

**UNCLASSIFIED**

**PARLIAMENTARY JOINT COMMITTEE ON  
INTELLIGENCE AND SECURITY:**

**REVIEW OF ADMINISTRATION AND  
EXPENDITURE NO 8: 2008-09**

---

**ASIO SUBMISSION**

**UNCLASSIFIED**

# CONTENTS

---

<b>ASIO's Roles and Functions</b> .....	<b>4</b>
<b>Executive Overview</b> .....	<b>6</b>
<b>Summary of Key Outcomes and Activities 2008–09</b> .....	<b>9</b>
<b>The Security Environment 2008–09 and Outlook</b> .....	<b>11</b>
<b>Expenditure</b> .....	<b>13</b>
Budget Growth	13
Financial Performance	13
Resource Allocation	14
Financial Management and Internal Controls	14
<b>Structure of the Organisation</b> .....	<b>16</b>
Organisational Structure	16
<b>Direction and Strategic Planning</b> .....	<b>18</b>
Management of Growth	18
Corporate Governance	19
Organisational Performance Management	21
Strategic Allocation of Resources	22
Audit, Evaluation and Fraud Control	22
<b>Legislation and Litigation</b> .....	<b>24</b>
Legislative Amendments	24
Litigation Matters	24
Use of ASIO's Special Powers	25
Training	25
<b>Security of ASIO and ASIO Security Assessments</b> .....	<b>26</b>
Vetting of ASIO Staff	27
Security Breaches	27
E-Security Arrangements and Enhancements	27
Security Assessments	27
<b>Human Resource Management</b> .....	<b>33</b>
Recruitment	33
Training and Development	35
Workplace Diversity	38
Staff Complaints	40
Separation Rates	40
<b>Accommodation</b> .....	<b>42</b>
Central Office, Canberra	42
Exemption from the Public Works Committee	43
State and Territory Offices	44
<b>Public Relations and Reporting</b> .....	<b>45</b>
ASIO's <i>Report to Parliament</i>	45
Parliamentary Oversight	45
Public Statements	45
Inspector-General of Intelligence and Security	46

## **FIGURES**

---

Figure 1: Revenue from Government, 2001–12.....	13
Figure 2: Financial performance, 2001–12.....	14
Figure 3: Purchase of capital items 2001–09 .....	14
Figure 4: Organisational structure at 30 June 2009 .....	17
Figure 5: Corporate governance arrangements.....	21
Figure 6: Visa security assessments process .....	29
Figure 7: Personnel security assessments process.....	31
Figure 8: Personnel security assessments 2000–09 .....	36
Figure 9: Counter-terrorism security assessments process.....	32
Figure 10: Staffing growth, 2005–09 .....	33
Figure 11: Advertisements from ASIO’s 2008–09 recruitment activity .....	34
Figure 12: Age of staff .....	39
Figure 13: Length of service of ASIO staff.....	39
Figure 14: Gender balance by classification.....	40
Figure 15: Separations by percentage of total staff and reason .....	41

## **TABLES**

---

Table 1: Price of ASIO’s outputs .....	22
Table 2: Visa security assessments 2003–09.....	29
Table 3: Counter-terrorism checks 2003–09 .....	32
Table 4: ASIO attachments .....	38

# ASIO'S ROLES AND FUNCTIONS

---

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

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

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

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

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

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

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

The ASIO Act also gives ASIO a function of more generally providing protective security advice to the Government. ASIO is responsible for collecting foreign intelligence under warrant within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence, and in collaboration with the Australian Secret Intelligence Service (ASIS) and the Defence Signals Directorate (DSD).

As ASIO is the only agency in the Australian Intelligence Community (AIC) authorised in the course of its normal duties to undertake investigations into – and collect intelligence on – the activities of Australian citizens, it operates within a particularly stringent oversight and

## **UNCLASSIFIED**

accountability framework. The foundation of this framework is the ASIO Act, which has been crafted to ensure there is an appropriate balance between individual rights and the public's collective right to security. The Inspector-General of Intelligence and Security (IGIS) – an independent statutory authority – also plays an important role in ASIO's oversight.

## EXECUTIVE OVERVIEW

---

The Australian Security Intelligence Organisation's (ASIO) submission to the review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into Administration and Expenditure No. 8 provides a detailed account of ASIO's activities during 2008–09 covering:

- the security environment 2008–09 and outlook;
- expenditure;
- the structure of the Organisation and distribution of staff across ASIO;
- direction, strategic planning and management of expansion;
- legislative changes that have an impact on administration;
- security of ASIO;
- ASIO security assessments;
- human resource management;
- staff performance management and evaluation;
- accommodation, including the New Building Project; and
- public relations and reporting.

### THE SECURITY ENVIRONMENT 2008–09 AND OUTLOOK

Security threats to Australia and Australian interests evolved further in 2008–09. As in previous years, the new dimensions of threats built on – rather than replaced – existing elements, adding new layers of complexity to the challenges of terrorism, espionage and foreign interference.

Australia will remain a terrorist target for the foreseeable future. Within Australia, terrorism-related activity will continue with a high likelihood of local terrorist groups emerging from time to time. ASIO's investigative and operational activity in 2008–09 was focused on the coordinated investigation of a Melbourne-based group of Islamic extremists and their alleged planning for an armed suicide assault on an Australian military facility.

Espionage and foreign interference directed against Australia and Australian interests will continue with new technologies allowing new and different forms of undeclared intelligence activity.

### EXPENDITURE

Funding to ASIO in 2008–09 expressed in terms of total price of Outputs was \$361.730m, an increase of \$57.621m (19 percent) from 2007–08. Revenue from Government increased \$62m to \$353m. The increase reflects the final stages of growth in staff and depreciation expense from previous equity injections arising from the *Review of ASIO Resourcing* (the Taylor Review) in 2005. ASIO's funding and growth levels will stabilise in 2010, when ASIO reaches the end point of its five-year growth and capability enhancement program.

ASIO received an equity injection of \$71m in 2008–09, a reduction from significant equity injections in 2007–08 (\$159m) and 2006–07 (\$113m). This injection allowed for further substantial investment in ASIO's information technology infrastructure and the state and territory offices network, and the commencement of ASIO's new central office building.

## **STRUCTURE OF THE ORGANISATION**

There were no major structural changes made to the Organisation during 2008–09. However, ASIO's ability to continue to provide the outcomes required by Government in an ever-evolving environment requires constant attention.

ASIO will continue to ensure that it is both professionally and structurally best positioned to respond to issues of security concern as they arise, and also able to identify potential threats and develop strategies to meet such threats.

## **DIRECTION AND STRATEGIC PLANNING**

ASIO has a strong corporate governance framework and culture that support the particular needs of an intelligence agency and the importance that the public and the Government place on ensuring ASIO is accountable, professional and impartial.

ASIO's corporate governance arrangements reflect the Organisation's sustained focus on risk management, accountability, performance measurement, building capability and managing growth.

## **LEGISLATION AND LITIGATION**

Amendments that commenced during the reporting period which had relevance to ASIO's administration were amendments to the *Telecommunications (Interception and Access) Act 1979*.

ASIO was involved in over 60 litigation matters in 2008–09, including criminal, civil and administrative proceedings.

## **SECURITY OF ASIO**

In 2008–09, ASIO reviewed and authorised 526 new security clearances, 314 probation revalidations, 152 thirty-month mid-cycle revalidations, and 179 full re-evaluations. Reforms in the clearance revalidation process in 2008–09 included mechanisms to better identify potential security concerns early in an employee's tenure.

## **ASIO SECURITY ASSESSMENTS**

ASIO contributed to the security of Australia's borders, including through security assessments for applicants for Australian visas, and continued to improve these client service timeframes.

## **HUMAN RESOURCE MANAGEMENT**

Recruitment remained a high priority in 2008–09. ASIO's net staffing increased by 13 percent to 1,690 – ASIO is on track to achieve staffing levels of approximately 1,860 by 2010–11, consistent with recommendations made in the Taylor Review in 2005.

ASIO increased its investment in training in 2008–09, to support the needs of a growing workforce with a focus on the development of management and leadership skills, language training and specialist training for ASIO's investigative work.

## **ACCOMMODATION**

Construction work commenced on ASIO's new special-purpose, high-security central office. The new building is being designed and constructed in partnership with the Department of Finance and Deregulation. It is expected to be completed by 2012.

**PUBLIC RELATIONS AND REPORTING**

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



# SUMMARY OF KEY OUTCOMES AND ACTIVITIES 2008–09

<b>Priorities</b>	Counter-terrorism remained ASIO's highest priority in 2008–09. However, counter-espionage, foreign interference and counter-proliferation were also high priorities.
<b>Partnerships</b>	ASIO strengthened partnerships with intelligence and law enforcement agencies, in particular the Australian Federal Police (AFP).
<b>Foreign Liaison</b>	ASIO continued to expand its overseas networks and representation, and as at 30 June 2009 had 316 approved liaison relationships with authorities in 122 countries.
<b>Business Liaison</b>	ASIO increased its liaison with the private sector, with subscribers to the Business Liaison Unit (BLU) increasing by 40 percent in 2008–09. The BLU made over 200 security reports available for business subscribers on its website.
<b>Customers</b>	The audience for ASIO reporting expanded in 2008–09, and included 80 Commonwealth and state and territory customers within Australia.
<b>Reporting</b>	ASIO produced 2,738 reports and assessments, including 1,092 threat assessments and 138 threat analysis papers.
<b>ASIO Security Assessments</b>	ASIO completed 59,884 visa security assessments including 1,466 assessments for protection visa applicants. ASIO issued adverse security assessments for two individuals seeking entry to Australia in 2008–09.
<b>Protective Security</b>	ASIO continued to provide high-quality protective security advice to clients including through protective security risk reviews, vulnerability assessments, ministerial office security reviews and technical surveillance counter-measures testing.
<b>Major Event Security</b>	ASIO's expertise in major event security planning was used to provide security advice in support of World Youth Day (Sydney), the Beijing Olympic and Paralympic Games, and the Asia-Pacific Economic Cooperation forum, Peru.
<b>Technical Collection</b>	ASIO continued its major investment in the development and delivery of technical collection capability and worked closely with domestic and international partners, including industry.
<b>Community Contact Program</b>	ASIO continued to build upon its long-standing program of confidential contact with leaders and influential members of various ethnic and religious community groups in Australia.
<b>Oversight and accountability</b>	The Inspector-General of Intelligence and Security conducted a series of monitoring, inspection and inquiry activities and was satisfied there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or human rights.
<b>Public statements</b>	The Director-General of Security addressed conferences and audiences from business, government and academia.
<b>Recruitment</b>	Recruitment remained a high priority. ASIO's net staffing increased by 13 percent to 1,690.
<b>Training</b>	ASIO increased its investment in training to support the needs of a growing workforce with a focus on the development of management and leadership skills, language training and specialist training for ASIO's investigative work.
<b>New Building</b>	Construction work commenced on ASIO's new special-purpose, high-security

**UNCLASSIFIED**

	central office. It is expected to be completed by 2012.
--	---

# THE SECURITY ENVIRONMENT

## 2008–09 AND OUTLOOK

---

### TERRORISM

Within Australia, ASIO identified new extremists and ASIO's intelligence investigations revealed a range of terrorism-related activity – the most serious being alleged planning by a Melbourne-based group of Islamic extremists for an armed suicide assault on an Australian military facility. The Middle East, South Asia and now East Africa are the primary sources of motivation and capability for extremists in Australia. Small numbers of Australians continue to look to conflict theatres overseas for inspiration and some aspire to participate in the violence or to learn from the tactics and techniques employed by extremists there.

