities. To facilitate the appropriate focus of recruitment activity, ASIO has adopted the following methodology to prioritise areas for growth:

- an initial cut of the structure into which ASIO will grow by 2010–11 has been determined;
- all vacancies are ranked against criteria assessing the criticality of the position to security intelligence priorities and to growth-enabling priorities;

## UNCLASSIFIED

- the allocation of new staff to all areas of ASIO is prioritised on a year-by-year basis and reviewed every six months;
- efficiencies have been introduced into the recruitment process by grouping positions in different parts of ASIO into 'job families' which can be selected and assessed simultaneously, minimising the number of individual recruitment campaigns and maximising the output from each campaign; and
- progress against targets is reviewed regularly by the Director-General's Meeting and the Corporate Executive.

Project plans from all areas contributing to ASIO's growth are aggregated and a traditional project planning methodology, which has been a long-standing feature of ASIO's operation, is used. Established internal performance reporting regimes are used to measure progress against meaningful implementation milestones.

The Cabinet Implementation Unit in the Department of the Prime Minister and Cabinet receives regular briefings on progress.

The Taylor Review commended ASIO's approach to recruitment and staff development and recommended these practices be maintained as ASIO moves toward the target of 1,860 staff by 30 June 2011. ASIO is working to strengthen the enabling areas within the Organisation such as recruitment, human resources, learning and development, and information technology. This approach will ensure new staff are brought into the Organisation in the most efficient manner and have quality development, training and support mechanisms to allow them to reach their full potential in the shortest possible time. In addition to the focus on the enabling areas of the Organisation, recruitment effort has been focused on Surveillance Officers, Intelligence Officers and Intelligence Analysts.

### FUTURE FOCUS

The nine-division structure provides for management arrangements which are better aligned with the needs of a larger organisation. ASIO will continue to focus on building its capabilities across the full range of functions it performs. Continuing to recruit the right people at the right time and in the right numbers will be challenging in a tight and competitive employment market. Similarly, retaining experienced staff who will be required to play a key role in training and mentoring newer staff will be particularly important.

## 4 Strategic Planning and Management

---

### OVERVIEW

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

Business priorities are regularly reviewed by senior management. ASIO also has an active audit, evaluation and fraud control program, and has a strong record of self-initiated reviews.

### RECENT DEVELOPMENTS/TRENDS

#### *Senior Executive Service of ASIO*

The senior executive of ASIO consists of the Director-General, Deputy Director-General, First Assistant Directors-General (division heads) and Managers (branch heads). All but three Senior Executive Service positions are Canberra-based.

#### *Corporate Governance*

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

The DGM is chaired by the Director-General and consists of the Deputy Director-General and all division heads. It meets twice weekly, or more frequently if required, to manage the day-to-day business of the Organisation, including urgent or emerging issues requiring consideration by the Executive.

The CE is chaired by the Director-General and its members include the Deputy Director-General, all division heads and two managers on rotation. The President of the ASIO Staff Association attends as an observer. The CE meets twice monthly, sets the overall strategic direction of the Organisation and oversees resource management. The CE is the main forum for managing strategic corporate priorities and resource issues. It also conducts detailed quarterly reviews of the Organisation's performance, the results of which feed into ASIO's *Annual Report*.

The CE is supported by the following corporate committees:

- *Intelligence Coordination Committee* – chaired by the Deputy Director-General and includes division heads involved in managing the various functions in connection with intelligence investigations.
- *Audit and Evaluation Committee* – chaired by the Deputy Director-General and includes a senior officer from the Australian National Audit Office (ANAO).

## UNCLASSIFIED

- *Organisational Development Committee* – chaired by the head of Corporate Management Division and includes representatives from the ASIO Staff Association. It provides guidance on staff development issues.
- *Staff Placements Committee* - chaired by the head of Corporate Management Division and includes all division heads. It makes strategic decisions on staff placements, particularly in relation to mobility and staff commencements following job-family recruitment processes, and provides recommendations to the DGM.
- *Security Committee* – chaired by the head of Security Division and includes representatives of the ASIO Staff Association. It promotes sound security practice.
- *Consultative Council*, comprising representatives from management and the ASIO Staff Association, providing a forum for discussions and negotiations on employment and conditions of service issues.
- *Information Management Committee* – chaired by the head of the Information Division. It provides guidance and sets priorities for the development of ASIO's information systems.
- *Research and Development Committee* – chaired by the head of the Technical Capabilities Division. It oversees ASIO's research and development work.

There is also a temporary corporate committee for the period of Australia hosting APEC which is chaired by a division head and which provides strategic management of ASIO's contribution to APEC security.

### *Corporate Planning*

ASIO's *Corporate Plan 2007–2011* sets the broad framework for how ASIO does its business, measures its performance and achieves outcomes. The new plan was released in early 2007.

### *Audit, Evaluation and Fraud Control*

ASIO has a *Fraud Control Plan 2006–08* and carries out the normal audit, evaluation and fraud control programs.

- ASIO's program of internal reviews, audits and evaluations are overseen by the Audit and Evaluation Committee.
- During 2005–06 nine 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.

### *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.

## UNCLASSIFIED

- ASIO conducts an annual survey of key clients from Commonwealth departments and agencies and from State and Territory police services. The results of these reviews 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.
  - In some cases, ASIO has established boards/steering committees to provide strategic oversight for major projects.

### *Strategic Allocation of Resources*

ASIO uses an Outcome/Outputs framework to provide accurate information in its *Annual Report* on how the Outputs are meeting the Outcome of 'A secure Australia for people and property, government business and national infrastructure, and special events of national and international significance' and the Government policy aim of 'a secure Australia in a secure region'. The Outcome/Outputs structure is outlined in ASIO's *Report to Parliament*.

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 before the beginning of the financial year. 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.

### *Review of Performance and Resource Allocation*

Across investigations, ASIO's Intelligence Coordination Committee (ICC) meets quarterly to formally review performance and resource allocation for ASIO's investigations.

The CE also oversees the strategic allocation of resources by tracking changes with a workforce profiling tool on a six monthly basis. The workforce profile is an analysis in table format of staff by job family. The profile shows staff in actual and percentage terms allowing:

- tracking of changes to the number of staff in each job family; and
- comparisons over time.



## 5 Legislative Changes in 2006

---

### OVERVIEW

Following is a brief summary of key legislative amendments to:

- the ASIO Act;
- the *Telecommunications (Interception) Act 1979*;
- the *Anti-terrorism (No.1) Act 2005* and the *Anti-terrorism (No.2) Act 2005*;
- ASIO-related amendments;
- police-related amendments; and
- amendments to terrorist financing offences.

### RECENT DEVELOPMENTS

#### *Amendments to the ASIO Act*

In June 2006 the ASIO Act was amended by the *ASIO Legislation Amendment Act 2006* (the *2006 Act*). The primary effect of the *2006 Act* was to amend ASIO's questioning and detention powers by extending the sunset clause [and making structural changes to the layout of the questioning and detention powers].

The *2006 Act* has extended the sunset clause applying to ASIO's questioning and detention powers by 10 years. ASIO's questioning and detention powers will now be reviewed by the Parliamentary Joint Committee on Intelligence and Security by January 2016, with the powers expiring on 22 July 2016.

The *2006 Act* has drawn a distinction between 'questioning-only' and 'questioning and detention' warrants. Other changes made by the *2006 Act* to the questioning and detention warrant regime include:

- introducing an explicit right for the subject of a 'questioning-only' warrant to contact a lawyer;
- clarification of the ability of subjects of both warrants to make complaints to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman, or a State or Territory complaints body;
- introduction of a requirement for the prescribed authority to explain more clearly her/his role; and
- codification of the right of the subject's lawyer to address the prescribed authority during breaks in questioning.

## UNCLASSIFIED

### *Amendments to the Telecommunications (Interception) Act 1979*

In July 2006 the *Telecommunications (Interception) Amendment Act 2006* amended the *Telecommunications (Interception) Act 1979* (the TI Act) and its name to the *Telecommunications (Interception and Access) Act 1979*. The new Act implemented certain recommendations of the Report on the Review of the Regulation of Access to Communications (the Blunn Report).

Among other things, the Bill established a warrant regime for access to stored communications held by a carrier, introduced 'B-Party' interception in limited circumstances, and introduced interception based on equipment identifiers. Further details are set out in Section 10.

### *Amendments to Acts Dealing with Terrorism Offences*

In November 2005 the *Anti-terrorism (no.1) Act 2005* was passed, which clarified that when proving someone is intending to commit a terrorist act, it is not necessary for the prosecution to identify an intention to commit a specific act.

In December 2005 the *Anti-terrorism (no.2) Act 2005* was passed, which made a number of amendments to ASIO's powers and those of the police to enhance the existing framework.

### *ASIO-related Amendments*

The *Anti-terrorism Act (no.2)* amendments enhanced ASIO's special powers warrant regime by:

- clarifying the scope of computer access warrants;
- extending the time period for the validity of search warrants and inspection of postal and delivery service warrants, and extending the equivalent periods for the purpose of foreign intelligence gathering warrants;
- providing greater access to aircraft and ship information; strengthening the offence for providing false and misleading information under a warrant for questioning;
- allowing for the removal and retention (for a reasonable time unless return would be prejudicial to security) of material found during the execution of a search warrant; and
- extending computer access warrants to allow entry on premises.

### *Police-related Amendments*

- *Control Orders*: the *Anti-terrorism (no.2) Act 2005* inserted a new regime to allow the AFP, with the consent of the Attorney-General, to seek from a court control orders (for up to 12 months) on people who pose a terrorist risk to the community or who have trained with a listed terrorist organisation.
- *Preventative Detention*: the new regime permits the AFP to detain a person for up to 48 hours in order to prevent an imminent terrorist act occurring or to preserve evidence of, or relating to, a recent terrorist act.

## UNCLASSIFIED

- *Advocating a terrorist act*: an organisation can be listed as a terrorist organisation under the *Criminal Code Act 1995* if the 'organisation is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act'. To provide a more comprehensive basis for the listing of organisations, the definition of a terrorist organisation under the Criminal Code has been amended to include advocating terrorist acts. 'Advocating' is defined in a way which captures statements in support of previous activity as well as any prospective activity.
- *Stop, Question and Search Powers*: the powers of the AFP to stop, question and search have been extended where there are reasonable grounds that a person might have just committed, might be committing or might be about to commit a terrorism offence in a Commonwealth place.

### *Amendments to Terrorist Financing Offences*

The amendments strengthen the existing offences by ensuring that they cover the full range of conduct that a person could engage in for the purposes of financing terrorist activity.

The amendments extend the existing Commonwealth offences dealing with receiving funds from, or making funds available to, a terrorist organisation, to also cover the collection of funds for, or on behalf of, a terrorist organisation.

## PREVIOUS LEGISLATIVE CHANGES

Following the terrorist attacks in the United States on 11 September 2001, Australia's counter-terrorism legal framework was amended:

- The *Security Legislation Amendment (Terrorism) Act 2002* was the key piece of legislation because it created a new offence of terrorism and a range of related offences. It also modernised Australia's treason offence and introduced a regime for making regulations to list organisations that have terrorist links.
- The *Suppression of the Financing of Terrorism Act 2002* is designed to prevent the movement of funds for terrorist purposes and to enhance the exchange of information about financial transaction reports with foreign countries.
- The *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* created offences relating to international terrorist activities that use explosive and lethal devices.
- The *Telecommunications Interception Legislation Amendment Act 2002* amended the *Telecommunications (Interception) Act 1979* to allow law enforcement agencies to use intercepted material when investigating a range of criminal activities, including terrorism.
- The *Border Security Legislation Amendment Act 2002* addressed the security of Australia's borders, including border surveillance, the movement of people, the movement of goods and the controls of the Australian Customs Service to monitor this activity.

