PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY:

REVIEW OF ADMINISTRATION AND EXPENDITURE NO 9: 2009–10

ASIO Submission

CONTENTS

FIGURES

TABLES

ASIO'S ROLE AND FUNCTIONS

The Australian Security Intelligence Organisation (ASIO) is Australia's security service. It is a critical component of Australia's national security community and deals with threats to Australia's security. ASIO's role and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). The *Anti-People Smuggling and Other Measures Act 2010*, which commenced on 1 June 2010, amended the definition of 'security' in the ASIO Act, enabling ASIO to use its existing capabilities to respond to people smuggling and other serious threats to Australia's territorial and border integrity.

ASIO's primary function is to collect, analyse and disseminate security intelligence. For this, the ASIO Act defines 'security' as the protection of Australia, its people and interests against:

- espionage;
- sabotage;
- politically motivated violence;
- the promotion of communal violence;
- attacks on Australia's defence system;
- acts of foreign interference; and
- serious threats to Australia's territorial and border integrity.

The ASIO Act extends ASIO's responsibility for security intelligence beyond Australia's borders and includes, in the definition of security, Australia's 'security' obligations to other countries. The ASIO Act also specifically authorises ASIO to communicate and cooperate with relevant authorities of foreign 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 the Attorney-General;
- assesses intelligence and provides advice to Government, including in the form of Threat Assessments;
- investigates and responds to threats to security;
- maintains a national counter-terrorism capability; and
- provides Security Assessments, including for visa applicants and for access to classified material and designated security-controlled areas.

Under the ASIO Act and other legislation, ASIO can be authorised to use more intrusive powers under warrant. These include the interception of telecommunications, entering and searching premises, and compelling persons to appear before a prescribed authority to answer questions relating to terrorism matters. ASIO also has specialist capabilities that can be deployed to assist in intelligence operations and incident response.

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

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. 9 provides a detailed account of ASIO's activities during 2009–10 covering:

- legislative changes, including:
    - the frequency and nature of the use of ASIO's special powers, including the amount of time expended on particular areas; and
    - the implications of legislative changes on staffing, training, the role of legal officers, the need for specialist staff, and ASIO's relationship with outside agencies such as the police and the judiciary.
- an update on ASIO's human resource management, including recruitment; retention; training; workplace diversity; language skills; staff complaints; separation rates and accommodation;
- ASIO's organisational structure and the distribution of staff across different areas of the Organisation, including the ratio of field and operational staff to administrative staff; the ratio of executive to middle and lower level staff and the ratio of central office staff to outlying staff;
- ASIO's response to the pressures of expansion;
- security clearances, including an overview of current procedures, timelines, delays and associated outsourcing arrangements;
- security breaches, including e-security arrangements and enhancements;
- public relations and reporting;
- direction and strategic planning, including the management of expansion; and
- performance management and evaluation.

The submission also provides an account of:

- areas of interoperability between the Australian Intelligence Community (AIC) and other relevant agencies;
- e-security arrangements underpinning this interoperability;
- Memoranda of Understanding providing the basis for interoperability; and
- accommodation requirements resulting from interoperability arrangements.

THE SECURITY ENVIRONMENT 2009–10 AND OUTLOOK

Two key events in the reporting period highlighted the persistent threat of terrorism. Within Australia, a major counter-terrorism investigation culminated in the arrest of five individuals on terrorism-related charges. Offshore, three Australians were killed in Jakarta during an attack on the JW Marriott Hotel in July 2009.

The protection of Australia from espionage also became more complex with globalisation and rapid technological advances. ASIO continued to build on relationships with government,

business and industry to raise awareness and promote security. Traditional forms of espionage also continued to be employed by foreign services attempting to access information.

Countering proliferation remained an international security challenge and ASIO continued to work with both domestic and international partners against the activities of foreign states that seek to gain materials or knowledge used to develop weapons of mass destruction.

EXPENDITURE

For the reporting period, ASIO received funding from the Australian Government for the outcome 'security intelligence for Australia and its interests – locally and internationally – through intelligence collection and advice that counters politically motivated violence, espionage, foreign interference, communal violence, sabotage, and attacks on the defence system'.

Funding to ASIO expressed in terms of total price of program expenses was $368m, an increase of five per cent from the total cost in 2008–09 of $352m. The estimated total cost for program expenses for 2010–11 is $413m, an increase of twelve per cent from 2009–10.

2009–10 was the last year of growth arising from the *Review of ASIO Resourcing* conducted by Mr Allan Taylor AM in 2005, and the end of consequential substantial funding increases to meet the additional staffing, operating and depreciation expenses.