Attacks in Islamabad, Mumbai, and Lahore in 2008–09 highlighted the enduring strategic intent of al-Qa'ida-inspired terrorism and the potential for Australians to be victims of attacks overseas. These and other events reinforced ASIO's assessment that terrorism continues to be a persistent threat to Australia and Australian interests, and that the possibility of an attack in Australia remains.

### ESPIONAGE AND FOREIGN INTERFERENCE

The threat of hostile intelligence services exploiting Australian information systems was brought into sharper focus, with traditional espionage methods supplemented by new high-technology techniques. ASIO found further evidence of hostile intelligence services using the Internet as a means of appropriating confidential Australian Government and business information.

### COMMUNAL VIOLENCE

No information came to ASIO's attention in 2008–09 to indicate significant ongoing tensions between any community groups within Australia. ASIO was alert to the potential for communal violence as police investigated criminal activity against Indian students in Australia. Specific incidents outside or within Australia have the potential to cause short-term tensions resulting in some violence between communities. Usually the communities engage in lawful and peaceful protest action to demonstrate their concerns.

Nationalist extremist and racist extremist (NERE) groups did not undertake organised or premeditated violence in Australia towards ethnic or religious communities in 2008–09.

### VIOLENT PROTESTS

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

No significant violent protest occurred in Australia in 2008–09.

### PROLIFERATION

ASIO's counter-proliferation work focused on detecting and preventing attempts to exploit Australia's industrial, technological and educational resources for the illicit development of

Weapons of Mass Destruction (WMD).

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

## **BORDER SECURITY**

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

ASIO's border network of aviation and maritime liaison officers worked in close partnership with key aviation and maritime partners including the AFP, the Department of Immigration and Citizenship, the Australian Customs and Border Protection Service and airport and seaport authorities. ASIO continued to contribute to the security of Australia's borders through visa security assessments.

- In 2008–09, ASIO completed 59,884 visa security assessments (compared with 72,688 in 2007–08) including 1,466 assessments for protection visa applicants.
- ASIO issued adverse security assessments for two individuals seeking entry to Australia in 2008–09. The visa applicants were assessed to pose a security threat due to links to a terrorist group or a foreign government.

## **OUTLOOK FOR THE SECURITY ENVIRONMENT**

Australia will remain a terrorist target for the foreseeable future. Within Australia, terrorism-related activity will continue. Extremist ideology will continue to resonate with a small but dangerous minority, so there is a high likelihood of local terrorist groups emerging from time to time. Some Australians will continue to support extremism financially, logistically or by involving themselves in terrorist operations in Australia or overseas.

Espionage and foreign interference directed against Australia and Australian interests will continue. New technologies will allow new and different forms of undeclared intelligence activity, but the tried and true methods of cultivating, recruiting and running human sources with access to confidential information, secrets and sensitive technology will continue to be used.

Most issue motivated groups will continue to use peaceful and non-violent disruptive protest tactics. A very small proportion of activists continue to believe violent protest tactics are an effective means of influencing government and business decision-makers. These individuals are likely to plan for violent protest activity at selective anti-war and anti-globalisation protests.

Countries of proliferation concern will continue to adapt and evolve their procurement activities to thwart WMD control efforts. Australia will remain of interest to them, including because of our technologically advanced industry and military, strategic alliances and world class educational facilities. ASIO expects the need for counter-proliferation intelligence support for regulatory and enforcement agencies to increase. ASIO also expects an increase in the need for its advice on WMD matters in general.

# EXPENDITURE

## BUDGET GROWTH

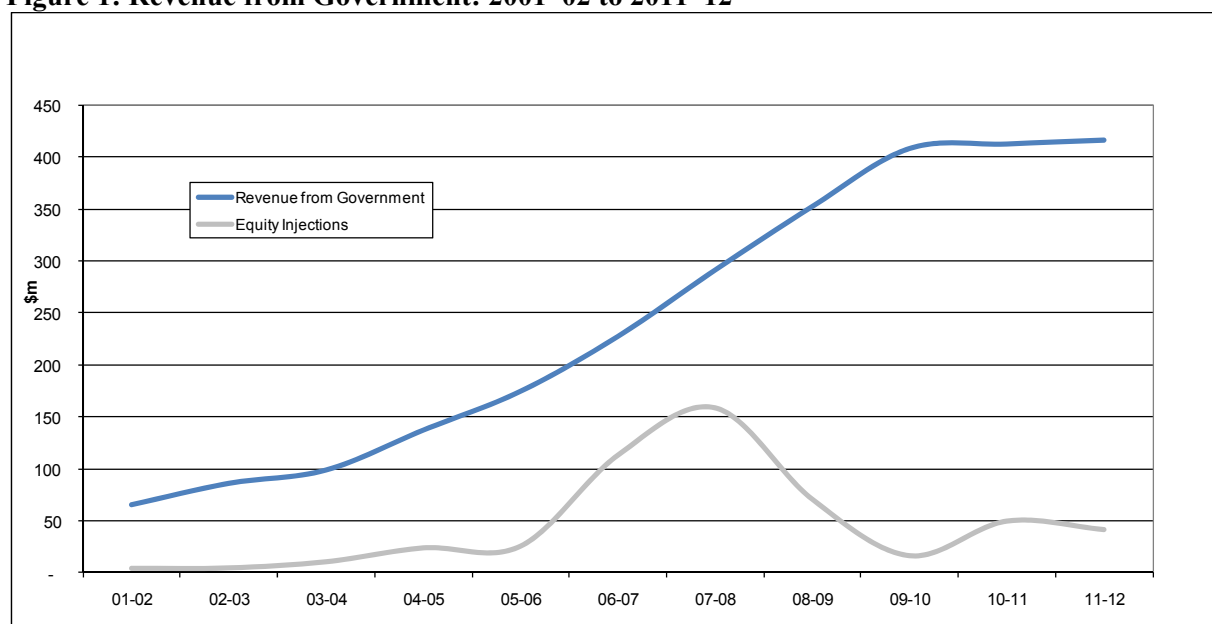
ASIO's budget is set out in the Portfolio Budget Statements with the audited outcome published in ASIO's annual *Report to Parliament*. Portfolio Budget Statements are prepared annually, consistent with the Commonwealth's budgeting requirements, with Portfolio Additional Estimates Statements (PAES) also prepared if new measures are approved by the Government post-Budget. ASIO did not publish a PAES in 2008–09.

Funding to ASIO in 2008–09 expressed in terms of total price of Outputs was \$361.730m, an increase of \$57.621m (19 percent) from 2007–08.

Revenue from Government increased \$62m (21 percent) to \$353m, from \$291m in 2007–08 and \$227m in 2006–07. The growth continues through 2009–10 with revenue from Government increasing \$56m (16 percent) to \$409m and total price of Outputs estimated to be \$413m. This reflects the final stage of growth in staff and depreciation expense flowing from previous equity injections arising from the Taylor Review in 2005.

ASIO received an equity injection of \$71m in 2008–09, a reduction from significant equity injections in 2007–08 (\$159m) and 2006–07 (\$113m). This injection allowed for further substantial investment in ASIO's information technology infrastructure and the state and territory offices network, and the commencement of ASIO's new central office building.

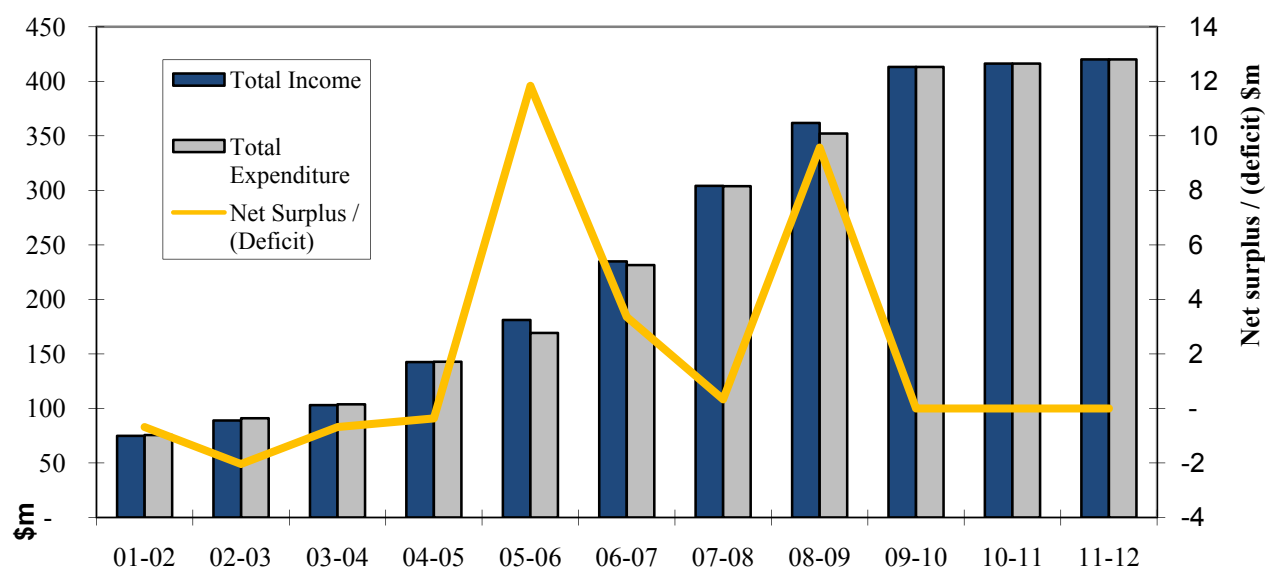
**Figure 1: Revenue from Government: 2001–02 to 2011–12**



## FINANCIAL PERFORMANCE

ASIO recorded an operating surplus of \$9.6m in 2008–09, with the last deficit occurring in 2003–04. This reflects ASIO's improved base funding profile, which was established as part of the Taylor Review. The 2008–09 surplus represents 2.5 percent of revenue with unpredictability in employee on-costs making the most significant contribution to the variance.

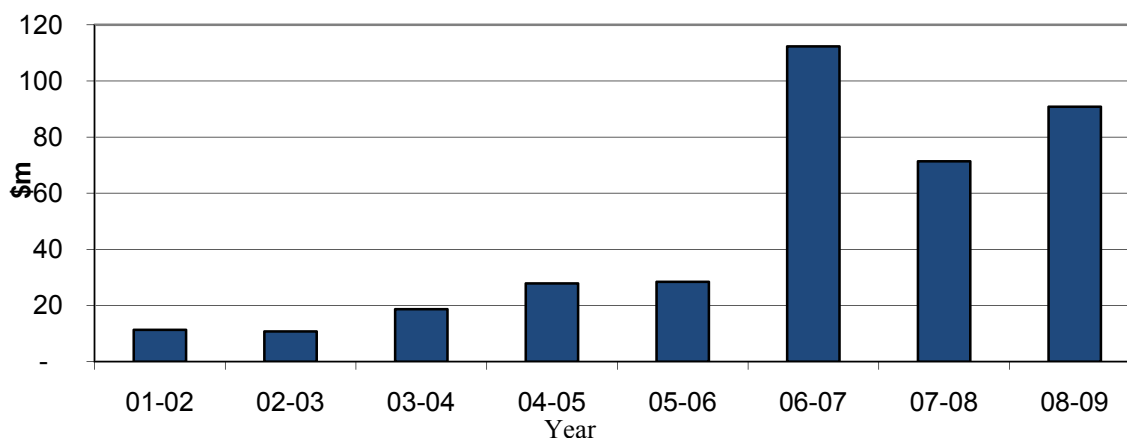
**Figure 2: Financial performance: 2001–02 to 2011–12**



### RESOURCE ALLOCATION

The significant capital expenditure of recent years has provided infrastructure to support ASIO's capability enhancement.