## UNCLASSIFIED

- The *Criminal Code Amendment (Terrorist Organisations) Act 2004* commenced on 10 March 2004. This legislation enables the Federal Government to list terrorist organisations based on Australia's national interest and security needs, as well as the advice of Australian intelligence organisations.
- The *Anti-terrorism Act (no. 3) 2004* strengthened the powers available to security agencies and police to ensure that those suspected of serious offences or harmful conduct, including suspected terrorists, are prevented from leaving Australia on a foreign travel document. It also amended the forensic procedure provisions in the *Crimes Act 1914* to facilitate effective disaster victim identification in the event that a disaster causing mass casualties were to occur within Australia.
- The *National Security Information (Criminal and Civil Proceedings) Act 2005* provided greater protection in criminal and civil proceedings for information that may damage national security if publicly disclosed.
  - Among other measures, it enables the Attorney-General to issue a certificate to allow documents to be used in a summarised or redacted form.
  - Additionally, it allows parties to enter into an arrangement to agree to orders for the protection of witnesses. These measures retain the essence of sensitive information without prejudicing Australia's national security.
- The *Surveillance Devices Act 2004* updated and modernised the surveillance device powers of the Commonwealth. Surveillance devices are data surveillance devices, listening devices, optical surveillance devices and tracking devices.
  - The Act aids law enforcement by both allowing a broader range of devices to be used and making warrants available for a wider range of offences.
  - It also enables senior law enforcement officers to authorise the use of surveillance devices in emergency circumstances.
- The *Australian Security Intelligence Organisation Amendment Act 2004* amended the ASIO Act to expand and clarify the ability of ASIO to furnish security assessments.
  - It ensured that ASIO can provide security assessments as part of its role in the national licensing regime for regulating ammonium nitrate.
  - The amendments are also intended to cover, to the extent that is possible, issues that may arise in the future, including ASIO's ability to furnish security assessments in relation to other hazardous materials.

## 6 Intelligence Capabilities: Collection

---

### OVERVIEW

ASIO has offices in all Australian States as well as the Northern Territory and the Australian Capital Territory. The State and Territory offices are engaged in the collection of intelligence through investigations and operations related to counter-terrorism, other politically motivated violence and counter-proliferation. This information is collected through human intelligence work, liaison with other agencies and the use of special powers (warrant) operations.

ASIO's collection resources have been in a growth phase since 2001, in particular with increased resources allocated following the Taylor Review in recognition of the challenges faced through the threat of terrorism. All areas are growing, although the bulk of the growth is still to occur, particularly in 2007–08.

Overall, the legislative changes outlined in Section 5 have increased ASIO's operational flexibility and capability to collect information in a challenging operational environment.

This portion of the Submission deals with the impact of increased resources and recent legislative changes in the context of ASIO's intelligence collection-related roles and responsibilities. It does not revisit matters previously the subject of the Review of ASIO's Questioning and Detention Powers by the former Parliamentary Joint Committee on ASIO, ASIS and DSD.

### RECENT DEVELOPMENTS/TRENDS

#### *The Role of ASIO's Collection Division*

ASIO's Collection Division is responsible for the collection of intelligence through the conduct of operations and investigations in pursuit of identified intelligence requirements and priorities. Its key focus is on terrorism and other politically motivated violence. Investigations of espionage and foreign interference matters are handled within the new Counter-Espionage and Interference Division.

Investigations are directed at individuals and groups whose activities, backgrounds and associations are assessed to be relevant to security and presenting a sufficient threat to warrant investigation by ASIO.

Techniques used by ASIO involve a range of overt and covert information collection methods and vary from overt interviews to intrusive warrant operations approved by the Attorney-General.

The special powers or warrant capabilities include:

- telecommunication interception;
- computer access;

## UNCLASSIFIED

- overt or covert entry and search of premises, vehicles and baggage;
- interception of postal and delivery service articles;
- the use of listening and tracking devices; and
- the application of ASIO questioning and detention powers with the consent of the Attorney-General and approved by issuing authorities.

ASIO also collects human intelligence from people who are willing to provide information on a confidential basis about individuals and groups of security interest. Declared ASIO interviews with members of the public and individuals of interest are also used to assist with investigations. ASIO surveillance teams also report on people of security interest. In addition to information obtained through covert means extensive use is made of open source information.

External liaison is also a significant component of intelligence collection. ASIO liaises with a broad range of agencies at the Commonwealth, State/Territory, Local Government and private/corporate level.

### *Resourcing*

In January 2006 the Collection Division was restructured to comprise three geographically defined branches. A fourth Branch – Collection Resource Coordination was established to provide for more flexible and effective national coordination of specialised resources.

- The restructure of the Collection Division has increased the number of ASIO senior managers and allowed for a closer focus by senior staff on complex operational and organisational matters.

### *Staff*

The security environment is complex, volatile and demanding and meeting the challenge of balancing the urgency, complexity and volume of information is resource intensive.

While in the first years of growth arising from the Taylor Review, additional resources have been allocated to the intelligence collection function, greater emphasis has been placed on building the enabling functions for the Organisation to support the growth (for example, staff in areas such as IT, recruitment, training and facilities management).

However, in 2007–08 a greater percentage of the new staff will be deployed to State and Territory Offices in accordance with identified intelligence requirements and priorities. Incremental increases to staffing numbers will see the Collection Division fully resourced by 2010–11.

Aside from the growth arising from the Taylor Review, events such as the Melbourne 2006 Commonwealth Games have seen extra resources allocated to the intelligence collection function for a limited period to increase ASIO's capability to provide event-related security intelligence. Events of national significance like these require increased levels of operational activity in order to ensure timely and accurate advice. This will continue as Australia hosts other international events.

## UNCLASSIFIED

Additional resources have increased the flexibility to allow for the temporary redeployment of ASIO officers.

### *Specialised Training*

Training of intelligence collection officers is time-intensive, with the initial one-year traineeship featuring formal courses and attachments and rotations to different areas of the Organisation. The additional skills required of intelligence collection staff are highly specialised and not readily replicated outside the intelligence community. Following the initial traineeship there is a requirement for ongoing on-the-job and formal training through more advanced or specialised courses. As there is no ready-made recruitment pool, it takes several years to recruit and train staff to be effective in the role of intelligence collection.

With the changing nature of the security environment ASIO needs to adapt and change its training from time to time to suit the situation and evolving policy and procedures.

While relevant language skills can add to the repertoire of skills and capabilities of ASIO's Intelligence Officers, of greater importance is the need for Intelligence Officers involved in collection work to be culturally aware and sensitive, understand the parameters of their role, and to have strong analytical and interpersonal and communication skills. ASIO places an emphasis on Intelligence Officers acquiring a thorough appreciation of different cultures and to that end ASIO officers undertake a range of courses which provide opportunities to obtain a more detailed understanding of Islam, extremism, and international and cultural issues. Training in Australia is delivered by external providers who are recognised as experts in their fields.

Recently, training courses have been developed to assist ASIO officers in dealing with the increased use of ASIO information in court proceedings.

### *Facilities*

The largest State and Territory offices are located in the major population centres. The requirement to house an expanding workforce has brought forward a program of works to relocate and/or upgrade the facilities in all State and Territory offices (see Section 18).

The re-opening of a permanent office in Hobart, made possible through the injection of additional funding, was not announced publicly at the time but is a welcome development.

The covert collection of intelligence and the security of ASIO operations requires anonymity. As a result, the locations of ASIO's State and Territory offices are not declared publicly and ASIO officers' identities are protected.

### *Foreign Language Capabilities*

ASIO's foreign language capabilities are spread across a number of job families, including specialised Linguists and other staff (such as Intelligence Officers) who have foreign language skills as part of a wider skill set used in investigative or liaison

## UNCLASSIFIED

work. ASIO's Linguist cadre is employed to undertake translation and interpreting work.

ASIO has increased its foreign language capability in terms of both the size of the Linguist cadre and the range of languages that they cover. ASIO's requirement for a wide-ranging foreign language capability means that the demand for people with highly developed foreign language skills – as well as being highly literate in English – and who meet ASIO's stringent entry requirements, is unlikely to abate for some time.

Recruitment of Linguists remains a challenge.

Other ASIO officers may be recruited with existing foreign language skills or may be supported in acquiring such skills through training but their role and function is not focused primarily on these skills. They are not employed as specialised 'linguists' but their foreign language proficiency may enhance their effectiveness across a range of roles.

ASIO seeks to recruit Intelligence Officers who have foreign language abilities and provides basic language training to other Intelligence Officers as part of a wider program of developing and enhancing the skills and abilities of the Intelligence Officer cadre.

### *Legislative Impact – Special Powers*

The changing security environment since 2001 has seen an increase in ASIO's legislated powers. Many of the new powers are specifically designed to enhance ASIO's intelligence collection capabilities.

One example where legislative changes have had a direct effect on ASIO's activities is in the area of information and communication technology.

The changes to the ASIO legislation relating to special powers have enabled the Organisation to grow and adapt to a changing security environment and to undertake intelligence collection activities by utilising a wider array of tools. Nonetheless, the legislative tests that must be met in connection with the application of these special powers remain stringent and subject to rigorous oversight and accountability mechanisms.

### *Computer Access*

Computer access warrants allow ASIO to obtain information stored on a computer.

### *Entry and Search Warrant Changes - Frisk Search*

The amendment to the entry and search powers to include an ordinary frisk search has provided ASIO with the ability in certain circumstances and within strict guidelines to search people to obtain concealed items which may be of intelligence value.



## UNCLASSIFIED

### *Entry and Search Warrant Changes - Extension from 28 to 90 Days*

In response to individuals engaging in behaviour that is intended to circumvent ASIO's ability to detect their activities the Organisation requires greater flexibility in how it plans and conducts special powers operations. This is particularly true when executing Entry and Search Warrants. Legislative amendments in connection with Entry and Search Warrants now provide ASIO with a 90 day window within which to execute a warrant rather than a 28 day window as was the case previously. This change reduces the administrative overhead involved in renewing warrants every 28 days in circumstances where it has not been possible to execute the warrant but the requirement remains extant.

### *Questioning and Detention Warrants*

ASIO has used its questioning warrant powers prudently since their inception. It has always been understood that these are powers of last resort.

ASIO is required to report annually on its use of these powers. In 2005–06 ASIO executed 1 questioning warrant compared to 11 in 2004–05 (involving 10 people) and 3 in 2003–04.

ASIO has not used the powers of detention. Again, the highly intrusive nature of this power necessitates strict procedures for ASIO to follow when implementing this type of warrant.

With the extension of the powers for a further 10 years, the questioning and detention powers will remain a valuable tool. ASIO's questioning and detention powers have been the subject of extensive debate and review by the Parliament.

### *External Liaison and Engagement*

ASIO has well-developed and long-standing relationships with a range of agencies, including the Australian Federal Police (AFP), and State and Territory police services. Changes in the security environment, as well as changes in legislation (particularly anti-terrorist legislation) has caused these relationships to be further refined and they continue to be integral to ASIO's whole-of-government approach toward protecting Australia from security threats.

- National Counter-Terrorism Committee arrangements provide an agreed model for cooperation between ASIO, the AFP, State and Territory police and other law enforcement bodies including the Australian Crime Commission and NSW Crime Commission.
- ASIO has the lead role in the provision of security intelligence advice and assessment based on information it has obtained directly and from intelligence and law enforcement agencies.
- Where intelligence investigations identify criminality and the potential for arrest and prosecution, the model calls for early police involvement in evidence collection activities.
- These arrangements aim to maximise the opportunity for law enforcement agencies to collect evidence. Liaison on a broad range of investigations takes place at the working, middle management and senior management levels on a regular

## UNCLASSIFIED

basis. Weekly or fortnightly working-level meetings focus on the day-to-day management of cases while management meetings determine the strategic direction of operations and ensure commonality of purpose.