STRUCTURE OF THE ORGANISATION

In 2009–10, ASIO's Senior Management group reviewed the Organisation's structure to position ASIO to meet future challenges through improving efficiency and functional alignment. The review of the structure was driven by ASIO's response to an evolving security environment as well as changes to ASIO's legislation, and occurred in parallel with work being undertaken as part of ASIO's strategic agenda.

ASIO's new structure involved a move from twelve to ten divisions, and was designed to achieve a more efficient allocation of resources, with better alignment of staff skills and work unit functions resulting in an overall enhancement of organisational performance. It better equips ASIO to contribute to a more broadly focused and interconnected national security community.

The new structure will be implemented on 1 July 2010.

DIRECTION AND STRATEGIC PLANNING

In 2009–10, ASIO embarked on a comprehensive program of strategic business review and reform. The program has two overarching objectives – to ensure ASIO is working effectively and efficiently to meet its responsibilities, priorities, and tasking; and working effectively and cooperatively as part of the broader national security community.

Outcomes of ASIO's strategic work program in 2009–10 included:

- a detailed examination of ASIO's operational and investigative processes and procedures to reduce administrative overhead and maximise intelligence outcomes;
- the implementation of ASIO's new Leadership Development Strategy;
- the development of a People Capability Framework to support and guide workforce management and strategic workforce planning;
- streamlining of visa security checking processes through an enhanced risk management methodology;
- the rationalisation of ASIO's intelligence product lines;
- review of ASIO's information management and Information Technology (IT) systems, including the development of an Information Sharing Business Model, with a view to ensuring that information and data is always accessible to those who need it, when they need it; and
- the review and implementation of an enhanced approach to training and developing intelligence officers that supports greater engagement with AIC partner agencies and academia.

In 2009–10, ASIO also improved its ability to work effectively and collaboratively within the national security community, including through the establishment of the Counter Terrorism Control Centre, and commencing a pilot study for the establishment of the National Interception Technical Assistance Centre.

LIAISON WITH FOREIGN SERVICES, BUSINESS AND THE COMMUNITY

ASIO continued to expand its liaison relationships in 2009–10. At 30 June 2010, ASIO had 329 approved liaison relationships with security, intelligence and law enforcement agencies in 123 countries around the world.

ASIO's Business Liaison Unit (BLU) website was upgraded during the reporting period, with improved functionality for users. At the end of the reporting period there were more than 200 reports on the BLU website. As at 30 June 2010, there were 778 subscribers to the BLU website, covering 227 corporations and a range of government agencies – an increase of 33 per cent since 2008–09.

ASIO's 2009–10 Client Survey was expanded to include respondents at Executive Level 2 and Australian Government clients located at overseas posts. ASIO's relationships with clients were viewed as generally positive and the Organisation's reporting product was regarded highly. Some Commonwealth customers noted a significant improvement in their engagement with ASIO, citing Partnership Forums and other relationship building activities as key to that improvement.

LEGISLATION AND LITIGATION

In 2009–10, ASIO continued to work collaboratively with other Commonwealth departments and agencies on policy development and proposed legislative amendments to ensure that the legislative framework supports ASIO's functions and capabilities. A number of legislative developments relevant to ASIO occurred during the reporting period, including:

- the *Anti-People Smuggling and Other Measures Act 2010;*
- the *Crime Legislation Amendment (Serious and Organised Crime) Act 2010;* and
- the *Tax Laws Amendment (2010 Measures No. 3) Act 2010.*

In 2009–10, ASIO was involved in over 40 litigation matters, including criminal (in particular terrorism) prosecutions, judicial and administrative review of Security Assessments, and a range of civil actions. Particularly complex litigation proceedings to which ASIO contributed include the Sydney and Melbourne Pendennis and Operation NEATH terrorism prosecutions.

ASIO was also involved directly in two legal matters initiated by Mr Mamdouh Habib, a number of challenges to its Security Assessments, and former ASIO officer James Seivers's appeal against his conviction for the unauthorised communication of intelligence.

SECURITY OF ASIO

The information held by ASIO is often highly sensitive in nature and, if compromised, has the potential to damage Australia's national security. These serious ramifications necessitate the need for stringent security practices at both the organisational level and also for each member of ASIO staff.

In the reporting period, ASIO continued to bolster security at ASIO's central office with the introduction of biometric measures to access the building. ASIO also updated internal security instructions documenting sound security practices and requirements for all ASIO staff.