**Figure 3: Purchase of capital items 2001–02 to 2008–09**



### FINANCIAL MANAGEMENT AND INTERNAL CONTROLS

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

Internally, the Chief Finance Officer reports monthly to the ASIO Corporate Executive (the main ASIO forum for managing strategic corporate resource issues). Reporting covers

## **UNCLASSIFIED**

current and future organisational financial performance matters and strategic financial management planning.

In addition, ASIO continually looks at current practices to ensure that financial resources are utilised in an effective and efficient manner within agreed financial parameters. 2009–10 will see ongoing resource allocation analysis to ensure ASIO is well placed, financially, at the end of the Taylor growth period.

Financial management practices are supported by a financial management information system with integrated internal controls aligned to the Organisation's financial framework.

In addition to audits conducted by the ANAO and internal system controls, ASIO's internal auditor also undertakes a range of financial audits.

# **STRUCTURE OF THE ORGANISATION**

---

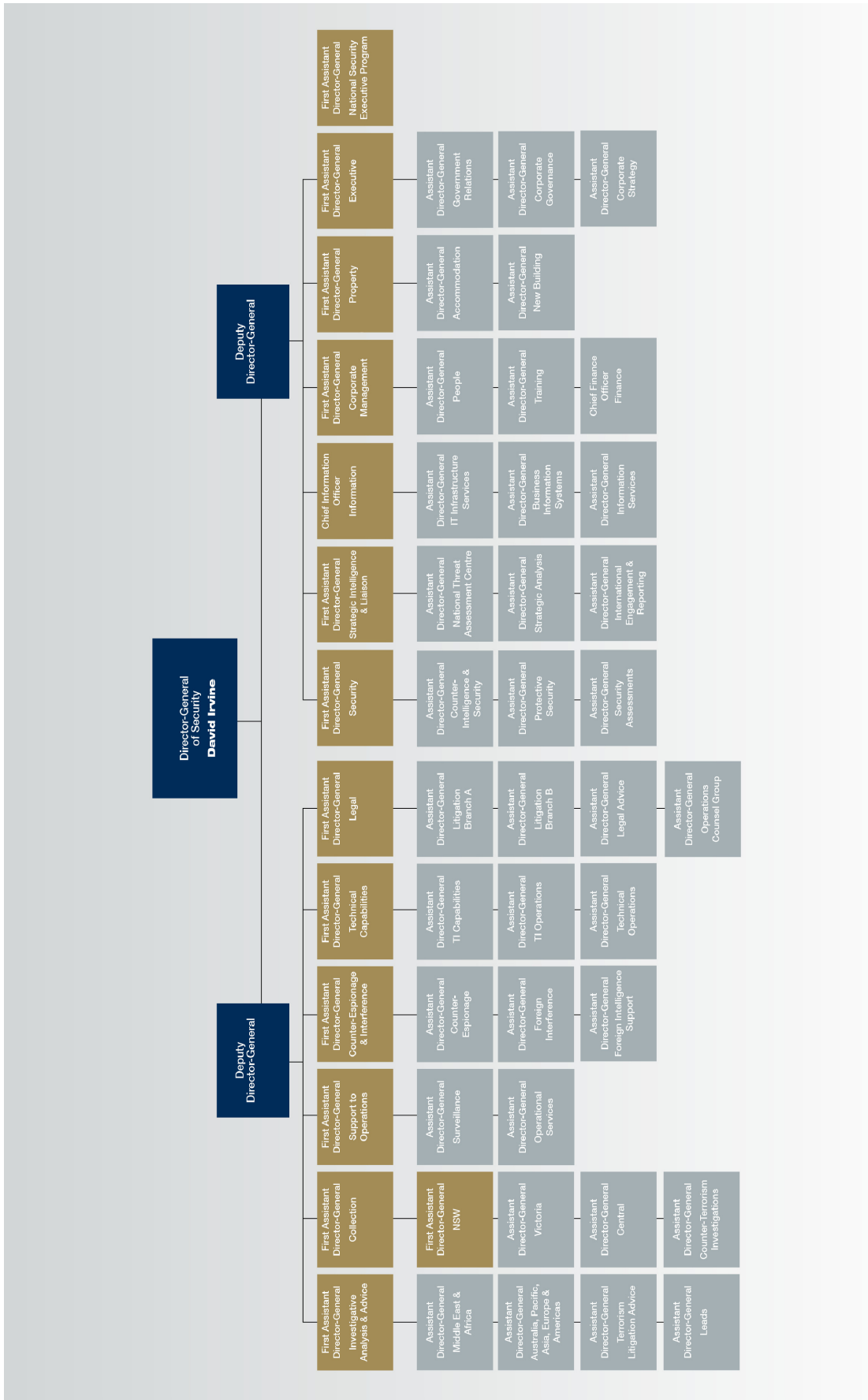
## **ORGANISATIONAL STRUCTURE**

During the reporting period, there were no major structural changes made to the Organisation. However, our ability to continue to provide the outcomes required by Government in an evolving environment needs constant attention.

ASIO's structure remains under review to ensure the capability we have achieved through growth is sustainable into the future.



Figure 4: Organisational structure at 30 June 2009



# DIRECTION AND STRATEGIC PLANNING

---

## MANAGEMENT OF GROWTH

Over the six years from mid-2003 to mid-2009, ASIO has grown in size, complexity, capability and reach. The Organisation:

- has more than doubled in staff size (1,690 in June 2009 compared with 688 in 2003):
  - around 64 percent (over 1,000) of staff currently work in the intelligence-focused areas
  - around 18 percent are Intelligence Officers (IO) (including IOs who are Senior Officers or Senior Executive Service (SES) officers)
    - this proportion is growing slowly. However, the IO job family remains difficult to grow and sustain
  - the separation rate has decreased from around 11 percent in 2002 to 4.5 percent in June 2009.
- has around one thousand (two-thirds) staff members who have joined since 2003 – some at entry level commencing their careers but many with prior experience in other government departments and the private sector;
- has a larger, stronger and more diverse SES with 60 SES officers and twelve divisions compared to 15 SES and five divisions in 2003;
- is slightly younger (mean age now 38 years compared to 40 years in 2003), with around 73 percent of staff aged 44 years or younger and 45 percent of staff aged 34 years or younger; and
- is more gender balanced (55 percent male and 45 percent female, compared with 58 percent and 42 percent respectively in 2003)
  - there continues to be a higher representation of males in the intelligence collection and analysis, technical and IT functions. Female representation is more widespread in the legal, corporate and security functions.

The growth and transformation of the Organisation has created many more career and promotional opportunities for staff but has also generated a number of challenges, including:

- *Managing expectations and career aspirations:* many staff members now expect more rapid advancement and promotion than was previously the case. As the growth rate of the Organisation slows there will be fewer opportunities available compared to the demand from staff seeking advancement. Retaining the highest calibre staff in an environment with more limited advancement options will require innovative and attractive solutions beyond the inherent interest and challenge in the work provided by the Organisation.
- *Leadership:* the need to fill critical Senior Officer vacancies, particularly in the intelligence-focused areas has drawn heavily on officers with limited or narrow experience in the Organisation and who may not have well-developed leadership skills. In response to this challenge, ASIO continues to invest heavily in leadership and management training and this will continue to be an ongoing focus;

## UNCLASSIFIED

- *Demography*: the relatively larger proportion of younger staff members, particularly those starting or raising young families, has seen an increase in the number of staff taking parental leave or entering into part-time working arrangements. This trend, which predominantly involves female staff members, is impacting on the capabilities of those areas with a significant proportion of females;
- *Advertising and Marketing*: ASIO's continued focus on quality has meant attracting and recruiting sufficient numbers of high calibre applicants continues to be challenging. A sustained effort to refresh and strengthen our advertising and marketing efforts directed at increasing our pool of suitable applicants remains a priority;
- *Growth vs. Maintenance*: growth needs to be balanced against the requirement to replace and replenish those areas that lose staff members through retirement and resignation. The long lead times associated with the recruitment and vetting process result in critical vacancies remaining unfilled for extended periods;
- *Culture*: ASIO continues to undertake a number of activities that are directed at nourishing an appropriate culture. These include the Workplace Diversity Program, the New Employee Support Officer program, the Senior Officer Orientation Workshops, the Reconciliation Action Plan and the review of the ASIO Code of Conduct; and
- *Engaging with and Managing Risk*: ASIO's growth has occurred at a time when there has been little, if any, relief in the rapid operational tempo. Strengthening of the SES ranks has allowed for narrower spans of control and more concentrated senior level focus on work units. While this structure has the potential to enhance risk management within the Organisation, it needs to be accompanied by a culture of excellence and accountability at all levels and a focus on driving forward the work of the Organisation.

ASIO has strengthened resources in workforce management and retention and is reviewing the policy framework and developing a number of initiatives aimed at ensuring the attraction and retention of valuable staff, including:

- generous studies assistance opportunities;
- the New Employee Support Officer Program;
- making information about employee benefits and entitlements more accessible;
- investigating phased retirement programs; and
- developing internship programs.

## CORPORATE GOVERNANCE

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

ASIO's corporate governance arrangements reflect the Organisation's sustained focus on risk management, accountability, performance measurement, building capability and managing growth.

ASIO's corporate committee structure is supported by a number of sub-committees and working groups that inform and strengthen the performance of the relevant committees, while also deeply embedding corporate governance principles at all levels of the Organisation (see Figure 6).

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

- The Director-General's Meeting comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. It manages the day-to-day business of

## UNCLASSIFIED

ASIO, including areas of ongoing corporate priority and urgent or emerging issues requiring consideration by the Executive.

- The Corporate Executive comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. Several Assistant Directors-General on rotation and the Staff Association President attend as observers. It sets ASIO's strategic direction and oversees resource management, providing the main forum for managing strategic corporate priorities and resource issues. It also conducts detailed quarterly reviews of performance across the Organisation. The Corporate Executive files are reviewed by the ANAO on a regular basis.

The Director-General's Meeting and the Corporate Executive provide oversight to eight ongoing and one non-ongoing corporate committees.

- The Intelligence Coordination Committee, chaired by a Deputy Director-General, includes senior managers involved in the intelligence process. The Committee establishes security intelligence investigative priorities and allocates broad resources on a risk management basis. It also performs quarterly reviews against strategic objectives and approves arrangements for ensuring the legality and propriety of ASIO's intelligence collection, analysis and advice.
- The Audit and Evaluation Committee, chaired by a Deputy Director-General, includes a senior executive officer from the ANAO. The Committee facilitates the internal audit of ASIO in accordance with the Internal Audit Charter, by setting priorities for audit, fraud control and evaluation planning. It considers the findings of the internal audits and evaluations, and ensures management-endorsed recommendations are implemented.
- The Organisational Development Committee, chaired by the head of Corporate Capability and Services Division and including the Staff Association President, provides strategic guidance on ASIO's growth with particular regard to growing the capabilities of ASIO's staff, shaping an appropriate culture and managing change.
- The Staff Placements Committee, comprising the two Deputy Directors-General, manages the strategic placement of staff across ASIO, addressing existing and longer-term priorities and capability gaps.
- The Security Committee, chaired by the head of Security Division and including the Staff Association President, reviews and addresses key issues relevant to the security of ASIO's people, property and Information Technology systems. The Committee also drives development of security policies and practices.
- The Research and Development Committee is chaired by the head of Technical Capabilities Division and includes ASIO's Science Adviser and a representative from the Defence Science and Technology Organisation. It provides strategic oversight and direction to technical collection and analysis capability.
- The Information Management Committee, chaired by the Chief Information Officer, provides strategic oversight and direction to ASIO's Information and Communication Technology (ICT) work program. Five program boards oversee ICT projects on a thematic basis, and report to the Committee.
- The ASIO Consultative Council, co-chaired by the head of the Corporate Capability and Services Division and the Staff Association President, comprises representatives from management and the Staff Association. The committee is an advisory board which makes recommendations to the Director-General on human resource policies and practices. It facilitates management and staff discussion and resolution of issues of mutual interest and concern.
- The New Building Committee (non-ongoing) provides strategic guidance on the new

building project, including direction on significant design milestones, review of significant risk issues and oversight of project budget and program.