A consequence of this cooperative arrangement has been the ability to effectively deploy significant resources for investigations and, importantly, increased interoperability in key areas, such as surveillance, foreign language capability, collection officers and analysts. ASIO's increased capabilities allow a further strengthening of these relationships. Cooperation also provides a force multiplier effect which has played an important role in joint investigations.

### *Airport and Maritime Security Liaison Officers.*

ASIO now has a greater presence at Australia's air and maritime ports. ASIO's border security capability has been boosted with Maritime Liaison Officers at seaports and Airport Liaison Officers in place at international airports. ASIO's increased presence at major air and seaports reflects ASIO's commitment to strengthening Australia's border security regime, and has enhanced interoperability with the Australian Customs Service, the Department of Immigration and Citizenship as well as effective liaison with the new Airport Policing and Security units.

ASIO's air and maritime liaison officers also perform a critical linking role with air and maritime carriers. The airport liaison officers are responsible for developing and maintaining liaison with airlines and other commercial enterprises based at the airport. These strategic partnerships are an essential plank in our border security regime.

The recruitment of additional staff to work at the airports has made it necessary to upgrade accommodation at those sites.

### *Accountability*

ASIO regularly develops and reviews policies and procedures for officers involved in intelligence collection work. Strict accountability mechanisms are employed in all ASIO operational policy documents to ensure that where more intrusive methods are required they have been authorised at an appropriately senior level.

ASIO's policies and procedures provide clear guidelines on how ASIO officers should conduct themselves in the execution of these powers and against which they can be held accountable.

## FUTURE FOCUS

Growth in any organisation brings in new staff who need to be trained and given the opportunity to develop the specialised skills required for the tasks they must perform. While greater numbers of staff in the longer term will alleviate some of the workload pressures on existing staff, in the shorter term experienced staff must play a role in mentoring and developing newer members of staff. In ASIO's case, they must carry this responsibility while continuing to operate in a fast-paced and demanding operational environment.

## UNCLASSIFIED

In the context of ASIO's intelligence collection work, the need to maintain a high level of operational effectiveness and responsiveness in the face of a complex threat environment, the increasing sophistication of targets and the impact of technological change, means the integration and development of new staff must be managed thoughtfully. That is why ASIO seeks to balance the development of human and technological intelligence collection skills, the expansion of liaison relationships, and continued investment in training in all aspects of intelligence collection.

## 7 Intelligence Capabilities: Technical Capabilities

---

### OVERVIEW

Prior to 2003, ASIO's technical capabilities were managed within the Collection Division. As the Organisation has grown, the demands on ASIO's technical resources and technical capabilities have increased. Consequently ASIO has implemented new management structures and arrangements aligned to the requirements of a larger organisation.

### RECENT DEVELOPMENTS/TRENDS

Technical Capabilities Division focuses on technical and surveillance operations against groups or individuals engaged or reasonably expected to be engaged in activities prejudicial to security. The Division also is responsible for the development and maintenance of a broad range of capabilities to ensure the effective delivery of its operational requirements. It works closely with other divisions to provide technical and surveillance capabilities in support of investigations.

The Division comprises three main components, Technical Operations, Surveillance and Telecommunications Interception. In common with other areas of the Organisation, Technical Capabilities Division is going through a period of expansion driven in part by:

- the increased demand for special powers operations;
- the increased complexity of technology; and
- the more hostile operating environment.

## 8 Intelligence Capabilities: Technical Operations

---

### OVERVIEW

Technical Operations has a broad range of responsibilities. In line with tasking from Collection and Counter-Espionage and Interference Divisions the area is responsible for the technical aspects of ASIO's special powers operations involving: the installation and maintenance of listening devices; tracking devices; interception of mail; computer access; and covert and overt entry and searches. It also manages the Organisation's covert radio communication systems and the execution of operational photographic activity.

The Technical Operations area also includes a capabilities development component which oversees the Organisation's operational engineering and software development programs.

### RECENT DEVELOPMENTS/TRENDS

In recent years most of ASIO's technical operational work has been devoted to counter-terrorism investigations.

Demand for technical operational support continues to rise and, in common with other areas of the Organisation, the area is going through a period of expansion.

#### *Technical Support Unit*

Under the National Counter-Terrorism Plan, ASIO also has responsibility for the management and maintenance of the Technical Support Unit (TSU). The TSU comprises technical officers with a broad range of technical operations skills. The officers are not deployed with the TSU permanently, but are drawn as required from other areas of the Organisation. The TSU provides unique and specialised technical capabilities to support the police and the Australian Defence Forces (ADF) in resolving a terrorist incident. The TSU was upgraded in 2005–06 to provide a more responsive and flexible capability.

### FUTURE FOCUS

Continued emphasis will be placed on maintaining and improving technical capabilities. Attracting, recruiting, training and retaining technical specialists will remain a major focus.

## 9 Intelligence Capabilities: Surveillance

---

### OVERVIEW

ASIO maintains a specialist surveillance capability to support the collection of intelligence. The information collected by Surveillance Officers supports the collection, analysis and assessment processes within the Organisation.

Surveillance Officer recruits graduate from an intensive six-month training program run by the Organisation. At this time officers are equipped with specialist surveillance skills and supporting skills such as photography and defensive driving. During their surveillance career, officers regularly receive refresher training and must maintain a high level of skill to remain in the unit.

### RECENT DEVELOPMENTS/TRENDS

Surveillance now operates in a substantially more complex environment against a diverse range of subjects.

The nature of the terrorist threat has seen an increase in the likelihood that traditional surveillance reporting will be required as evidence, or Surveillance Officers as witnesses, in court proceedings. This has necessitated a modification to reporting processes, standards and formats and a need to provide training in evidentiary procedures.

ASIO's surveillance capability will experience significant growth over the next four years. To ensure staff acquire the correct skills and are acculturated, ASIO provides a recruit training program that covers all aspects of tradecraft within a strong values-based framework. The program concludes with staff placed in a mentor/buddy arrangement with more experienced officers.

ASIO's surveillance capability has been growing since 2003 and is expected to reach full capacity in 2009. This will result in an ongoing challenge to balance operational requirements with the training and development of new staff.

Surveillance skills are mainly acquired through experience. As the proportion of new Surveillance Officers grows relative to those with more experience, the importance of sound training and strategic partnerships with relevant agencies will grow.

### FUTURE FOCUS

ASIO's surveillance capability is dependant on the quality of the people engaged in this activity. The nature of surveillance work can be quite demanding on the people involved who are required to manage the effects of shiftwork, an itinerant work style, and day-to-day isolation from their colleagues in the rest of the Organisation.

## UNCLASSIFIED

Continuing the training framework will be important to raising skill levels quickly and closing the experience gap. Included in capability development is leveraging technology to provide better logistics support and developing an operational planning capability.

# 10 Intelligence Capabilities: Telecommunications Interception

---

## OVERVIEW

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

ASIO's telecommunications interception capabilities consist of two main aspects:

- Telecommunications interception operations under warrant and investigations involving the use of the telecommunications system including obtaining communications traffic and subscriber data under section 283 of the *Telecommunications Act 1997*.
- Acquiring and maintaining telecommunications interception capabilities in Carriers/Carriage Service Providers (C/CSPs) networks. The Attorney-General has assigned ASIO a 'lead house' role in terms of acquiring telecommunications interception capabilities on behalf of law enforcement agencies, as well as for its own needs.

## RECENT DEVELOPMENTS

### *Industry and Technological Environment*

The telecommunications industry has experienced considerable growth since deregulation in the early 1990s. There are now approximately 170 licensed telecommunications carriers active in Australia, as well as some 1,600 carriage service providers (CSPs), including approximately 700 internet service providers (ISPs). The industry is highly competitive and operating margins are low, especially in the Internet industry.

### *Growth*

As a consequence of the Taylor Review, ASIO's telecommunications capability is increasing through the injection of additional resources.

### *Impact of Legislative Change*

In the past two years there have been significant legislative developments impacting on telecommunications interception. Some of these have been part of the Government's counter-terrorism legislative reform agenda and others have been part of ongoing programs to amend the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979* to deal with specific issues. Other legislative amendments have flowed from recommendations of the August 2005 *Report of the Review of the Regulation of Access to Communications* (the Blunn Review) and the June 2003 *Review of Certain Provisions of the Telecommunications (Interception) Act 1979* (the Sherman Review).



## UNCLASSIFIED

The *Telecommunications (Interception) Amendment Act 2004* received Royal Assent on 27 April 2004 and entered into force on 28 April 2004. Amendments included:

- permitting ASIO to record calls to its public lines without any additional authorisation; and
- removing the requirement for ASIO to notify the telecommunications carrier where a warrant has been issued for the interception of telecommunications service operated by the carrier and the assistance of the carrier is not required in order to execute the warrant.

The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* received Royal Assent on 14 December 2004 and entered into force on 15 December 2004. This Act amended the *Telecommunications (Interception) Act* to exclude the interception of ‘stored communications’ from the prohibition against interception, with the result that the prohibition was limited to ‘real-time’ interception of communications over a telecommunications system.

The *Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005* received Royal Assent on 6 July 2005, with most provisions commencing on that day. While not having any direct effect on ASIO as an intercepting agency, this Act amended the *Telecommunications (Interception) Act* to:

- allow the interception without a warrant of communications to and from certain telecommunications services used by the public to seek assistance in emergencies;
- insert a limited exception to the general prohibition against interception regarding the investigatory duties of the Australian Communications and Media Authority (ACMA) pursuant to the *Radiocommunications Act 1992*;
- extend the availability of telecommunications interception warrants to include accessories after the fact;
- implement those recommendations of the Sherman Review accepted by the Government and requiring legislative amendment – including the introduction of ‘named person warrants’; and
- amend the definition of employee of a carrier in recognition of changed corporate structures and the use of contractors.

The *Communications Legislation Amendment Act (No.1) 2004* received Royal Assent on 20 April 2004 and entered into force on 21 April 2004. This Act made a number of amendments to the *Telecommunications Act 1997* relevant to the Australian telecommunications regime. These amendments included:

- requiring the ACMA to consult with the Agency Co-ordinator before granting a carrier licence under the *Telecommunications Act 1997*, and permitting the Attorney-General, after consultation with the Prime Minister and the Minister for Communications, Information Technology and the Arts, to direct the ACMA to refuse to grant a carrier licence to a particular applicant on national security grounds;
- permitting the Attorney-General, after consultation with the Prime Minister and the Minister for Communications, Information Technology and the Arts, to direct a C/CSP not to use or supply, or to cease using or supplying, a carriage service where such use or supply is or would be prejudicial to national security;

## UNCLASSIFIED

- requiring the Agency Co-ordinator to deal with applications for exemptions from interception obligations within 60 days, with a failure to do so resulting in the exemption being deemed to be unconditionally granted until the Agency Co-ordinator makes a decision on the application; and
- requiring interception capability plans to be lodged by 1 July, rather than 1 January each year, and requiring these plans to be signed by the Chief Executive Officer of the carrier and to contain:
  - a statement of policies of the carrier in relation to interception generally;
  - strategies for compliance with its interception obligations in relation to each service that it offers; and
  - a statement of compliance with its legal obligations.

*The Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act 2004* received Royal Assent on 31 August 2004 and the relevant provisions entered into force on 1 March 2005. This Act repealed the telecommunications offences in Part VIIb of the *Crimes Act 1914* and inserted updated telecommunications offences into Part 10.6 of the Criminal Code, including those relating to IMEI modification, SIM cloning, telephone threats and hoaxes, and interference with telecommunications facilities.

The *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Bill 2005* extended the operation of the stored communications regime for a further six months beyond its expiry date of 14 December 2005.