The protection of information held by ASIO is ultimately the responsibility of every member of ASIO staff. For this reason all ASIO permanent staff must maintain a security clearance of Top Secret. In the reporting period ASIO conducted 291 probation revalidations and 149 full re-evaluations.

ASIO SECURITY ASSESSMENTS

During 2009–10 ASIO provided security assessment advice for Government consideration in a range of decision-making processes:

- ASIO conducted 38,438 visa Security Assessments and a further 989 assessments for protection visa applicants. Nineteen adverse assessments were made in relation to visas;
- ASIO issued adverse Security Assessments in respect of the Australian passports of eight individuals;

- ASIO completed 22,343 personnel Security Assessments; and
- ASIO conducted 98,086 counter-terrorism Security Assessments. These include assessments for aviation/maritime security identity cards and access to restricted areas and/or sensitive goods.

During the reporting period, ASIO prioritised assessments for Irregular Maritime Arrivals (IMAs) and individuals in detention. This affected the time taken for assessments for protection visa applicants not currently in detention, which were being managed by the same work area. ASIO has since quarantined resources to address the backlog in protection visa Security Assessments.

HUMAN RESOURCE MANAGEMENT

Despite a low attrition rate, employment market conditions combined with the necessarily stringent and lengthy security vetting of potential new staff meant ASIO did not reach its ambitious recruitment targets for the year. ASIO's recruitment focus was on the more specialised areas of intelligence analysis and collection, where ready-made expertise is rare and must be taught in-house.

Lower than anticipated staffing levels and the decision to defer some expenditure to align better with the timing of ASIO's new building resulted in ASIO returning a budget surplus. Recruitment will continue to be a priority for the forthcoming year, with new people management strategies developed to assist in meeting the higher net recruitment targets necessary to build and sustain a more effective national security intelligence capability.

In November 2009 the Staff and Family Liaison Office was launched as one of the first implemented initiatives under ASIO's strategic agenda reform. The Office is managed by a qualified social worker to provide an integrated model of wellbeing services that meets the needs of staff and families while supporting the Organisation's requirements.

ACCOMMODATION

The construction of ASIO's new central office in Canberra is progressing on schedule and is expected to be completed in 2012, with the main relocation of ASIO staff to commence in late 2012.

In the 2008–09 Budget the Australian Government approved $606m for the construction of ASIO's new central office in Canberra. In 2009–10 this was reduced to $589m when the Office of National Assessments, a proposed subtenant, withdrew from the project to pursue alternative leased accommodation.

Given the nature of the security environment and the pace of technological change, it is inevitable that some capability will need to be added to the new central office as construction and fit-out progress. Funding for new capability will need to be committed from ASIO's ongoing appropriation in the next two years. ASIO has developed a range of plans to limit the impact of this expenditure on ASIO's core capabilities, such as examining which current assets can be migrated into the new central office.

PUBLIC RELATIONS AND REPORTING

During 2009–10, ASIO continued to implement initiatives to improve accessibility and contact points into ASIO. In 2010, the Director-General of Security decided, under the provisions of the ASIO Act, to reveal publicly the identity of one of ASIO's Deputy Directors-General, Mr David Fricker.

Throughout the reporting period, ASIO engaged in outreach activities to promote understanding of ASIO's unique role, to highlight challenges in the security environment, and to contribute to broader policy considerations and debate. The audience included Commonwealth and state and territory partners through initiatives such as Partnership Forums; academia through seminars; as well as the wider community through ASIO's new website. The redeveloped website was launched by the Attorney-General, the Hon. Robert McClelland MP, on 12 March 2010, and provides easy-to-access information across a range of topics, including broad details on the nature of ASIO's work.

THE SECURITY ENVIRONMENT 2009–10 AND OUTLOOK

TERRORISM

The Middle East remains a primary source of motivation and capability for extremists in Australia. However, South Asia, South-East Asia and East Africa continue to be key regions for Islamist terrorist activity. In particular, concern is growing about the entrenched terrorism threat emanating from Yemen.

ASIO's counter-terrorism investigations over the reporting period revealed the re-emergence of the trend of Australians aspiring or planning to travel overseas for terrorism-related activity, including training and terrorist operations.

On 17 July 2009, three Australians were killed in Jakarta during an attack on the JW Marriott Hotel. This, along with the attempted bombing of Northwest Airlines flight 253 on Christmas Day 2009, highlighted the proximity and endurance of the threat posed by terrorism.