**Figure 5: Corporate governance arrangements**



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

**ORGANISATIONAL PERFORMANCE MANAGEMENT**

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

- The Corporate Executive meeting reviews the performance of key areas of activity through regular reporting on budget and finance, growth, IT, security, property management and accommodation, and the general 'health' of ASIO.
- The Director-General's Meeting oversees performance of a range of critical issues, including recruitment, some legal and litigation matters, and critical business areas such as security assessments.

In 2009 ASIO interviewed representatives from key Commonwealth, state and territory and private sector agencies to seek feedback on their engagement with ASIO, the quality of ASIO advice and product, and ASIO's overall performance in meeting their requirements. The survey also looked to identify areas for further engagement or improvement in the relationship and services provided by ASIO.

Commonwealth customers generally considered their relationships with ASIO have improved. ASIO officers were seen to be more willing to assist and more focused on customer needs. Some customers said they would value expanding their existing network of contacts within ASIO. ASIO is facilitating this in response, and as part of a broader effort to ensure the Organisation is seamlessly integrated within Australia's national security architecture. ASIO will continue its successful Partnership Forum series and the program of attachments, which enable direct interaction between partner agencies and ASIO.

The Australian Federal Police and state and territory law enforcement agencies reported a highly satisfactory level of engagement with ASIO. In the last twelve months, these relationships have strengthened and are considered even more positive, useful and cooperative than previously reported. There has also been an improvement in engagement at the senior officer level. These agencies consider ASIO product and advice is valuable and relevant to their requirements. Continuing to develop ASIO's relationship with law enforcement agencies will remain a high priority for ASIO.

Private sector clients reported increasingly positive levels of engagement with ASIO, particularly via the Business Liaison Unit. ASIO is considered responsive and client-focused, which has instilled a high level of trust and confidence. These clients believe their decisions are well informed as a result of ASIO's reporting, which is regarded as timely and relevant.

## **STRATEGIC ALLOCATION OF RESOURCES**

**Table 1: Price of ASIO's Outputs**

Output	01-02	02-03	03-04	04-05	05-06	06-07	07-08	08-09
Output Group 1: Security Intelligence	\$74.915m	\$88.945m	\$103.023m	\$142.449m	\$181.099m	\$234.764m	\$304.109m	\$361.730m

Resource allocation is formally reviewed and considered between February and May each year, with the Corporate Executive Committee (CE) approving internal divisional base budgets and an organisational project budget. Allocation of funding to projects reflects both the need to maintain current capabilities and the ability to meet emerging priorities.

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

## **AUDIT, EVALUATION AND FRAUD CONTROL**

The Audit and Evaluation Committee maintains oversight of internal audit activity and fraud control within the Organisation, reporting to the Director-General of Security.

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

ASIO has an active program of internal audits and evaluations. During 2008-09, ASIO

## UNCLASSIFIED

undertook an extensive review of risk management. This resulted in a draft *Strategic Risk Management Plan*, a risk-based *Annual Work Plan for 2009–10*, a *Strategic Audit Plan 2009–11*, a Risk Management Toolkit and Risk Management Policy and Framework.

In 2008–09, nine internal audits were completed and were the subject of (classified) reporting to ASIO's Audit and Evaluation Committee. No loss of public monies was reported in these audits. Recommendations for improvements to administrative or procedural anomalies have been reviewed and accepted through the Committee and responsible work areas.

Fraud control in ASIO is a collective responsibility. Staff have two prime responsibilities – to not commit fraud and to report suspected instances of fraud. Investigation of one case of suspected fraud was completed, which found there was no case to answer, and no further cases were reported in 2008–09.

A new *Fraud Control Plan (2008–2010)* was implemented in December 2008 based on the 2008 Fraud Risk Assessment.

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

As required under both the Commonwealth and New South Wales assumed identity schemes, audits were conducted in January and July 2009 on records of authorisations, variations and revocations approved under the schemes in 2008–09. No discrepancies were detected.

As required by the legislation, a report for 2008–09 on the number of authorisations, the general activity undertaken with the use of assumed identities, and relevant audit results was provided to the IGIS.

# LEGISLATION AND LITIGATION

---

## LEGISLATIVE AMENDMENTS

During the 2008–09 financial year, ASIO liaised with Commonwealth departments and agencies regarding policy development and proposed legislative amendments relevant to ASIO’s activities. Many of these proposals are still being developed, or considered by Parliament, and have not impacted on ASIO’s administration. ASIO also continued to foster close working relationships within government to ensure that the legislative framework supports ASIO’s functions and capabilities.

The following legislative changes were relevant to ASIO’s activities during the 2008–09 financial year.

The *Telecommunications Interception Legislation Amendment Act (No.1) 2009* (which commenced on 22 May 2009) amended the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). The amendments facilitated declarations, subsequently made on 8 July 2009, to allow the Queensland Police Service (QPS) and the Crime and Misconduct Commission (CMC) to access interception capabilities and delivery systems already paid for by ASIO and other law enforcement agencies pursuant to existing agreements executed with telecommunications carriers. Deeds were executed that allowed ASIO to cost recover a financial contribution from QPS and CMC in 2009–10.

## LITIGATION MATTERS

In the 2008–09 financial year, ASIO was involved in over 60 litigation matters. These included criminal, civil and administrative proceedings. While the overall litigation volume remained comparable with that of 2007–08, it is considerably higher than during any period preceding 2005. This high volume and the diversity and complexity of matters generated a significant work load. ASIO also responded to numerous requests for a broad range of material for use in litigation.

During 2008–09, there were a number of high profile litigation outcomes:

Melbourne Pendennis: 13 people were charged with a range of terrorism offences, including membership of a terrorist organisation. ASIO produced 67 witness statements and responded to 17 subpoenae. No ASIO officers were required to give evidence at the trial. Of the 13 accused, one pleaded guilty before trial, seven were found guilty at trial, four were acquitted and one was re-tried after the jury could not reach a unanimous verdict. That accused later pleaded guilty. Those found guilty were convicted and sentenced to periods of imprisonment ranging from six to 15 years.

Sydney Pendennis: Nine people were charged with conspiring to do an act/acts in preparation/planning for a terrorist act/acts. Four of the nine subsequently pleaded guilty to various terrorism offences and five proceeded to trial. ASIO responded to 39 subpoenae, and 23 ASIO officers gave evidence at trial. Belal Khazaal: Mr Khazaal was found guilty of making a document in connection with assistance in a terrorist act. The jury could not reach a unanimous verdict in relation to the other charge of inciting others to commit a terrorist act. ASIO produced four witness statements and responded to six subpoenae. One officer gave evidence at trial.

James Seivers: Mr Seivers, a former ASIO officer, was re-tried and found guilty of



## UNCLASSIFIED

the unauthorised communication of intelligence. Matthew O’Ryan was found guilty of aiding and abetting Mr Seivers. ASIO provided 18 witness statements and ten ASIO officers gave evidence at the re-trial. Mr Seivers and Mr O’Ryan were sentenced to periodic detention.

Mamdouh Habib: ASIO was directly involved in two legal matters initiated by Mr Habib: an appeal to the Full Federal Court against the Administrative Appeals Tribunal’s upholding of an adverse security assessment and passport denial, and a Federal Court compensation claim alleging the Commonwealth had defamed Mr Habib and aided and abetted his alleged mistreatment during his detention overseas. In March 2009, the Federal Court struck out a number of Mr Habib's claims against the Commonwealth on the grounds they had no reasonable prospects of success. The proceedings are ongoing.

During 2008-09, ASIO supported Commonwealth legal efforts by developing and maintaining close relationships with a range of departments and agencies, in particular the Australian Federal Police and state and territory police forces, and the Commonwealth Director of Public Prosecutions. ASIO provided instructions and advice in relation to the protection of national security classified material in connection with legal proceedings, including through the negotiation of protective orders made under the *National Security Information (Criminal and Civil Proceedings) Act 2004*. ASIO also liaised with the courts (through the Australian Government Solicitor) to help produce closed court transcripts in a form suitable for public release.

### USE OF ASIO’S SPECIAL POWERS

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

ASIO’s Legal Division reviews every warrant request prior to its consideration by the Attorney-General.

### TRAINING

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

# **SECURITY OF ASIO AND ASIO SECURITY ASSESSMENTS**

---

## **VETTING OF ASIO STAFF**

ASIO employees require a Top Secret (Positive Vetting) (TSPV) national security clearance. ASIO initiated over 564 TSPV security clearances from recruitment activity in 2008–09. A further 297 national security clearances were initiated, at varying security clearance levels, for a range of contractors and consultants engaged by ASIO.

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

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

In 2008–09, ASIO implemented a number of practices which resulted in, on average, an efficiency saving of around 20 working days for security clearance processing.

### *Revalidation and Re-Evaluation Program*

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

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

In 2008–09, ASIO reviewed and authorised 526 new security clearances, 314 probation revalidations, 152 thirty-month mid-cycle revalidations, and 179 full re-evaluations. All ASIO staff responded to the annual revalidation process.

Reforms in the clearance revalidation process in 2008–09 included mechanisms to better identify potential security concerns early in an employee's tenure.

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

ASIO contributed to the Australian Government's 2008 *Review of E-Security*, working with the Defence Signals Directorate and the Australian Federal Police to produce a wide-ranging classified assessment of the electronic threat environment.

ASIO's IT Security directorate monitors ASIO systems and responds to threats. The directorate identifies and implements methods to mitigate risks to ASIO systems, including its externally connected systems. These include:

- the establishment of a dedicated intrusion detection and network monitoring team;
- enhanced audit and investigation capability across ASIO ICT systems, including real-time monitoring and response;
- ICT system security inspections and provide recommendations for improvement;
- sharing ICT threat advice within the Australian Intelligence Community;
- developing and reviewing internal ICT Security Policies;
- targeted ICT security education programs for ASIO staff, ICT staff and ICT contractors; and
- provision of ICT security advice, including advice in response to general enquiries and design, development, and implementation advice to ICT projects.

ASIO collaborated closely with other agencies to strengthen Australia's e-security during the conduct of the 2008 E-Security Review and examination of issues related to the National Broadband Network.

## **SECURITY ASSESSMENTS**

ASIO is responsible for furnishing security assessments to Commonwealth agencies, including for:

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

## UNCLASSIFIED

- applications for Australian citizenship; and
- the cancellation of Australian passports or the seizure of foreign passports.