The *Telecommunications (Interception) Amendment Act 2006* amended the *Telecommunications (Interception) Act* to:

- introduce a new warrant regime for access by law enforcement agencies to stored communications under warrant. (ASIO continues to have access to stored communications under a telecommunications interception warrant or a computer access warrant (section 25A of the ASIO Act));
- introduce 'B-Party' interception in limited and controlled circumstances; and
- introduce 'equipment-based interception' (including interception based on GSM handset identifiers (IMEI)).

In addition, the name of the *Telecommunications (Interception) Act 1979* was changed to the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

A Bill for further amendments to this Act, to implement other recommendations of the Blunn Review including transfer of elements of Parts 13, 14 and 15 of the *Telecommunications Act 1997* to the TIA Act, is anticipated to be introduced during 2007.

From the ASIO perspective, all of these legislative amendments have been positive.

# 11 Intelligence Capabilities: Intelligence Analysis

---

## OVERVIEW

The nine-division structure includes two divisions focused on intelligence analysis and provides a management structure which separates investigative analysis and advice from strategic intelligence analysis, including threat assessment work. While the two divisions work together closely and with high levels of visibility across their respective work programs and priorities, the current structure provides for greater specialisation across these important areas.

The primary focus of ASIO's intelligence analysis effort is on counter-terrorism investigations, although as additional resources have come on line it has been possible to boost the effort against other threats to security. The volume of information flowing to ASIO has increased exponentially since 2001. This has presented a number of challenges, not the least of which is the need to have the capability to review quickly all information and accord it a priority for action.

In addition, increased ASIO support for counter-terrorism prosecutions has required that staff be allocated specifically to this function (see Section 12). This separation of duties has freed Intelligence Analysts to focus on investigations.

With the commencement of 24/7 operations by the National Threat Assessment Centre (NTAC) in May 2004, ASIO has had an enhanced capability to disseminate advice rapidly in response to developments in the security environment in Australia and internationally. The NTAC is housed within ASIO and managed as part of the Strategic Intelligence and Liaison Division. The NTAC includes integrated officers from the Australian Federal Police, the Australian Secret Intelligence Service, the Department of Foreign Affairs and Trade, the Defence Intelligence Organisation, the Department of Transport and Regional Services, the Defence Signals Directorate and the Office of National Assessments. All the integrated officers have full connectivity back to their parent agency's systems.

## RECENT DEVELOPMENTS/TRENDS

### *Boost to Counter-Proliferation*

Since 2001, the number of ASIO officers devoted to counter-proliferation work has grown.

An important role for ASIO's counter-proliferation efforts is to provide chemical, biological, radiological, nuclear and explosives terrorism advice to government to guide policy development and national preparedness, and assist in identifying and addressing capability gaps that require research and development.

# UNCLASSIFIED

## *National Security Hotline (NSH)*

The introduction of the National Security Hotline (NSH) in December 2002 marked a significant increase in the volume of new leads coming to ASIO.

ASIO is responsible for the evaluation and investigation of all new leads referred to it.

**Table 11.1: Number of NSH Calls**

	<i>Dec 2002–03</i>	<i>2003–04</i>	<i>2004–05</i>	<i>2005–06</i>	<i>1 July 06– present</i>	<i>Total</i>
<i>Referred to ASIO</i>	11,000	7,000	7,000	17,000	3,400	<b>45,400</b>
<i>Require further Investigation</i>	1,500	1,500	2,500	6,500	1,500	<b>13,500</b>

Since its inception, the NSH has significantly and progressively increased the volume of lead information referred to ASIO. This increase likely reflects an increased public awareness of security issues following several terrorist incidents worldwide since 2001, compounded by the Australian Government's active media campaign promoting the Hotline. Security-related events in Australia and overseas also significantly increase the number of calls to the NSH.

For example, spikes were seen following the Australian Embassy bombing in Jakarta in 2004, the London transport attacks in 2005, and the terrorism-related arrests in Australia in late 2005

## *Support for Special Events*

The security implications, complexity and risks associated with hosting or participating in large-scale or high-profile events has increased significantly since 11 September 2001. The changed security environment and the increased profile of Australian interests and many other countries' interests as terrorist targets means that preparing for special events of national significance requires thorough and considered planning and coordination with concomitant resource deployment.

ASIO is responsible for the collection, analysis and dissemination of security-related advice and assessments in support of Police, Commonwealth agencies, or overseas authorities involved in securing major events.

## *Development of Complex Analytical Capabilities*

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

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

- better collate, search and sort data;
- access and analyse material in a variety of formats; and

## UNCLASSIFIED

- visualise complex information sets.

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

Progress is being made on better ways of collating, searching and sorting data, as well as improving and extending these capabilities across ASIO's information holdings.

## 12 Intelligence Capabilities: Support for Litigation

---

### OVERVIEW

Following the introduction of legislation which criminalised a range of activities related to terrorism ASIO's involvement in litigation increased. As a result of the increased workload, on 1 July 2006 a new Executive and Legal Division was created to meet the increased requirement for in-house legal services in connection with both litigation and advice. In addition, a Counter-Terrorism Litigation Advice Branch was created within the Investigative Analysis and Advice Division. Resources have also been located in the Collection Division directed at supporting the counter-terrorism litigation advice function.

### RECENT DEVELOPMENTS/TRENDS

#### *Counter-Terrorism Litigation Advice*

The counter-terrorism litigation advice capability is directed at:

- supporting counter-terrorism legal proceedings;
- protecting ASIO's methods, capabilities, sources, intelligence holdings and people in legal proceedings;
- contributing to ASIO's policies and procedures; and
- contributing to the training and development of staff who require a sound understanding of this aspect of ASIO's work.

Counter-terrorism litigation advice can be provided either actively or reactively.

- ASIO may offer to support a prosecution by providing intelligence for use as evidence which involves: identifying what ASIO holds; determining its relevance, context and sensitivities; determining whether it may or may not be used in a proceeding; and, if it can be used, considering the protective framework for the provision of ASIO information and any witnesses.
- ASIO may respond to various legal demands such as subpoenas or provide support to ASIO witnesses in court and manage national security issues as they arise in proceedings.

Counter-terrorism litigation advice can also take on an advisory role in relation to matters involving persons who are the subject of an adverse or qualified ASIO security assessment.

## 13 Intelligence Capabilities: Counter-Espionage and Foreign Interference

---

### OVERVIEW

ASIO's work in countering espionage and acts of foreign interference is conducted within a separate division from other security intelligence investigations. The establishment on 1 July 2006 of the Counter-Espionage and Interference Division within ASIO's new nine-division structure put in place arrangements tailored to the particular requirements of this aspect of security intelligence investigations.

That responsibility relates to espionage and foreign interference activity conducted in Australia and activity directed against Australian interests here and overseas.

### RECENT DEVELOPMENTS/TRENDS

Espionage is not defined in the ASIO Act but criminal offences relating to espionage and similar activities are set out in Division 91 of the *Criminal Code Act 1995* (Cth) (the Code). These offences were enacted in 2002 in the *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth).

Section 91 of the Code provides that a person commits an offence if he or she communicates, or makes available, information concerning the Commonwealth's security or defence or information concerning the security or defence of another country which has been acquired from the Commonwealth. The action must have been done with the intent of prejudicing the Commonwealth's security or defence and result in, or be likely to result in, the information being communicated or being made available to another country or foreign organisation (or a person acting on behalf of the other country or foreign organisation).

It is also an offence if a person communicates or makes available such information without lawful authority and with the intention of giving an advantage to another country's security or defence. Section 91 also provides that it is an offence for a person to make, obtain or copy a record of such information if the person does so with the intention that it will or may be delivered to another country or foreign organisation (or a person acting on behalf of the country or foreign organisation) and with intent to prejudice the Commonwealth's security or defence.

Section 91 further provides that it is an offence for a person to make, obtain or copy a record of such information without lawful authority and with the intention that it will or may be delivered to another country or foreign organisation (or a person acting on behalf of the other country or foreign organisation), and with the intention of giving an advantage to another country's security or defence.

Some offences relating to official secrets and unlawful soundings that are relevant to some espionage activity are also to be found in Part VII of the *Crimes Act 1914* (the Crimes Act).

## UNCLASSIFIED

Prosecutions for espionage and related offences have been uncommon in Australia.

Acts of foreign interference are defined in section 4 of the ASIO Act to mean:

*Activities relating to Australia that are carried on by or on behalf of, are directed or subsidised by or are undertaken in active collaboration with, a foreign power, being activities that:*

- (a) *are clandestine and deceptive and:
  - (i) *are carried on for intelligence purposes;*
  - (ii) *are carried on for the purpose of affecting political or governmental processes; or*
  - (iii) *are otherwise detrimental to the interests of Australia; or**
- (b) *involve a threat to any person.*

The term “foreign power” is defined in section 4 of the ASIO Act to mean:

- (a) *a foreign government;*
- (b) *an entity that is directed or controlled by a foreign government or governments; or*
- (c) *a foreign political organisation.*

ASIO also is responsible for collecting foreign intelligence in Australia on behalf of the Minister for Foreign Affairs and/or the Minister for Defence in accordance with section 17(1)(e) of the ASIO Act. Foreign intelligence is defined in section 4 of the ASIO Act to mean:

*‘intelligence relating to the capabilities, intentions or activities of a foreign power.’*

### *Investigations*

In broad terms, ASIO’s investigations in this area are carried out using the same range of capabilities, techniques and approaches as are used in ASIO’s other security intelligence investigations (see Section 6). Counter-espionage and foreign interference investigations can include the use of the same array of special powers as are available for other security intelligence investigations, with the exception of questioning and detention powers which are applicable only to the investigation of terrorism offences.

Counter-espionage and foreign interference investigations are inherently sensitive for a number of reasons, including:

- they go to activities in Australia of a range of foreign governments and other foreign powers and to activities that they direct against Australian interests outside Australia;
- they frequently involve the activities of capable foreign intelligence services tasked to collect intelligence on Australia and its allies by both human and technical means and with well-developed counter-intelligence arms tasked to discover and counter Australian activity directed against them;
- damaging espionage operations usually involve large investments over long periods by the foreign intelligence services who run them and require comparable long-term efforts by ASIO to counter them; and



*Resourcing*

Additional resources have been directed to this area with further growth planned through to 2010–11.

*Staff*

The establishment of a division dedicated to counter-espionage, foreign interference and foreign intelligence collection has permitted a closer and more intensive focus by senior managers on these particular functions. The additional staffing will allow ASIO to broaden the scope and reach of its counter-espionage and foreign interference investigations and to expand its outreach activity to government departments and agencies.

It has been important to stage the growth of resources in this area carefully so as to maintain a balance between experienced and new staff and to allow for effective mentoring and training.

*Training*

ASIO's Intelligence Officer training has necessarily shifted to focus more intensively on aspects relevant to ASIO's counter-terrorism work, given the high proportion of ASIO's overall effort directed to this end and the need for graduating officers to be operationally effective as quickly as possible. Intelligence Officers engaged in counter-espionage and foreign interference work undergo the same basic training as their counterparts who are engaged in other security intelligence work.

Skills in particular foreign languages are valuable in some circumstances, though they are secondary to the essential qualities of the operational officer – including subject knowledge, cultural sensitivity, self-awareness, and the ability to read others' verbal and non-verbal communication, to respond appropriately and flexibly, and to instil confidence and trust in people who are prepared to contemplate providing assistance and information to ASIO, often for a prolonged period and at some risk to their personal situation.

*Legislative impact – Special Powers*

Many of the technical and practical challenges addressed through changes to legislation are as applicable to this aspect of ASIO's work as they are to other security intelligence investigations, noting that the questioning and detention powers can be used only in connection with counter-terrorism investigations.