ESPIONAGE AND FOREIGN INTERFERENCE

Espionage is a constant in the international threat environment and draws increasingly on ASIO's resources. Technological developments present foreign states and non-state actors with greater opportunities to access and exploit electronic information systems remotely. ASIO works with the government and business and industry sectors to raise awareness and promote appropriate security against cyber intrusion and exploitation. In January 2010, a multi-agency initiative was established to coordinate work against the threat. The Cyber Security Operations Centre (CSOC) was established in the Defence Signals Directorate (DSD) in 2009 as an initiative of the *Defence White Paper* to coordinate work against this threat. Personnel from ASIO, the Attorney-General's Department and the Australian Federal Police (AFP) are embedded within the Centre.

COMMUNAL VIOLENCE AND VIOLENT PROTEST

There was little violent protest activity within communities in Australia in 2009–10.

ASIO observes the provisions of section 17A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), which protects the right of persons to engage in lawful advocacy, protest or dissent. ASIO does not target particular groups or individuals, unless there is a security-related reason to do so — it is behaviour and activity that directs ASIO's interest.

The promotion of communal violence, meaning activities directed at promoting violence between different groups of persons in the Australian community so as to endanger the peace, order or good government of the Commonwealth, is an area of security specifically defined in the ASIO Act and is, therefore, of interest to ASIO. ASIO continues to utilise its Community Contact Program to enhance community leaders' understanding of ASIO's role and functions, particularly as it relates to violent protest activity. In 2009–10, ASIO maintained a dialogue with

representatives of community, ethnic and religious groups to ensure issues of concern to ASIO and the relevant community groups could be aired and discussed directly and discreetly.

ASIO continues to liaise closely with law enforcement agencies and will continue to assess possible threats to the community that may arise through the incitement or promotion of communal violence.

PROLIFERATION

ASIO's counter-proliferation work focuses on thwarting the efforts of countries or individuals of proliferation concern accessing weapons of mass destruction (WMD) technology and materials.

Australia supports international efforts to prevent the spread of WMD and participates in major arms control treaties and multilateral export control regimes. Australia is a signatory to the United Nations Security Council Resolution 1540 which requires states to criminalise the proliferation of WMD, enact strict export controls and secure sensitive materials.

BORDER SECURITY

ASIO engaged with its domestic partners to prevent harm to Australian interests by preventing entry to Australia by people assessed to be a threat to security.

In recognition of ASIO's key role in Australia's border security arrangements, new legislation (*Anti-People Smuggling and Other Measures 2010)*, which came into effect in June 2010 paved the way for ASIO to contribute to the whole-of-government effort to maintain border security.

In 2009–10, ASIO completed 38,438 visa Security Assessments (compared with 59,884 in 2008–09) including 989 assessments for protection visa applicants.

ASIO issued adverse Security Assessments for nineteen individuals seeking entry to Australia in 2009–10. Fourteen of these adverse assessments were issued on counter-terrorism grounds and five were issued on espionage or foreign interference grounds.

OUTLOOK FOR THE SECURITY ENVIRONMENT

Terrorists will continue to target Australia for the foreseeable future. Al-Qa'ida-affiliated groups and others inspired by similar ideology are likely to be the primary source of terrorism threats to western lives and interests for years to come.

ASIO's investigative and operational activity has shown consistently that overseas drivers and links remain central to the threat to Australia. Australians travel and live in all corners of the globe, and Australian interests – government, business and industry – are also scattered widely, including in locations with volatile and unpredictable security environments such as Pakistan and Afghanistan. This provides opportunity for those seeking to target Australia. At the same time, concerns are growing at the rise of 'homegrown' potential terrorists and an increase in the number of Australians seeking to travel overseas for terrorism-related purposes.

Australia and Australian interests will continue to be a target of espionage or foreign interference. Technological developments will present foreign states and non-state actors with greater opportunities to access and exploit electronic information systems remotely. However, traditional methods, such as cultivating the cooperation of Australian citizens in positions of access or influence, will also continue.

The majority of Australia's issue motivated groups will continue to use peaceful and non-violent means of protest. ASIO assesses a small number of activists believe violent protest is a legitimate and effective means of influencing government and business decision-makers, and are likely to plan violent protest activities during anti-war, anti-globalisation and climate change protests. ASIO maintains close liaison with law enforcement agencies and will continue to assess possible threats to the community that may arise through the incitement or promotion of communal violence.

The ambitions of some states to obtain WMD will continue to threaten global security. For several reasons, including Australia's technologically advanced industry and military, strategic alliances and world class education facilities, Australia will remain of interest to these states.

ASIO expects the need for counter-proliferation intelligence support for regulatory and enforcement agencies to continue.