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

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

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

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

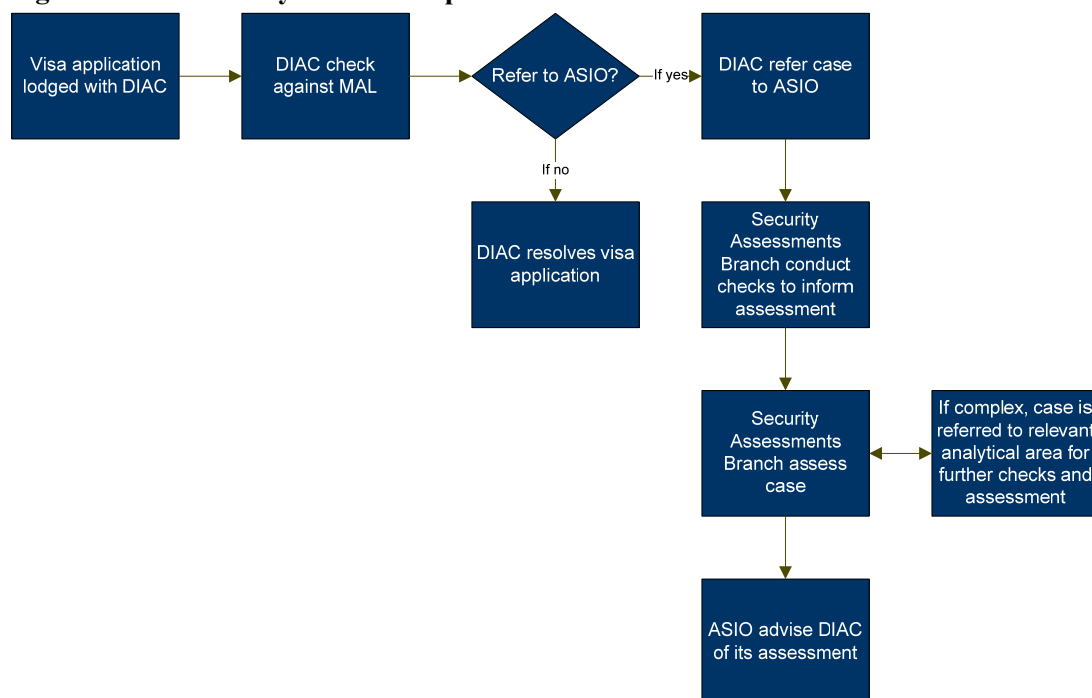
Requesting agencies then make a determination, based on ASIO's security assessment as well as the agency's own assessment. Any administrative action taken in response to an ASIO assessment is the responsibility of the requesting agency – ASIO is not responsible for granting or denying security clearances,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

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

### *Visa Security Assessments*

ASIO contributes to the security of Australia's borders through visa security assessments. Any person applying for a visa to travel to, and remain in, Australia may have their application referred by DIAC to ASIO for a security assessment – an assessment of the threat that the person's presence in Australia would pose to security (as defined in the ASIO Act).

**Figure 6: Visa security assessment process**



ASIO processes visa security checks in order of referral from DIAC, taking into account any agreed priority cases (with particular emphasis on refugee, humanitarian and protection cases, and genuine compassionate or compelling cases).

ASIO has continued to improve client service timeframes. The Next Generation Border Security initiative, predominantly involving ASIO and DIAC, has improved the effectiveness and efficiency of security checking processes conducted by ASIO for applicants for Australian visas. Direct connectivity between DIAC and ASIO for the electronic transfer of security referrals and responses is now in place. This new system has improved the tracking and reporting of security referrals.

ASIO completed 59,884 visa security assessments in 2008–09 (see Table 2). These comprised 12,988 assessments for permanent visa holders and 46,896 assessments for temporary visa holders.

In 2008–09, ASIO issued adverse security assessments for two individuals seeking entry to Australia. The visa applicants were assessed to pose a security threat due to links to a terrorist group or a foreign government.

**Table 2: Visa security assessments 2003–09**

Type of entry	2003–04	2004–05*	2005–06*	2006–07*	2007–08*	2008–09*	% decrease from 2007–08
Temporary	30,841	39,015	39,973	44,197	56,126	46,896	16
Permanent	13,881	13,402	13,174	9,190	16,562	12,988	22
<b>Total</b>	<b>44,722</b>	<b>52,417</b>	<b>53,147</b>	<b>53,387</b>	<b>72,688</b>	<b>59,884</b>	<b>18</b>

*Personnel Security Assessments*

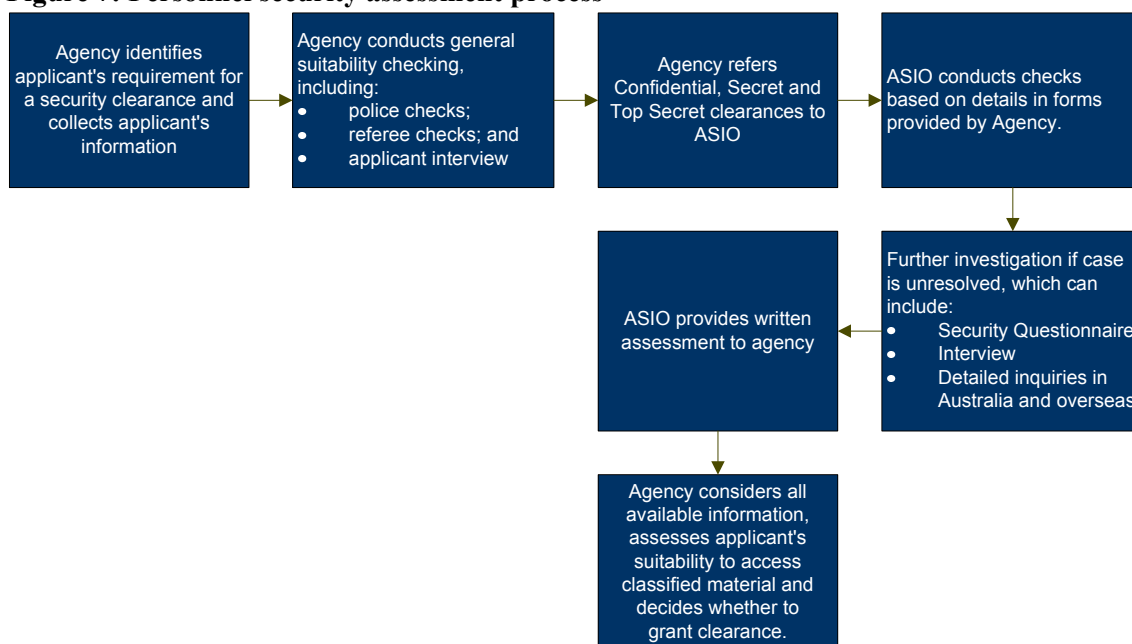
ASIO provides personnel security assessments to assist government departments and agencies

in deciding whether to grant access to national security classified information.

Applicants for security clearances must provide detailed background information to their sponsoring agency and ASIO. ASIO’s personnel security assessments take into account intelligence information held by ASIO, as well as known risk factors. ASIO completed 21,699 personnel security assessments in 2008–09, consistent with a long-term trend of growth in the overall personnel security assessment workload.

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

**Figure 7: Personnel security assessment process**

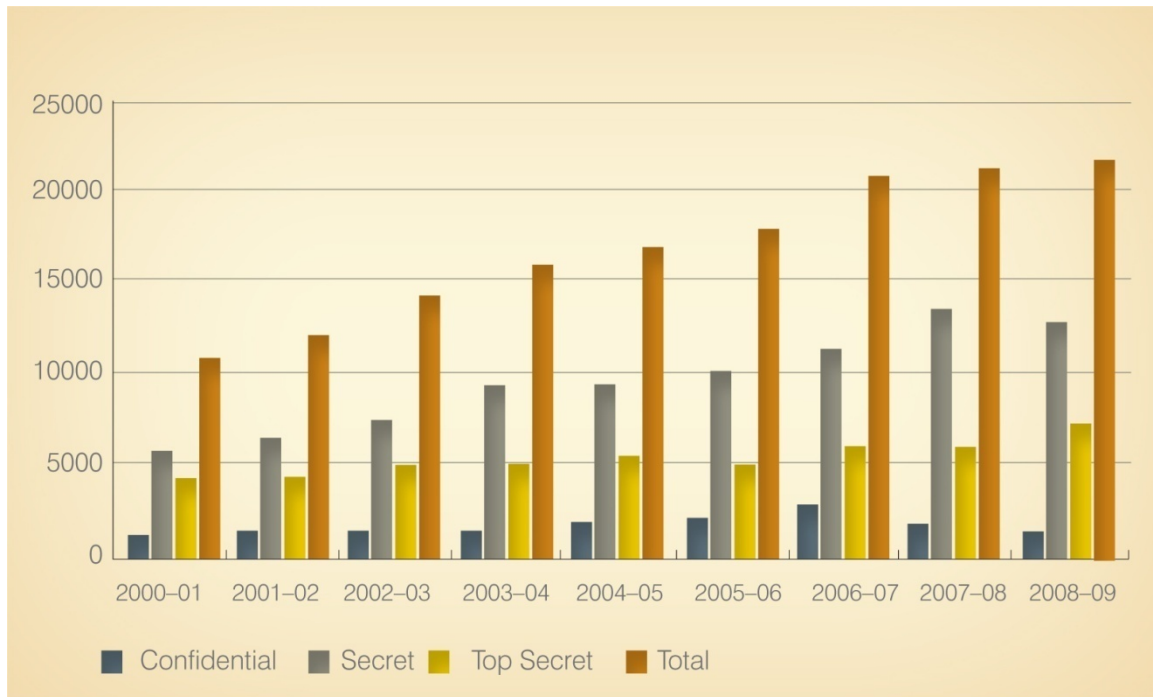


ASIO does not assess general suitability for the access proposed, nor does it issue security clearances for other agencies – this remains the responsibility of the requesting agency. ASIO’s assessment is considered by the requesting agency, in conjunction with information gathered from other avenues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

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

As part of ASIO’s ongoing efforts to improve service, it has established direct electronic connectivity with primary clients, including the Defence Security Authority. These refinements enhance administrative processes and reporting arrangements.

**Figure 8: Personnel security assessments 2000–09**



*Counter-Terrorism Security Assessments*

ASIO’s counter-terrorism security assessments are carried out at the request of government authorities who are responsible for accreditations, predominantly the AFP and AusCheck. In 2009, ASIO established direct connectivity with AusCheck for the electronic transfer of the information required to undertake counter-terrorism checks. This has provided greater efficiencies, and improved the tracking and reporting of security referrals.

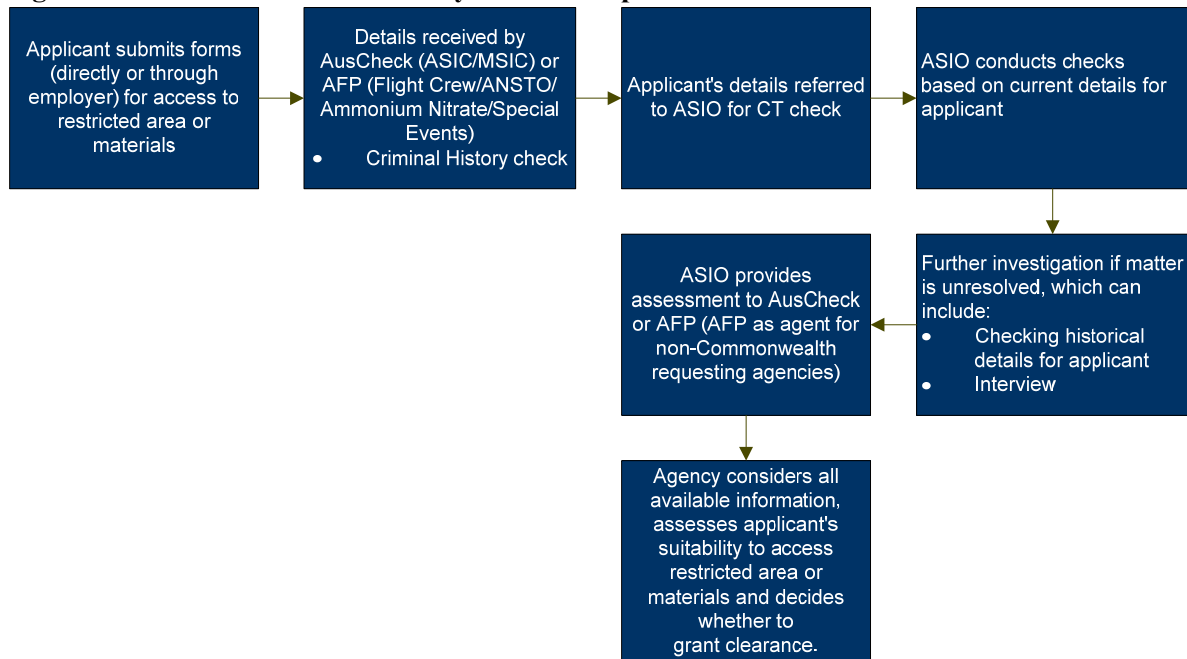
ASIO completed 65,119 counter-terrorism checks in 2008–09 (see Table 3), 98 percent of which were completed within ten days. These included:

- 56,266 checks for Aviation and Maritime Security Identity Cards for pilots, trainee pilots, air and sea vessel crew, and persons requiring access to controlled areas at air and seaports;
- 7,948 checks for persons requiring licences to access ammonium nitrate; and
- 905 checks for staff and visitors to the Australian Nuclear Science and Technology Organisation (ANSTO) facility at Lucas Heights, Sydney.