*Accountability*

This aspect of ASIO's activities is governed by the same accountability arrangements and policy and procedural arrangements as apply to the rest of the Organisation. There is broad consistency of operational policy and practice across the Organisation. The Inspector-General of Intelligence and Security reviews activities in this area in the same way as he does elsewhere in the Organisation.

UNCLASSIFIED

## FUTURE FOCUS

Training of new staff will remain a particular focus.

UNCLASSIFIED

## 14 Human Resource Management: Recruitment

---

### OVERVIEW

Recruitment targets to support ASIO's growth are ambitious – an average of 170 (net) per year over the next four years – particularly noting specific skill-sets required for ASIO recruits, the requirement for Top Secret Positive Vetting clearance and the competitiveness of the labour market. Nonetheless, ASIO achieved net staff growth of 155 in 2005–06 and is confident of meeting the annual net growth of 170 in 2006–07 that has been endorsed by Government.

Challenges remain in meeting targets for some specific job families, including Intelligence Analysts and specialist technical areas. Further work is being undertaken to improve the attraction strategies including enhanced and targeted advertising; development of an organisational 'brand'; and possible financial inducements to join the Organisation. Recruitment processes also continue to be refined and improved – in particular, an ASIO recruitment internet tool which is scheduled to go online in March 2007 is expected substantially to improve the efficiency with which individual applications are received and processed.

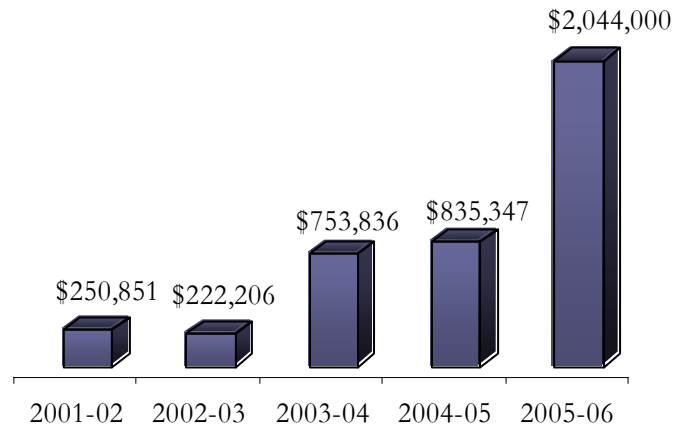
### RECENT DEVELOPMENTS/TRENDS

Prioritised 'job family' campaigns were extended to most ASIO vacancies in 2006–07. This new approach has minimised the number of separate recruitment processes and allowed us to streamline selection processes. It also has enabled more effective forward planning to ensure availability of necessary resources.

ASIO continued to utilise various recruitment and advertising agencies to develop inventive advertising campaigns for a number of job families. These initiatives drew upon commissioned market research results and were aimed at appealing to those who may not normally consider a career with ASIO. Innovative campaigns for Intelligence Officers and Intelligence Analysts attracted 960 and 350 applications respectively (recruitment advertising costs and examples of advertisements are Chart 14.1 and Figures 14.2 and 14.3 respectively).

# UNCLASSIFIED

*Chart 14.1: Recruitment Advertising Costs*



The security clearance process remains resource intensive, but necessary to ensure the suitability of applicants to work in a sensitive environment. The process takes between three and nine months to complete – delays are often due to the time taken for applicants to acquire and provide necessary documentation and availability to engage in the vetting process. ASIO reviewed and updated several key vetting forms to assist applicants complete them in a timely manner.

Staff numbers in the recruitment area have been increased to enable the processing of new applicants and to move them expeditiously through security vetting processes, without compromising standards.

## FUTURE FOCUS

The development and introduction of the Internet online recruitment tool in the first quarter of 2007 will provide greater efficiencies in our recruitment processes. This process will be phased in and result in a more streamlined process, accurate and timely reporting and ease of access to historical recruitment data. Applicants will find the system easy to use and professional and they will receive timely and regular updates on their progress (where appropriate).

ASIO understands the importance of having a strong and professional presence on the Internet and our website reflects our need to attract quality and applicants. Our website will continue to focus on promoting the Organisation as offering a flexible and challenging career, with ongoing training opportunities and the chance to make a meaningful contribution towards Australia's security.

Figure 14.2: Example of an advertisement for Intelligence Officers


# To an Intelligence Officer, this could be a threat, not a receipt.



Intelligence is the key to protecting Australia. That's why ASIO is looking for intelligent people who notice the kind of information that others miss. If you're capable of both left-brain and right-brain thinking the role of an Intelligence Officer will test you like no other. To apply visit [www.asio.gov.au/employment/to](http://www.asio.gov.au/employment/to) by Monday November 6th.



*Figure 14.3: Example of an advertisement for Intelligence Analysts*



**ANOTHER SUCCESSFUL DAY AT THE OFFICE.**



**ASIO Intelligence Analysts**  
**\$54,026 - \$74,717 plus super**

ASIO provides vital advice and analysis to help ensure the security of special events and the people involved.

Your job as an ASIO Intelligence Analyst is to provide the security intelligence that keeps Australians safe every day of the year.

ASIO is looking for self-starters who enjoy a challenge and have high level conceptual, analytical and research skills and well developed oral and written communication skills. You will be energetic, flexible and innovative, and have a keen interest in contributing to the national security effort.

Visit [www.asio.gov.au](http://www.asio.gov.au) before **20 November** for more information and to apply.

## 15 Human Resource Management: Training

---

### OVERVIEW

The training and development of ASIO staff remains a high priority for both newly recruited staff and those who have been with the Organisation for some time.

### RECENT DEVELOPMENTS/TRENDS

As key enabling components of the Organisation, our training and development areas were allocated high recruitment priority in the early years of the growth arising from the Taylor Review.

To ensure ASIO's training and development is optimal during the years of growth ahead, in late 2006 ASIO's Audit and Evaluation Committee commissioned an external evaluation of ASIO's training and development strategies by experienced consultants with the overall purpose of assessing the strategic direction of training and development in ASIO. Specifically, the review sought to:

- assess ASIO's non-intelligence training and development against Australian Public Service frameworks and standards;
- examine the appropriateness of the content of non-intelligence training programs;
- assess the return on investment from non-intelligence training and improve the Organisation's ability to measure this aspect;
- recommend improvements to the strategic approach to delivering non-intelligence training and development services to the Organisation;
- establish a validated framework to support a structured re-launch of training and development services to the Organisation, including the exploitation of human resources software; internal promotion of training and development through a comprehensive prospectus or similar reference; and refinements to the Personal Development Program process; and
- identify a system to encourage staff to retain language skills.

The findings of that evaluation currently are being compiled and, once assessed and endorsed by the Audit and Evaluation Committee, will be implemented throughout 2007.

The evaluation excluded operational intelligence training aspects which already had been the subject of separate reviews.

#### *Corporate Training Programs: Introduction to ASIO Program*

- The effective induction of staff into ASIO has taken on an enhanced importance in light of the increased tempo of recruitment and desirability to have an effective and efficient acculturation process for new staff.

## UNCLASSIFIED

### *Corporate Training Programs: Management and Leadership Skills*

A full range of leadership and management development activities continues to be offered to the leadership group and to Senior Officers.

- A new orientation program for newly appointed or promoted Senior Officers was developed and delivered in 2006. The objective of the program is to ensure that new Senior Officers have an opportunity to gain a solid understanding of their management responsibilities.

### *Corporate Training Programs: General Corporate and Administrative Training*

Training programs in administrative practices and processes were attended by 332 staff in 2006. Topics covered included project management, contract management, perceptive interviewing, selection panels, effective writing and smart reading.

Demand for IT training is anticipated to increase with the rollout of new and upgraded IT systems.

### *Corporate Training Programs: Counter-terrorism Response Training*

ASIO officers continue to support and participate in counter-terrorism training exercises.

### *Corporate Training Programs: Ethics and Accountability*

ASIO's ethics and accountability program was revamped in March 2006 and programs are now delivered monthly by a professional facilitator and SES officer (on a rotational basis). The frequency and size of courses are structured so that every ASIO officer is scheduled to attend one of the courses at least every three-years. The course is designed to ensure familiarity with: principles and ethical standards and accountability within ASIO and the Australian Public Service, ASIO's code of conduct and internal audit processes. The Inspector-General of Intelligence and Security or his representative also usually presents on the course.

### *Language Training*

ASIO continues to focus on developing and maintaining language capability across the range of ASIO's investigations and liaison functions with a number of programs and activities delivered to support this requirement. These included:

- continuation of full-time language training for several officers each year which includes an in-country component;
- support of formal studies in relevant languages through the ASIO Studies Assistance Program;
- pre-posting language training for officers selected for language designated overseas posts; and
- refinement of the methods of identifying and recording language capabilities across the Organisation.



## UNCLASSIFIED

ASIO will implement strategies to encourage the development and retention of language skills across a range of job families, in accordance with the outcomes of the external evaluation of training and development.

### *Other Training and Developmental Opportunities*

ASIO staff also have access to a range of other training and development opportunities including:

- exchanges with and secondments to overseas liaison partners;
- exchanges with and secondments to Australian Intelligence Community (AIC) agencies and Australian Government departments, including the Australian Secret Intelligence Service, the Australian Federal Police, the Office of National Assessments and the Department of the Prime Minister and Cabinet; and
- joint AIC training programs developed by the AIC training Secretariat, established as a result of Flood Report recommendations aimed at boosting co-operation and resource sharing in the AIC. ASIO provides both participants and presenters to joint AIC courses – including the AIC induction course and AIC Senior Officers' course. [C]

### *Intelligence Training*

A critical enabling function of ASIO's intelligence training is the delivery of competent and effective Intelligence Officers and Intelligence Analysts in the workplace.

Intelligence Officers undertake a 12-month traineeship during which they are required to develop and demonstrate specific competencies, predominantly in relation to ASIO collection and analysis work. The traineeship comprises a combination of formal classroom-based intelligence training, on-the-job work placements (including to Collection Offices), experience in an enabling functional area to broaden awareness of the breadth and nature of work undertaken across the Organisation, and attendance on specific courses designed to enhance critical thinking skills, cross-cultural awareness, ethics and accountability, conflict resolution, and teamwork, leadership and management skills. Post-traineeship operational training is also provided to graduates undertaking Collection roles. (See Section 6)

Intelligence Analysts also complete a structured training program designed to ensure familiarity with and competence in the range of analytical tasks performed within the Organisation.

## FUTURE FOCUS

Training for Intelligence Officers and Intelligence Analysts is consistently reviewed to ensure it is contemporary, focused and appropriate to the duties to be performed. Further adjustments to the Intelligence Officer traineeship are likely to be made in 2007.

# 16 Human Resource Management: Workplace Diversity, Retention and Complaints

## OVERVIEW

ASIO has a range of strategies and programs designed to enhance our people management capacity and capabilities. In order to ensure that the Organisation remains competitive in the employment market both in attracting and retaining highly skilled people, the senior management group continually monitors workforce planning issues such as commencements and separations, employment profiles/mixes and workplace diversity, including through quarterly statistical reporting.

## RECENT DEVELOPMENTS/TRENDS

### *Workplace Diversity*

Given the Organisation's mission and vision, ASIO requires a workforce that reflects the diversity in the broader Australian community and has implemented strategies to address this issue such as the (classified) *Workplace Diversity Program 2005-09*, the (classified) *Disability Action Plan* and ongoing monitoring and quarterly reporting of age, length of service and gender to the Corporate Executive (CE). The diversity of the Organisation's workforce is presented in Table 16.1.