No adverse or qualified counter-terrorism security assessments were issued as a result of counter-terrorism security assessments conducted during 2008–09.

There has been a steady growth in ASIO’s counter-terrorism security assessment responsibilities since 2003–04, although variations in workload from year to year have been marked. The variation has been driven by the introduction of additional categories of checking (such as ammonium nitrate access) and surges in the lead-up to major events. This is likely to continue for the foreseeable future.

**Figure 9: Counter-terrorism security assessment process**



**Table 3: Counter-terrorism checks**

Type of check	2003–04	2004–05	2005–06	2006–07	2007–08	2008–09
Aviation/Maritime Security Identity Cards	58,147	38,466	71,733	118,118	70,084	56,266
Ammonium Nitrate	-	1,634	7,428	6,419	4,502	7,948
ANSTO	-	-	-	1,027	1,251	905
Commonwealth Games	-	-	56,149	-	-	-
G20 Finance Ministers' Meeting	-	-	-	1,580	-	-
Asia-Pacific Economic Cooperation forum and World Youth Day	-	-	-	7,837	13,453	-
<b>Total</b>	<b>58,147</b>	<b>40,100</b>	<b>135,310</b>	<b>134,981</b>	<b>89,290</b>	<b>65,119</b>

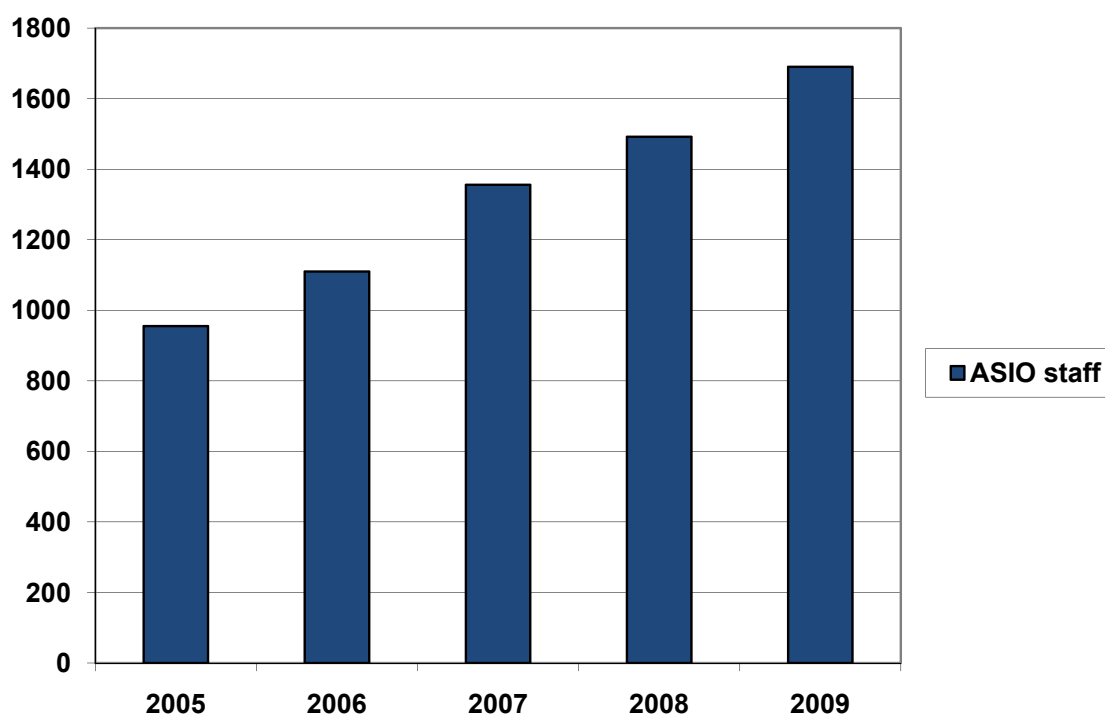


# HUMAN RESOURCE MANAGEMENT

## RECRUITMENT

ASIO's success depends on the commitment and calibre of its staff. Recruitment is, therefore, a high priority, particularly as ASIO is in the final stages of a substantial growth program. In 2008–09, ASIO's net staffing increased by 198, exceeding the growth forecast of 170 additional staff and taking the total staff number to 1,690. ASIO is on a growth program, set to achieve staffing levels of around 1,860 by 2010–11, consistent with recommendations made in the Taylor Review in 2005.

**Figure 10: Staffing growth, 2005–09**



In 2008–09, ASIO's exposure to the employment market was enhanced through the use of innovative and diverse recruitment advertising. Employment market research in 2008–09 resulted in a new recruitment brand for ASIO – 'ASIO something more...' ASIO expanded its use of on-line, electronic, outdoor and radio advertising and industry specific publications. ASIO was represented at university career fairs around Australia to promote it as an employer of choice.

There was a strong response to ASIO's advertisements with 12,550 applications in 2008–09, compared with 9,567 applications received in 2007–08. Recruitment strategies were successful in attracting appropriately skilled applicants. They were also more cost effective as ASIO spent less on recruitment advertising – \$1,962m in 2008–09, down from \$2,192m in 2007–08.

Figure 11: Advertisements from ASIO's 2008-09 recruitment activity

ASIO's Job Family Advertising 2008-09

A chance presents itself.  
An opportunity to experience the something more you've been looking for.  
This is that chance.  
What happens next is up to you.

<b>Workforce Planning Analyst</b> \$71,807 - \$101,509 + super	<b>Intelligence Support Officers</b> \$55,223 - \$64,647 + super + Sydney	<b>Director, Advanced Analytical Applications</b> \$106,850 - \$117,550 + super
<b>Systems Administrator</b> \$94,040 - \$101,509 + super	<b>Client Service Officers, Security Force</b> \$51,645 - \$55,649 + super + Canberra & Melbourne	<b>Web Services Officer</b> \$55,649 - \$64,647 + super
<b>Administration &amp; Intelligence Support Officers</b> \$51,645 - \$55,649 + super	<b>Security Assessors</b> \$51,645 - \$55,649 + super	<b>Administration Officer</b> \$71,807 - \$81,906 + super
<b>Technical ICT Specialists</b> \$55,649 - \$81,906 + super	<b>Electronics Specialists</b> \$59,223 - \$81,906 + super	<b>IT Specialist - Network Maintenance &amp; Analytical Support</b> \$55,649 - \$81,906 + super
<b>Electronics Production Leader</b> \$71,807 - \$81,906 + super	<b>Logistics Support Officer</b> \$55,223 - \$64,647 + super + Sydney	

Closing date: Friday, 28 August 2009. All roles are based in Canberra unless otherwise stated.

ASIO.GOV.AU

Australian Government  
Australian Security Intelligence Organisation

**ASIO**  
something more...

Intelligence Officer Advertising 2008-09

**Find yourself.**

- you stop.
- you talk.
- you listen.
- you connect.
- you guide.
- you develop.

not everybody can do this job.  
but then.  
you're not everybody.

**are you?**

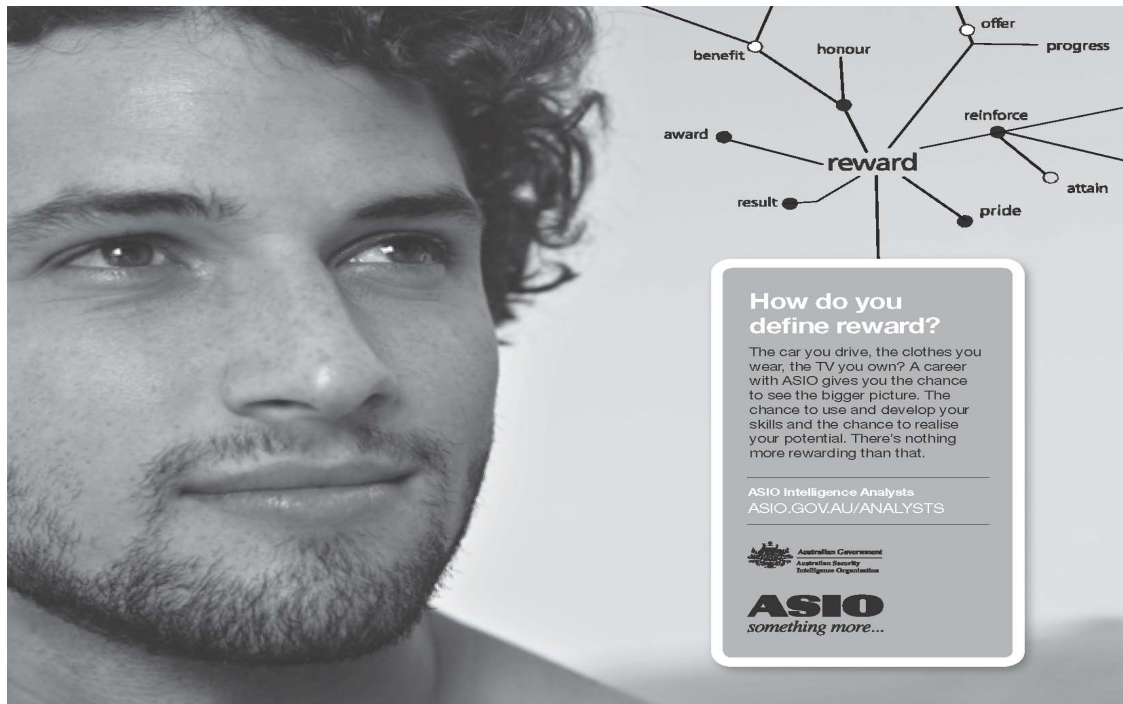
ASIO.GOV.AU/INTELLIGENCE

Australian Government  
Australian Security Intelligence Organisation

**ASIO**  
something more...

Applications close 2 October 2009

**Intelligence Analyst Advertising 2008–09**



Throughout 2009, ASIO Recruitment Directorate maintained contact with graduates from Careers Fairs through the use of update HTML emails advising them when job opportunities were available.

ASIO's focus continued to be on building the intelligence-focused areas while maintaining capability in the enabling functions. In particular, the recruitment of Intelligence Officers, Intelligence Analysts and Linguists remained challenging.

Legal functions continued to receive recruitment support to meet the ongoing demands for legal advice and assistance.

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

**TRAINING AND DEVELOPMENT**

In 2008–09, ASIO invested over 40 percent more in training (\$10.3m compared with \$6.4m in 2007–08). This additional investment supported the needs of a growing workforce, and reflects a commitment to ensuring staff members are adequately skilled.

Training is ongoing, and investment is set against the skills and knowledge that employees require to carry out their duties to the highest level. ASIO's Learning and Development Strategy informs training course development and delivery is targeted to business needs. Throughout 2008–09 there was a continuing focus on technical skill development, complemented by training in interpersonal skills to support management and leadership practices, including relationship management.

The New Employee Support Officer (NESO) program, introduced in 2007–08, provides support and guidance to new staff members. New starters are allocated an experienced staff member from a different workgroup to assist their transition to ASIO. A review of the NESO program has commenced with preliminary findings that the program has been positive and beneficial in providing support and assisting the integration of new starters into the Organisation.

### *Corporate Training Programs*

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

- an induction program for all new starters;
- wide-ranging administrative training – contract management, project management, staff selection skills, presentation skills, trainer training, interviewing skills, strategic thinking, communication, finance and budgeting;
- information technology training – basic and advanced training in the use of ASIO's computer systems;
- ethics and accountability training – all members of staff are required to attend at least once every three years;
- discipline-specific courses covering subjects such as Islamic history and culture, and the political and social drivers of terrorism;
- Studies Assistance Program – supporting tertiary study by members of staff – the program now has over 144 staff members; and
- the Director-General's Study Bursaries – supporting members of staff who achieve outstanding results in their studies while maintaining high levels of work performance.

In 2008–09, ASIO implemented a study initiative allowing up to 13 high-potential staff full-time postgraduate study for up to a year, fully funded by ASIO. This initiative is an investment in ASIO's future and provides high-calibre staff with an avenue to undertake advanced career and personal development activities.

ASIO conducted a series of internal seminars on topics of professional interest to staff. The seminars seek to foster a sense of teamwork and a shared culture, through broadening knowledge of work areas across the Organisation.

### *Management and Leadership Skills*

ASIO continues to place a strong emphasis on the development of its SES and Senior Officers. The development of its leaders during 2008–09 included a range of learning activities, with over 200 senior staff trained in management and leadership.

Three SES forums were held, which focused on managing growth, corporate planning, whole-of-government operations and legal challenges. Leading academics and practitioners in a range of fields addressed these forums. Two combined SES and Senior Officer forums considered issues such as legal matters, priorities and plans, and upgrades to technical capabilities.

ASIO's suite of leadership programs was evaluated and reviewed in 2008–09. This led to short workshops on specific management skill-sets and a new internal management development program for high-potential ASIO officers who may be promoted to the Senior Officer level.

### *Performance Management*

ASIO's Performance Management Framework continues to remain a strong focus within the Organisation with 88 percent of staff having a formal, written 'Performance Agreement' with their line manager. As a result of the changes made to the Framework in 2007–08, such as the automation of the process and the introduction of a new rating system, the Performance Management Framework is embedded within the Organisation.

As part of the negotiation process of the Organisation's Enterprise Bargaining during 2009, the Performance Management Framework will be reviewed to ensure it is aligned with best practice strategies and is still a useful management tool for frontline management and staff.

*Australian Intelligence Community Training*

ASIO continued to support a whole-of-government approach to intelligence needs and partnerships. This included providing presenters and participants to the AIC-wide Induction and Senior Officer Development programs and allocating places for participants from other agencies on ASIO training programs.

*Language Training*

ASIO continues to invest in language skills to support its operations, and to enable it to engage effectively with foreign liaison partners. ASIO's commitment in 2008–09 included:

- full-time training in languages relevant to ASIO's investigative work;
- full-time language training for ASIO overseas-posted officers, provided by the Department of Foreign Affairs and Trade;
- training for linguist staff to refine and enhance their skills; and
- a Language Skills Allowance (up to \$12,000 per year) for staff with language proficiencies.

*Attachments*

ASIO has a well-developed attachment program with staff posted both from and to ASIO as outlined in Table 4. In 2008-09, this included the attachment of an ASIO senior manager to AFP. ASIO's attachment program has improved cooperation and interoperability with a range of other agencies and encourages the sharing of skills, capability, knowledge and information.

**Table 4: ASIO Attachments**

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

**WORKPLACE DIVERSITY**

ASIO's staffing profile compares favourably with that of the broader Australian Public Service. Recruitment of new staff members over recent years has boosted the diversity of skills and experience within the Organisation. While some two thirds of ASIO's staff have been with the Organisation for less than five years, the injection of knowledge, skills and experience gained elsewhere in the public and private sectors has been of considerable benefit. At 30 June 2009, 88 percent of ASIO's total staffing of 1,690 was working on a full-time basis. This represented a full-time staff equivalent (FTE) of 1,599.

Approximately eight percent (or 135) of ASIO's staff was employed on a part-time basis compared with around 12.9 percent in the broader APS in 2008–09. Most of these part-time staff members (86 percent, or 116) were women, with around half being in the 35–44 year age group.

The median age of ASIO's workforce is now 36 years (compared to the APS median of 42 years in 2008–09). The median age has continued to decrease with the growth of the Organisation. Only 17 percent of ASIO's workforce is aged 50 years or older compared with 27 percent in the APS in 2008–09.

ASIO officers from non-English speaking backgrounds now comprise 17.1 percent of ASIO staff, an increase from 16.4 percent in 2007–08. While ASIO has been able to attract and recruit a larger number of individuals from ethnically diverse backgrounds, and will continue to seek to attract more applicants from diverse backgrounds, a range of cultural and other factors mean that the ethnic diversity of ASIO's workforce remains below APS levels.

Figure 12 compares age profiles of staff members in this reporting period with those from the last three years.

Figure 12: Age of staff

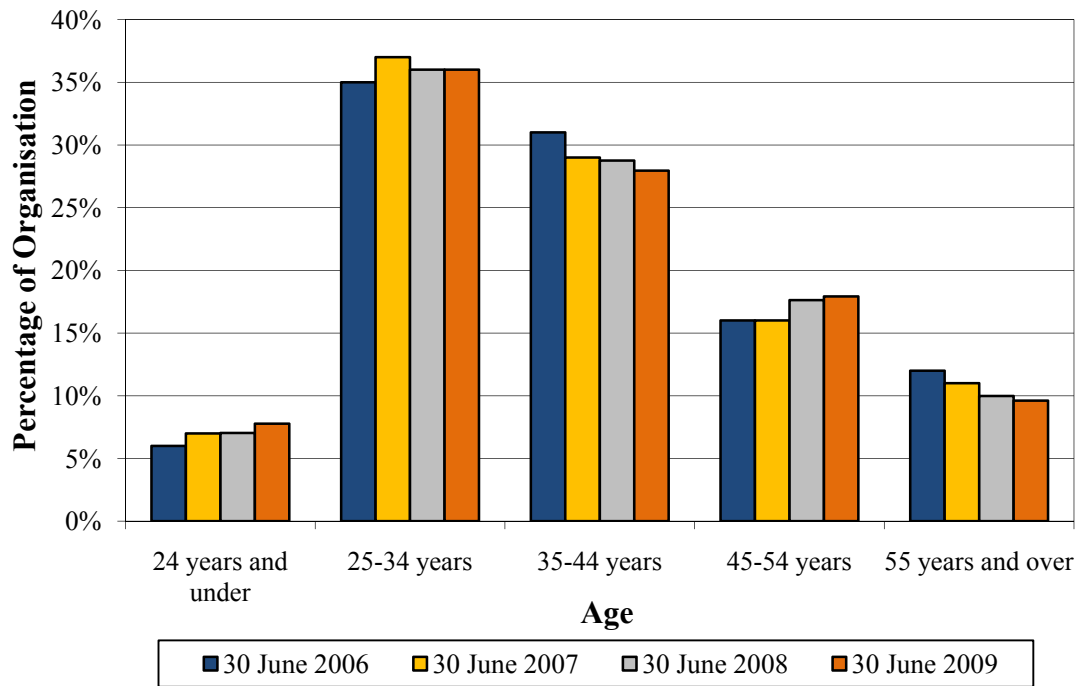
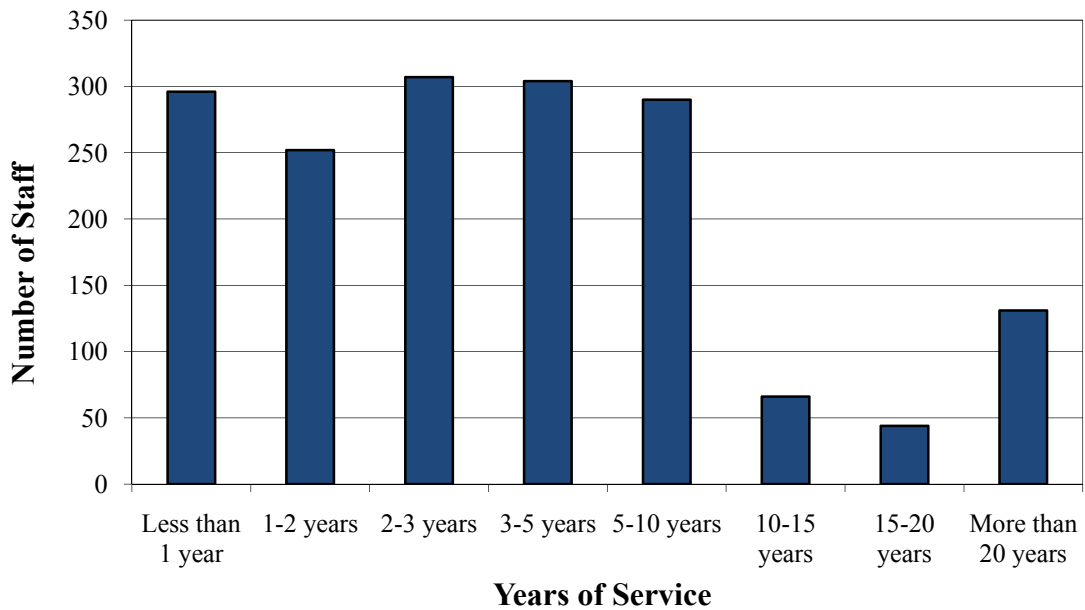


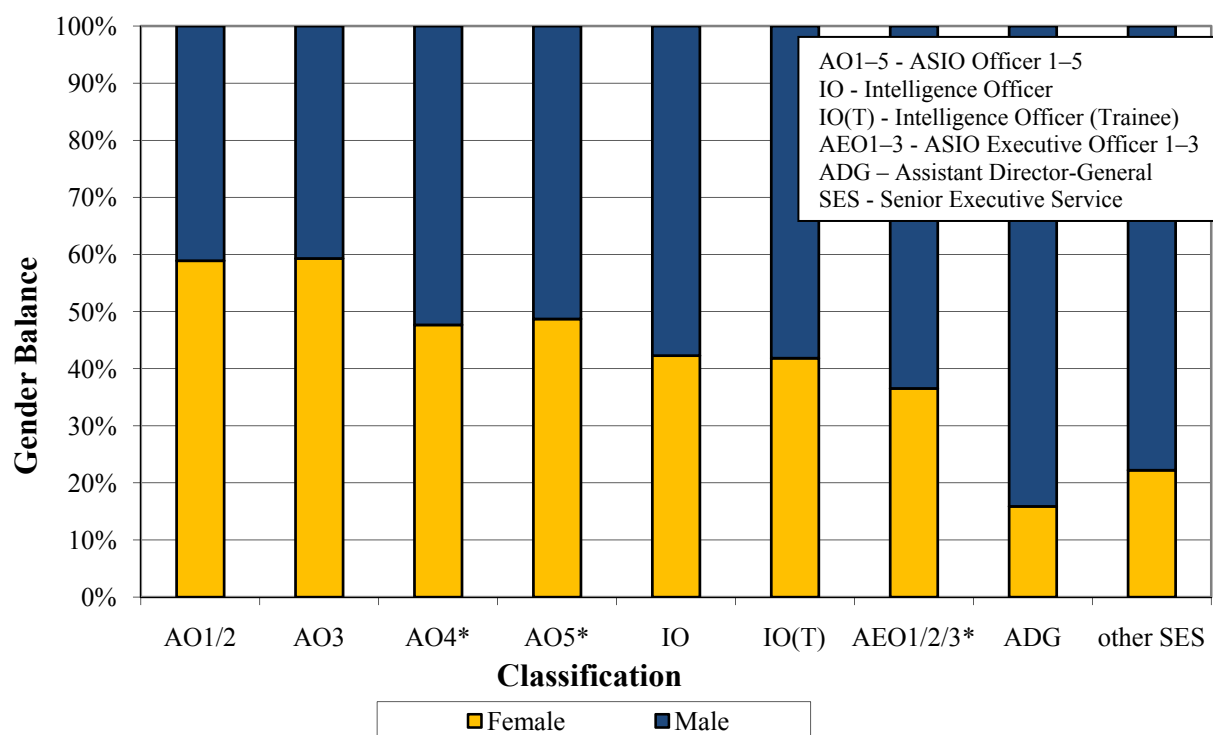
Figure 13: Length of Service of ASIO staff



While women now make up 45 percent of ASIO’s workforce – an improving trend – they remain under-represented in the Senior Officer (37 percent) and Senior Executive Service (18 percent) ranks compared to the APS norms (46 percent and 37 percent respectively).