**Table 16.1: Representation of Designated Groups at 31 December 2006**

Group	Total Staff <sup>1</sup>	Females	Race / Ethnicity <sup>2</sup>	Aboriginal & Torres Strait Islander	People with a disability	Available EEO Data <sup>2</sup>
SES (excl DG)	34	7	0	0	0	33
Senior Officers <sup>3</sup>	242	83	29	0	3	226
AO5 <sup>4</sup>	388	182	76	1	3	348
AO1-4 <sup>5</sup>	492	270	72	2	8	448
ITO1-2 <sup>6</sup>	80	17	16	1	1	72
ENG1-2 <sup>7</sup>	3	0	0	0	0	3
<b>Total</b>	<b>1,239</b>	<b>559</b>	<b>193</b>	<b>4</b>	<b>15</b>	<b>1,130</b>

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

<sup>2</sup> Provision of EEO data is voluntary

<sup>3</sup> Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the engineer and information technology classifications

<sup>4</sup> ASIO Officer grade 5 group translates to APS Level 6 and includes Intelligence Officers

<sup>5</sup> Translates to span the APS 1 to 5 classification level. Intelligence Officer Trainees are included in this group (equivalent to APS Level 5)

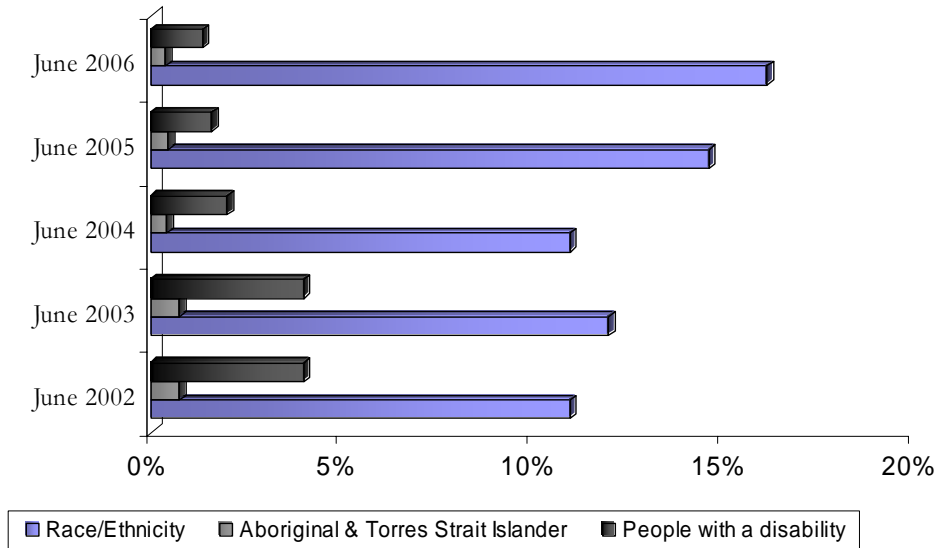
<sup>6</sup> Information Technology Officers grades 1 and 2

<sup>7</sup> Engineers grades 1 and 2

UNCLASSIFIED

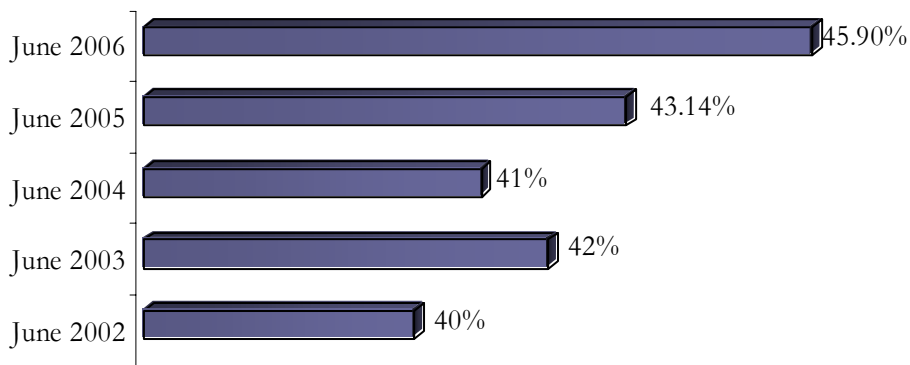
As shown in chart 16.2, since 2001–02 there has been a steady increase in the proportion of ethnically diverse staff relative to the overall staffing numbers, with ASIO currently having 16% of employees falling into this category.<sup>1</sup>

*Chart 16.2: Designated Groups in ASIO – 2001 to 2006*



The percentage of females in ASIO’s workforce generally has shown a steady increase from 40% in the year ending 30 June 2002 to 46% in the year ending 30 June 2006 (refer to Chart 16.3). ASIO’s recruitment policies and practices are based on APS standards of merit and impartiality.

*Chart 16.3: Percentage Representation of Females*



<sup>1</sup> Definitions used to calculate non-English speaking background (NESB) employee rates vary. The State of the Service Report considers only those employees born overseas whose first language was not English (called ‘NESB1’) – 5.6% of the Australian Public Service as at 30 June 2006. The Australian Public Service Employment Database (APSED) includes both NESB1 as well as NESB2 (which includes children of certain migrant populations) which is 13% in total as at 30 June 2006. ASIO’s definition is closest to that of APSED’s, but is slightly broader as it includes those employees who have a parent who did not speak English as a first language.

## UNCLASSIFIED

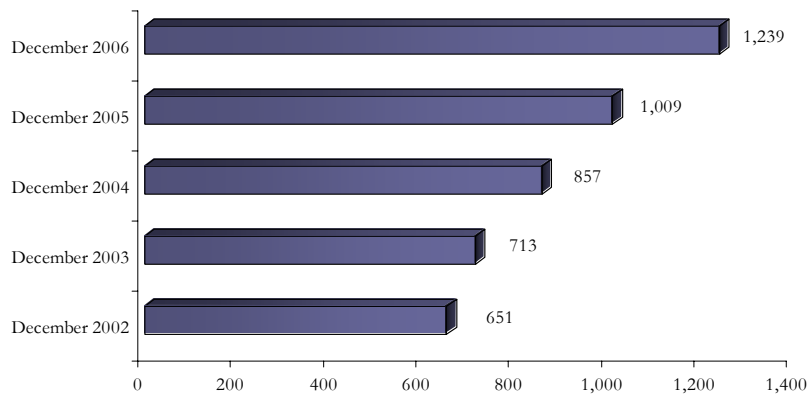
In addition, the percentage of females in senior roles within ASIO has increased to approximately 33%, with increases in both the Senior Officer and Senior Executive Service ranks.

In addition to monitoring workplace diversity issues, ASIO has recently re-evaluated the harassment contact officer network and has expanded the network to reflect the July 2006 structure.

### *Staffing Levels*

ASIO's staffing levels were increasing before the Taylor Review. However, with the Government's endorsement of the findings of the Taylor Review, ASIO is able to plan strategically for growth over the four years to 2010–11. As at 31 December 2006 ASIO had 1,239 staff. Chart 16.4 represents Organisational growth since December 2002.

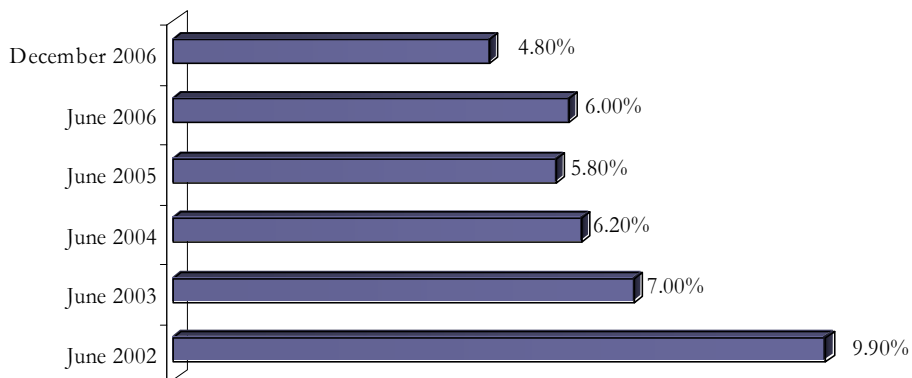
**Chart 16.4: Staffing Levels – 2002 to 2006**



### *Separation rate and reasons*

ASIO's separation rate is monitored quarterly and has been decreasing steadily since 30 June 2002 (see Chart 16.5).

**Chart 16.5: Separations – 2001–02 to 31 December 2006**



## UNCLASSIFIED

While the separation rate for the first six months of the 2006–07 financial year is approximately 4.8%, this is likely to increase to about 6% over 12 months based on historical trends of increased separations in the second half of the financial year.

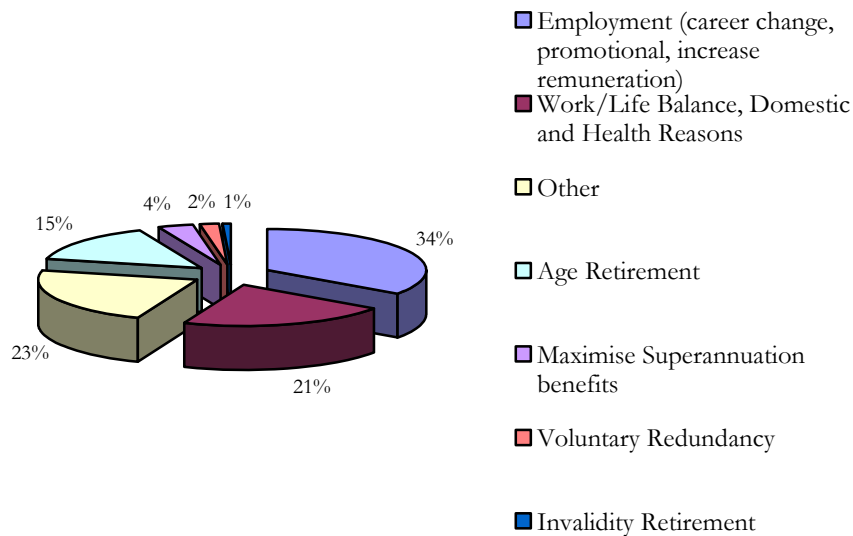
ASIO staff are invited to participate in a separation interview process in which they are asked to identify reasons for leaving the Organisation. The main factors cited include:

- employment (career change, promotion, remuneration);
- work/life balance; and
- ‘other’, including job satisfaction and to pursue study.

This process enables ASIO to identify any underlying issues or trends and facilitate the development of strategies to ensure they are addressed where appropriate.

Chart 16.6 provides greater detail on separation reasons since 30 June 2004. As illustrated the majority of staff leave for reasons relating to employment, work/life balance and other factors (such as geographic mobility, job satisfaction and the security environment).

**Chart 16.6: Reasons for Separation since 30 June 2004**



### *Staff Complaints*

Formal and informal complaints are monitored on a quarterly basis by the CE. No formal complaints or grievances were lodged during the first half of this financial year.

## 17 Staff Performance Management and Evaluation

---

### OVERVIEW

ASIO's 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 and compliance with the Organisation's values and security principles are key assessable elements of the framework.

Effective performance management is an important component of the Organisation's ability to meet its mission and outputs as it improves performance, encourages success and facilitates the achievement of potential. The current 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 actively 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 staff (security practices are integral to all professional and personal activities, and standards of work and behaviour are in accordance with ASIO's values);
- assessment of performance by line managers against the active participation by all staff in performance management and personal development; and
- identification of individual development requirements for current and future roles/careers.

Consolidations of the individual plans are used to identify emerging developmental needs to assist in the preparation of corporate strategies and budgets for the following financial years.

## RECENT DEVELOPMENTS/TRENDS

A continuing commitment to effective performance management is essential as ASIO undertakes significant workforce growth. Consequently a series of development activities have been introduced 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.

## FUTURE FOCUS

With the growth in ASIO's human resources over the next four years, maintaining and refining the framework will be an important plank in our broader human resource management strategy.

An effective performance management framework contributes to the Organisation's wider recruitment and retention efforts, specifically by assisting line managers to manage proactively underperformance, recognise staff expertise and performance excellence and to encourage initiative, innovation and resourcefulness.

## 18 Accommodation

---

### OVERVIEW

The growth in staffing numbers that flowed from the Taylor Review has put pressure on ASIO's accommodation nationally. A new Central Office building is required in Canberra to accommodate an expanded ASIO co-located with an expanded ONA. Our offices in each State capital also will grow and each office has been, or will be, relocated to larger premises.

ASIO is a national organisation with its Central Office located in Canberra and offices in the State and Territory capitals. ASIO also has Maritime Liaison Officers at seaports and Airport Liaison Officers in place at international airports. Internationally, ASIO has offices in other countries to enhance the exchange of information with international partners.

The Central Office building in Russell, Canberra is the only building that is declared publicly.

### RECENT DEVELOPMENTS/TRENDS

In April 2005, to allow for the growth of ASIO and the Office of National Assessments (ONA) and our continued co-location as recommended in the Flood Report, the Government committed \$132.6 million over four years for an extension to ASIO's Central Office building in Canberra.

However, construction of the extension was subsequently delayed pending the outcome of the Taylor Review. In October 2005 the Government agreed to the Taylor Review recommendations and announced a five-year strategic program to take ASIO's staffing to 1,860 by 2010–11.

As a consequence of this growth, ASIO reviewed its accommodation needs nationally and established a strategic accommodation planning framework to prioritise accommodation requirements and ensure the provision of new office space was aligned with business needs.

#### *Central Office, Canberra*

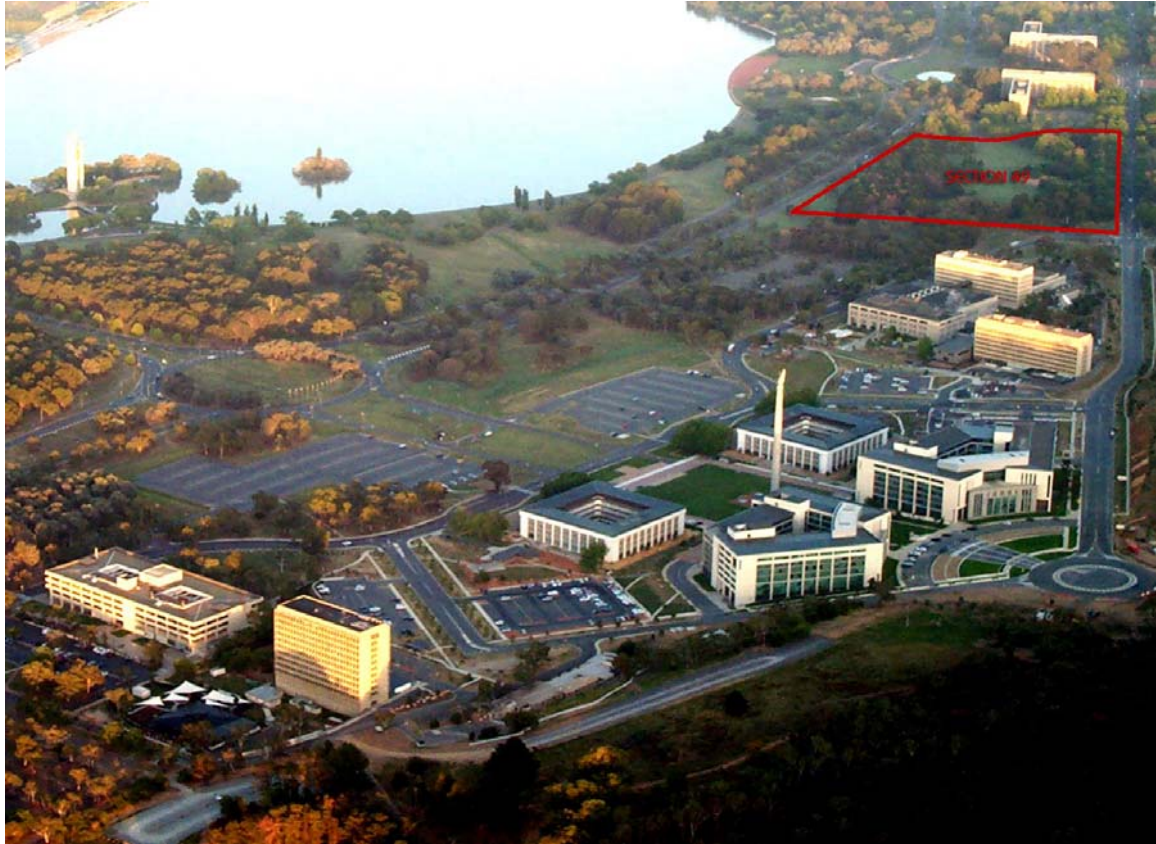
On 12 April 2006 the Government agreed that ASIO and ONA needed more adequate space and a new Central Office building in Canberra was appropriate. On 16 August 2006 the Attorney-General and Minister for Finance and Administration announced that ASIO and ONA will move to a purpose-built building within Canberra's security precinct by 2010–11.

The new building will be constructed in partnership between ASIO and the Department of Finance and Administration (DoFA) on Commonwealth land between Constitution Avenue and Parkes Way, next to Anzac Park East. The site is known as Section 49 and is located within the Parliamentary Triangle. The location is



## UNCLASSIFIED

in close proximity to the Russell Precinct and other counterpart intelligence and law enforcement agencies (see Figure 18.1).



*Figure 18.1 - Russell Precinct at Sunrise*

The site selection process was expansive with various options being considered, including 'green field' sites outside of Canberra's security precinct, other sites located within the Parliamentary Triangle and the use of existing commercially constructed buildings. Section 49 was selected with the assistance of professional advice from a range of consultants within the property industry.

The new accommodation will be purpose-designed, operating 24 hours a day with a level of security commensurate with the threat Australia faces.

DoFA currently is running tender processes for the procurement of architectural and construction services for the new building project. A project consultant was appointed recently.

The funding for the project is subject to normal budget processes and will be offset against the funding already provided for the superseded extension.

The Public Works Committee, National Capital Authority and the Department of the Environment and Water Resources have been consulted as part of the process. A full briefing on the new building project will be provided to the Parliamentary Joint Committee on Intelligence and Security.

## UNCLASSIFIED

ASIO is working closely with DoFA and ONA on this joint project, which is subject to the Gateway Review process to provide independent peer review at key stages during the life of the project.

Reconfiguration of the existing office space in Russell will commence in 2007 to make maximum use of the space pending the relocation to the new Central Office building in 2010–11.

ASIO also is taking up additional temporary accommodation to meet growth in the period leading up to occupation of the new Central Office building. The temporary sites will provide ASIO with interim accommodation for staff, corporate facilities, systems and equipment.

### *State Offices*

The Organisation's growth also has put pressure on accommodation in our State Offices to accommodate growing numbers of staff.

Funding was provided in the 2005–06 Additional Estimates and in the 2006–07 Budget for the expansion of these offices.

Significant progress has been made to deliver new accommodation nationally.

The new office premises are providing flexible multi-functional environments which can be converted rapidly to accommodate operational task force units in response to emerging issues. The new offices provide contemporary fit-out solutions while maintaining the rigorous security standards that are a necessary requirement of the Organisation.

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

### *Overseas Posts*

New overseas posts were established in 2005–06 and arrangements are in place for further expansion in 2006–07. There has also been an increase in staffing at some existing posts.

ASIO's strategic accommodation planning framework ensures all accommodation projects are planned, budgeted, scheduled and managed to align accommodation delivery with business needs. However, market conditions can cause a change in planning, either to take advantage of a commercial opportunity, or because suitable accommodation is simply not available. These issues are managed through proven, established governance arrangements.

The Corporate Executive monitors accommodation issues and receives regular briefings on progress. Project boards are established for all major projects. Information, Technical Capabilities and Security Divisions are represented on the project boards to ensure accommodation solutions are coordinated with the delivery of infrastructure and technical capability upgrades and that they meet stringent security standards. A joint ASIO, DoFA and ONA Steering Committee oversees the new building project.

## UNCLASSIFIED

For security reasons ASIO does a large component of its IT, security and technical fit-outs itself. ASIO's accommodation projects involve challenges that most government agencies do not face because a high level of security measures and specialised information and communications infrastructure must be incorporated into the office environment. When leasing commercial premises ASIO needs to upgrade components of the base building to ensure adequate business continuity provision, and to provide a secure Top Secret environment.

### FUTURE FOCUS

ASIO must continue to embrace emerging technology to provide staff with the infrastructure and capacity to communicate effectively under any feasible circumstance. Redundancy planning and contingency strategies play an important role in informing both base building and fit-out design to ensure that essential services are fully functional under a range of conditions to provide a secure 24/7 operating environment.

Ultimately, ASIO must provide contemporary office accommodation to attract and retain quality staff in a highly competitive employment market.

## 19 Security

---

### OVERVIEW

ASIO's own internal security is integral to its ability to provide advice to protect Australia and its people from threats to national security. ASIO must ensure the integrity of its information, operations, assets and relationships to preserve its covert intelligence collection role and for the continued flow of intelligence from overseas liaison partners. Without good intelligence, ASIO cannot provide advice on threats to national security.

It follows that ASIO has a strong security framework comprising structures, policies and training, and that it closely monitors emerging issues in protective security and developments in counter-intelligence to maintain security best practice.

#### *Security Framework*

ASIO's Counter-Intelligence and Security Branch is responsible for the identification and investigation of threats to the security of ASIO's personnel, information and operations; developing procedures to protect the Organisation from penetration and compromise; and ensuring the procedures are implemented properly. The focus of ASIO's security culture and systems is on prevention with a heavy emphasis on security awareness education and the identification and development of security policies and procedures.

ASIO's corporate governance structure includes a Security Committee. This committee's role is to provide a consultative forum to review and address key issues relevant to the security of ASIO's people, property and performance.

The *Australian Government Protective Security Manual 2005* (PSM) and the *Australian Government IT Security Manual* (ACSI 33) provide the minimum standards for ASIO's security policies and procedures.

#### *Contribution to Whole-of-Government Security Best Practice*

In addition, ASIO has a leading role in coordinating the development and implementation of best practice security policies and practices within the Australian Intelligence Community (AIC) and related policy departments by providing the secretariat for the Inter-Agency Security Forum (IASF) and its working groups – personnel security, physical and administrative security and information management security.

ASIO also takes a leading role in providing security awareness training in various training courses run by the AIC.

#### *Personal Security*

ASIO staff must be cleared to Top Secret Positive Vetting (TSPV) level if they are to access our information technology systems. Before joining ASIO, prospective staff

## UNCLASSIFIED

members are subject to stringent background and security checking. The revalidation/re-evaluation program then ensures staff members 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.

Psychological assessments for suitability are a minimum PSM requirement for TSPV clearances. ASIO has its own in-house psychologists who conduct assessments as well as provide counseling to staff members in need of such support. The psychologists' role is important in maintaining the security health of ASIO. If staff members are given the strategies to deal with their problems, they are less likely to develop vulnerabilities to external coercion or pressure that might lead to the compromise of ASIO's information.

Security education is provided to all staff, including at induction, through formal training programs, security awareness briefings, articles published in ASIO's in-house magazine.

### *Physical and Administrative Security*

Physical and administrative security refers to the measures of protection employed in ASIO's day-to-day working environment. They are based on the minimum standards set out in the PSM for all Australian government departments and agencies handling national security classified material and are further defined in the *House Security Instructions*.

ASIO's internal security area provides physical and administrative security advice. A staff member is designated as the House Security Officer (HSO) in each State and Territory Office. An HSO conference is conducted annually to update HSOs on the latest security policies and to identify where new policies and procedures need to be developed. A newsletter is produced every three months for the HSOs outlining new security policies and developments.