Figure 15 provides a breakdown of gender by classification.

Figure 14: Gender balance by classification



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

### STAFF COMPLAINTS

Three formal grievances were lodged in 2008–09. Outcomes of the formal grievances processes were concluded without the need for formal proceedings to be initiated. A number of matters were raised informally with Harassment Contact Officers, Human Resource Management Section and the Organisation’s Ombudsman; all informal matters were also resolved without the need for formal proceedings to be initiated.

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

ASIO continued to train and develop its network of Harassment Contact Officers. Nominated officers participated in a two-day training program delivered by a specialist external provider. An internal Harassment Contact Officer Newsletter continues to operate to ensure another means of communication is available to the network.

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

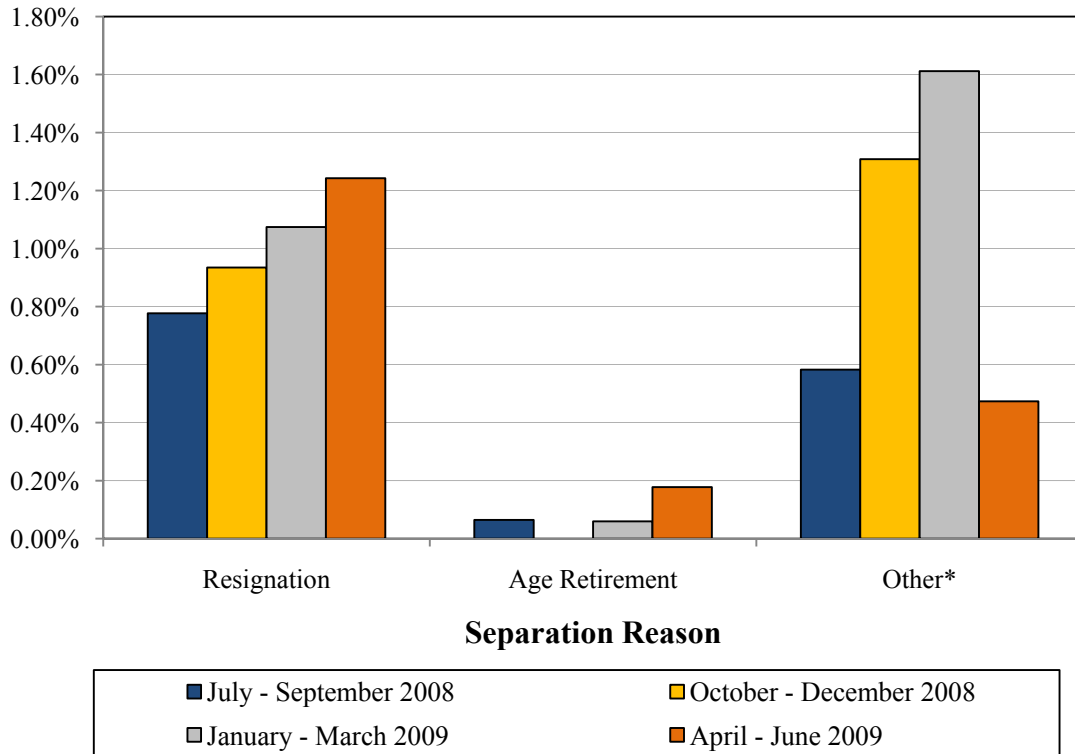
### SEPARATION RATES

ASIO’s separation rate for 2008–09 decreased to 4.5 percent compared with 7.6 percent in 2007–08. This compares favourably with seven percent across the APS in 2008–09 and



provides an acceptable level of turnover while retaining skilled and experienced staff.

**Figure 15: Separations by percentage of total staff and reason**



\* Includes contract expiries, early cessation of contracts and end of secondment/consultancies.

Separating staff members can participate in a voluntary exit interview in order to track reasons for separation and address concerns requiring a management response. Approximately half of all separating staff choose to participate in the exit interview. Reasons cited by separating staff include promotion/career opportunities, work/life balance issues, job satisfaction issues, retirement and a range of personal reasons. The exit interview process did not reveal any systemic concerns requiring management response.

# ACCOMMODATION

---

## CENTRAL OFFICE, CANBERRA

In 2007–08, the Government approved a new special-purpose, high-security building for ASIO. In 2008–09, the Government approved a budget of \$606m. The new building is being designed and constructed in partnership with the Department of Finance and Deregulation (Finance). While the Office of National Assessments (ONA) was originally to share the building, in mid-2009, the Government agreed to ONA withdrawing from the project to pursue commercially leased accommodation. The project budget was subsequently reduced to \$589m.

Site establishment works commenced in March 2009 and excavation works commenced in July 2009. Occupation of the building is expected in late 2012. The location is Section 49, Parkes, within the Parliamentary Triangle and in close proximity to the Russell precinct and partners in the AIC and broader national security community. The building will be in keeping with the National Capital Plan and the Griffin Legacy (under guidance of the National Capital Authority) and includes elements of environmentally sustainable design. The building will meet ASIO's future needs, with a design concept that integrates form and function.



**Artist rendering of the Front Façade from Constitution Avenue.**

The building will accommodate up to 1,800 people and will operate 24 hours per day, with a level of security commensurate with ASIO's intelligence functions and in accordance with Australian and international security accreditation standards. The design of the built space and infrastructure will allow for future growth in information and communication technology, technical capabilities, and for life cycle accommodation changes to be delivered. The inclusion of redundancy in the design of the building services and structural resilience will enable ASIO to continue operating in the event of utility outages or physical attacks. The new work environment encompasses open plan work areas, purpose designed technical workspaces, a data centre, training areas and staff amenities. Incorporated into the design will be natural light and other amenities to enhance its appeal as an attractive workplace.

## UNCLASSIFIED

The building is being designed to achieve a 5 star energy rating for the base building in accordance with the National Australian Built Environment Rating System (NABERS). Environmental design features will include:

- photo voltaic cells (solar panels) located on the roof and a co-generation plant utilising natural gas to generate electricity for use within the building;
- energy efficient lighting;
- an 'active ventilation system' which will provide venting of heat during the summer months and further insulation during winter;
- air conditioning with 100 percent fresh air at floor level for a healthier work environment;
- the harvesting of storm water for use in landscaping, irrigation and toilet flushing; and
- opportunity for the adoption of improved waste minimalisation and recycling practices.

In October 2008, the planning phase was completed which included the development of the functional design brief, concept design and cost plan. On 24 November 2008, Bovis Lend Lease, the managing contractor, entered into the delivery phase contract with the Commonwealth. The delivery phase encompasses the detailed design documentation and construction of the building. GHD, the project consultant, continues to provide construction program oversight on behalf of the Commonwealth.

During 2009, local residents raised a number of concerns including whether the relevant planning processes had been followed. In response, the National Capital Authority (NCA) confirmed publicly that approvals had been given in accordance with the National Capital Plan.

In March 2009, Finance lodged an Environmental Protection and Biodiversity Conservation (EPBC) referral with the Department of the Environment, Water, Heritage and the Arts (DEWHA). The referral included a Heritage Impact Assessment and DEWHA confirmed in April that the development is a 'non-controlled' action. This means the proposed works do not have any restrictions placed on them.

Information on the progress of the project is regularly provided to the public through:

- the ASIO and NCA websites ([www.asio.gov.au](http://www.asio.gov.au) and [www.nationalcapital.gov.au](http://www.nationalcapital.gov.au));
- regular briefings to the commercial neighbours including Defence, ACT Department of Territory and Municipal Services, actewAGL, Action buses, etc.;
- letterbox drops to residents; and
- a hotline to take enquiries from the public and media.

The project is progressing within budget and on program for occupation in late 2012.

### **EXEMPTION FROM THE PUBLIC WORKS COMMITTEE**

The Governor-General granted ASIO's New Building Project an exemption from scrutiny by the Parliamentary Standing Committee on Public Works because of the high security nature of the building.

Detailed enquiries could lead to public disclosure of sensitive information regarding the building's protective security features. In the public arena, this information would be of particular interest to hostile intelligence services and, potentially, terrorist groups. This would be prejudicial to national security and contrary to the public interest.

On 4 December 2008, ASIO and the Department of Finance and Deregulation provided a confidential briefing to the Parliamentary Standing Committee on Public Works. Further confidential briefings will be offered to the Committee as the Project progresses.

## **STATE AND TERRITORY OFFICES**

The need to accommodate additional staff, undertake increased operational activities and refresh ageing facilities, has led to the establishment of an integrated property upgrade program.

During 2008–09 significant progress was made in upgrading accommodation as a result of funding received in 2006–07 and 2007–08, including the reconfiguration and relocation of a number of ASIO offices, including the reconfiguration of the current ASIO central office in 2009.

ASIO is on track to finalise the current funded reconfiguration and relocation program by the end of 2009–10.

# PUBLIC RELATIONS AND REPORTING

---

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

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

## **ASIO'S REPORT TO PARLIAMENT**

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

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

## **PARLIAMENTARY OVERSIGHT**

In addition to Parliamentary oversight by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), ASIO's activities are overseen by the:

- Senate Standing Committee on Constitutional and Legal Affairs as part of the Senate Budget Estimates process; and
- Senate Finance and Public Administration Committee.

In 2008–09, ASIO responded to six Questions on Notice from both Houses of Parliament.

## **PUBLIC STATEMENTS**

Public comments about the activities of ASIO may be provided by the Attorney-General, as ASIO's Minister, the Director-General of Security, or ASIO's Media Liaison Officer (MLO).

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

ASIO does not comment to the media on sensitive national security matters. It does, however, respond to general media enquiries through the MLO. In 2008–09, ASIO expanded its contact with journalists and the media, including through interviews on recruitment matters.

In 2008–09, the Director-General of Security addressed conferences and audiences from business, government and academia. Nine of these speeches are available on the ASIO

website.

The ASIO website is the primary source of public information about ASIO. It was updated frequently throughout 2008–09, including with transcripts of the Director-General of Security’s speeches, and job vacancies. The website also provides publications such as ASIO’s *Reports to Parliament* and its *Corporate Plan 2007–2011*.

The website also provides links to related sites including the Attorney-General, the PJCS, the Inspector-General of Intelligence and Security (the IGIS) and other members of the Australian Intelligence Community (AIC).

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

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

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

- use of special powers under warrant;
- access to and use of Australian Transaction Reports and Analysis Centre and Australian Taxation Office information;
- compliance with the Archives Act 1983;
- liaison with, and provision of information to, law enforcement agencies;
- provision of information on Australian persons to foreign liaison partners;
- inspections of ASIO’s internal approvals of investigations;
- inspections of ASIO’s interception management systems;
- authorisations for access to prospective telecommunications data; and
- retrospective inspections of selected ASIO operations.

Based on the various monitoring, inspection and inquiry activities undertaken by the Office of the IGIS in 2008–09, the IGIS was satisfied that there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or human rights. Further details can be found in the IGIS’s Annual Report at [www.igis.gov.au](http://www.igis.gov.au).