## RECENT DEVELOPMENTS/TRENDS

### *Personal Security*

The number of revalidations and re-evaluations per year is growing exponentially, consistent with the growth in ASIO staff numbers since 2001.

### *Physical and Administrative Security*

No significant security issues were identified and no major security incidents occurred during 2006.

There has been a steady decline in the percentage of security breaches incurred by ASIO staff since the introduction of a revised security breach policy in July 2005.

UNCLASSIFIED

## UNCLASSIFIED

This is a pleasing result given the numbers of new staff and their inexperience in working in a security culture. It reflects an emphasis on security awareness training for new staff, the use of benchmarks for security breaches and the invocation of stronger sanctions for multiple offenders.

During the year, ASIO conducted security audits in line with the scope and framework set by the IASF. Security audits are designed to ensure adherence to relevant security standards, to identify areas where improvement is needed or desirable and to enhance security in line with ASIO's commitment to security best practice.

### *Information and Communications Technology Security*

ASIO continues to monitor its computer networks for insecure, unauthorised and inappropriate usage.

### *Counter-Intelligence*

Counter-intelligence describes the measures to prevent attacks against ASIO from organisations, groups or individuals hostile to ASIO. The greatest threat is from within – a staff member who becomes disgruntled, a penetration of the Organisation through the recruitment stream, or a staff member who has been coerced or manipulated to work for a hostile group.

However, there are a number of incidents that have been investigated by ASIO and/or the police, including the impersonation of ASIO officers, threats made against ASIO staff, suspicious activity around ASIO premises and the compromise of ASIO undeclared premises.

## FUTURE FOCUS

### The Five Guiding Principles of Security

- Security must be considered actively and given realistic weighting in all ASIO decision-making.
- Security procedures are to be applied consistently and fully accepted by all.
- Specific accountability and responsibility for security is to be allocated to managers and their staff.
- The need-to-know principle is to be understood and applied by all.
- Security decision-making is to be based on risk management methodology.

## 20 Public Relations and Reporting

---

### OVERVIEW

ASIO provides the public with as much information as possible, within the constraints of security. The most visible aspect of ASIO's public reporting is the unclassified *Report to Parliament*. ASIO continues to be the only agency in the Australian Intelligence Community that produces an unclassified annual report that is available publicly. ASIO has published an unclassified annual report since 1982–83 under the provisions of section 94 of the ASIO Act.

In addition to the annual *Report to Parliament*, information about ASIO continues to be available publicly through: the *Annual Report of the Inspector-General of Intelligence and Security*; other reporting to the Parliament (Portfolio Budget Statements, Senate Estimates, Questions on Notice and Parliamentary Committees); interviews of the Director-General by media representatives; public statements by the Director-General; ASIO publications; and the ASIO website.

ASIO's website is the main dissemination channel for public information about the Organisation. In 2005–06, ASIO's most popular website pages were the annual *Report to Parliament* and employment-related pages.

As a security service, it is a reality that information that would be of most interest to the public (for example, details of targeting and operational capabilities, particularly those conducted under warrant) is exactly the type of information that – if released – could cause great harm to Australia's national security.

With the need to provide assurance to the community about the integrity and appropriateness of ASIO's activities, ASIO's current reporting activities are directed at achieving an appropriate balance between the need to protect its capabilities and ability to provide high-quality advice to government about threats to national security.

### RECENT DEVELOPMENTS/TRENDS

#### *Report to Parliament*

ASIO's annual report is structured to comply 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. The first version is classified and contains an account of ASIO's performance during the previous 12 months, including sensitive reporting on security risks and investigative outcomes that cannot be released publicly. That report is provided to the Attorney-General, the National Security Committee of Cabinet (NSC), the Leader of the Opposition, and a small group of senior government officials. In particular, it provides performance

## UNCLASSIFIED

information which is used by the Department of the Prime Minister and Cabinet in the preparation of its review of the performance of the intelligence agencies for consideration by NSC.

An abridged version of the classified report is then prepared for the Attorney-General to table in the Parliament, excluding all sensitive information in accordance with section 94 of the ASIO Act.

This unclassified *Report to Parliament* provides similar information to the reports of other public sector agencies although, because of security sensitivities, it is more limited in detail in relation to some operational aspects of ASIO's work. The report includes an overview of the security environment, discussion of trends (for example, changes in demand for threat assessments) and identifies, in broad terms, investigative and corporate priorities. Capability enhancements, ASIO's role in the National Counter-Terrorism Plan and ASIO's protective security responsibilities are also discussed.

Other information contained in the *Report to Parliament* includes:

- the number of threat assessments issued each year;
- the number of security assessments issued for the Department of Immigration and Citizenship to assist its decisions on visa issue;
- the number of security assessments which resulted in recommendations against visa issue;
- information about the number of questioning or questioning and detention warrants sought by ASIO;
- the number of personnel security assessments for public servants requiring security clearances, including the number of appeals against adverse assessments to the Administrative Appeals Tribunal and the outcomes of those appeals;
- the number of requests under the *Archives Act 1983* (the Archives Act) for access to ASIO records more than 30 years old, together with the percentage that were finalised within the statutory requirement of 90 days;
- information on ASIO's workplace diversity program, categories of employment, occupational health and safety, equal opportunity employment practices and senior executive service profile; and
- financial statements for the reporting year, audited in accordance with the Australian National Audit Office Auditing Standards.

### *Inspector-General of Intelligence and Security*

ASIO's activities also are the subject of a report to Parliament by the Inspector-General of Intelligence and Security (IGIS).

The IGIS reports to the Government and tables an unclassified annual report in the Parliament. The report contains an overview of complaints against the intelligence agencies and the outcome of the IGIS's inquiries into them. The IGIS report usually attracts some media attention.



## UNCLASSIFIED

If it is in the public interest, other IGIS reports on specific issues or complaints may be tabled in the Parliament and sometimes published.

### *Senate Estimates*

Since 1993 the Director-General has appeared before the now Senate Standing Committee on Legal and Constitutional Affairs ("Senate Estimates") and been questioned on aspects of its work. Senate Estimates hearings are open to the public and recorded in Hansard. Questions from the Committee can be taken on notice and the replies become part of the Hansard record.

Additionally, the Director-General can provide members of the Committee with a private briefing on sensitive security matters which does not form part of the Hansard record.

### *Other Parliamentary Business*

Members of ASIO also can be called to give evidence before other Parliamentary committees. During 2005 and 2006, ASIO appeared before the:

- Senate Foreign Affairs, Defence and Trade References Committee;
- Senate Committee on Foreign Affairs, Defence and Trade;
- Joint Parliamentary Committee on Public Accounts and Audit; and
- Senate Standing Committee on Legal and Constitutional Affairs.

### *Questions-on-Notice*

ASIO is required to respond to questions-on-notice in the same manner as any other agency. The responses become part of the Hansard record.

### *Portfolio Budget Statements*

General details of ASIO's proposed activities for the coming year, including financial expenditure, are provided in the *Portfolio Budget Statements*. These follow the standard outcome/output reporting framework, but in comparison with other agencies ASIO's statements are less detailed, reflecting the classified nature of most of ASIO's work.

### *Media Policy*

Since the late 1970s, ASIO has had a modified 'neither confirm nor deny' policy in relation to requests for information by the media. This followed a recommendation by Justice Hope in the report of the Royal Commission on Intelligence and Security 1977, that consideration should be given to the Director-General speaking in public about ASIO and its role.

In 1985 ASIO established the position of Media Liaison Officer (MLO). The MLO has a direct telephone line which is listed in the telephone directories of the State and Territory capital cities. This complements the 1800 toll free number for the ASIO Central Office switchboard which appears in every Australian telephone directory.

The MLO is responsible for:

- being the central point of contact for telephone inquiries from journalists;

UNCLASSIFIED

## UNCLASSIFIED

- coordinating interview requests from members of the media; and
- supplying inquirers with information that is publicly available on ASIO, including directing them to information contained in ASIO's *Report to Parliament*, public statements by the Director-General or the Attorney-General, or ASIO's website.

ASIO does not make any public comment on sensitive national security matters such as targeting of individuals and organisations; operational methods; or liaison arrangements with other Australian and foreign intelligence and security agencies.

### *ASIO's publications*

ASIO has a number of publications which are available to members of the public:

- *ASIO Now* (first published in 1996) is a booklet which provides a plain English account of ASIO's role and functions. It is used to respond to common or regularly asked enquiries by members of the public, for example school students doing assignments and as part of an information package for applicants for ASIO employment. This publication is being updated and will be released in 2007.
- ASIO's *Corporate Plan* has been publicly available since 1993. The *Corporate Plan 2007-2011* is scheduled for release in early 2007. In addition to information on ASIO's Outcomes and Outputs, the *Corporate Plan* provides information on ASIO's mission, vision and values.
- ASIO also publishes protective security information.

### *Website – [www.asio.gov.au](http://www.asio.gov.au)*

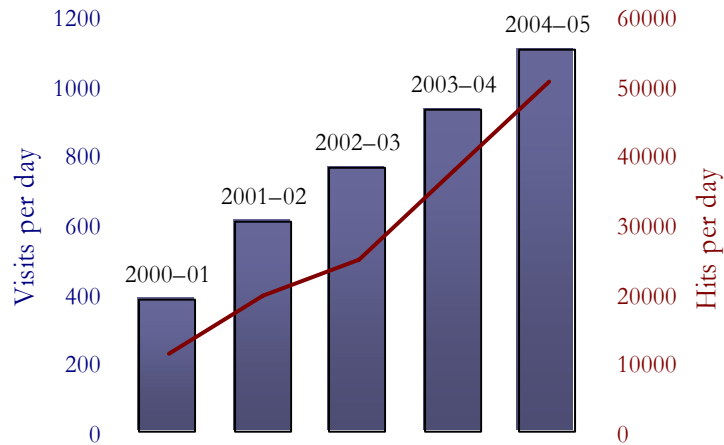
ASIO's website was launched by the then Attorney-General on 22 June 2000. It provides an extensive consolidation of background information on ASIO. Importantly, it provides members of the public with 24-hour access to information about ASIO. Chart 20.1 shows the level of public interest in ASIO's website.

The website has several main sections which contain information about various aspects of the Organisation including ASIO's work, publications, employment, and contact information.

The website incorporates links to other 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.

Redevelopment of the website commenced in 2005–06 with a revised site scheduled for implementation in 2006–07. The website is updated regularly with new information, particularly public statements by the Director-General.

*Chart 20.1: Interest in ASIO's website*



*Public Statements*

In 2005–06 the Director-General delivered 19 public addresses including to business forums, conferences and institutions. These addresses are on ASIO’s website.

ASIO also makes a presentation to the annual Security in Government Conference. This conference, organised by the Protective Security Coordination Centre, was originally intended for government agency security advisers. It has since been opened up to security advisers from private industry. ASIO’s protective security area also has a stand at the conference, a fact which is usually reported in the media.

*Letters from Members of the Public*

ASIO receives approximately one letter a day from members of the public who are requesting or volunteering information. Many of the requests are from those seeking ASIO assistance but are not of direct relevance to ASIO’s functions, that is, not a matter for national security. In those cases they are sent a brief letter directing them to the appropriate agency. The requests that are of relevance to national security are disseminated to the appropriate areas within the Organisation.

Others seeking information include school and university students who ask for ASIO assistance with a project or assignment. In the case of the former, it is usually possible to help by directing them to the ASIO website or other relevant websites. For university students, the ASIO library can provide assistance through part of the inter-library loan system.

FUTURE FOCUS

ASIO's website provides new opportunities for ASIO to communicate with the public. Re-design and upgrading of the website will provide additional opportunities for ASIO to make information available publicly where it is appropriate and consistent with the requirements of security.