EXPENDITURE

BUDGET GROWTH

In 2009–10, ASIO received funding from the Australian Government for the outcome 'security intelligence for Australia and its interests – locally and internationally – through intelligence collection and advice that counters politically motivated violence, espionage, foreign interference, communal violence, sabotage, and attacks on the defence system'.

ASIO delivers and reports to the Australian Government against four program components of the outcome:

- Security Intelligence Analysis and Advice;
- Protective Security Advice;
- Security Intelligence Investigation and Capabilities; and
- Foreign Intelligence Collection.

Funding to ASIO expressed in terms of total price of program expenses was $368m, an increase of five per cent from the total cost in 2008–09 of $352m. The estimated total cost for program expenses for 2010–11 is $413m, an increase of twelve per cent from 2009–10.

Revenue from Government in 2009–10 increased 15 per cent to $406m, while revenue from independent sources (such as for services rendered) was similar to the 2008–09 figure of $10m.

This reporting period saw the last year of growth arising from the *Review of ASIO Resourcing* by Mr Allan Taylor AM, and the end of consequential substantial funding increases to meet the additional staffing, operating and depreciation expenses.

Separately, ASIO received an equity injection of $16m for 2009–10, to fund telecommunications interception capabilities ($2m) and capability enhancements ($14m).

ASIO achieved efficiency savings, including through the identification and elimination of duplication created during the period of sustained growth and the refinement of resource allocation and management across priorities.

A further equity injection will be received in 2010–11 of $89m. This provides funding for asset replacement ($28m) and for ASIO's new building project ($61m).

FIGURE 1: REVENUE FROM GOVERNMENT 2002–13
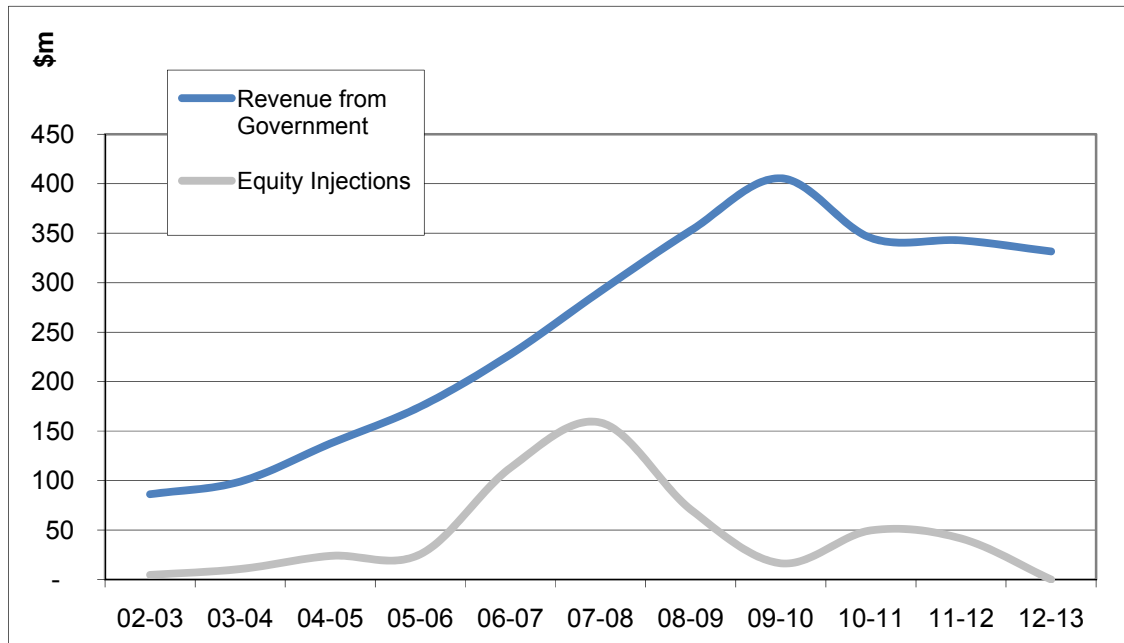
Note: The reduction in funding from 2010–11 onwards is a consequence of the Government's introduction of *Net Cash Funding* and the removal of depreciation funding, and does not, per se, have an impact on ASIO's level of activity.

FINANCIAL PERFORMANCE

ASIO recorded a budget surplus in 2009–10 of $39m. Lower than anticipated staffing levels, the decision to defer some expenditure to better align with the timing of ASIO's new building and an actuarial adjustment contributed to this outcome.

FIGURE 2: FINANCIAL PERFORMANCE 2002–13
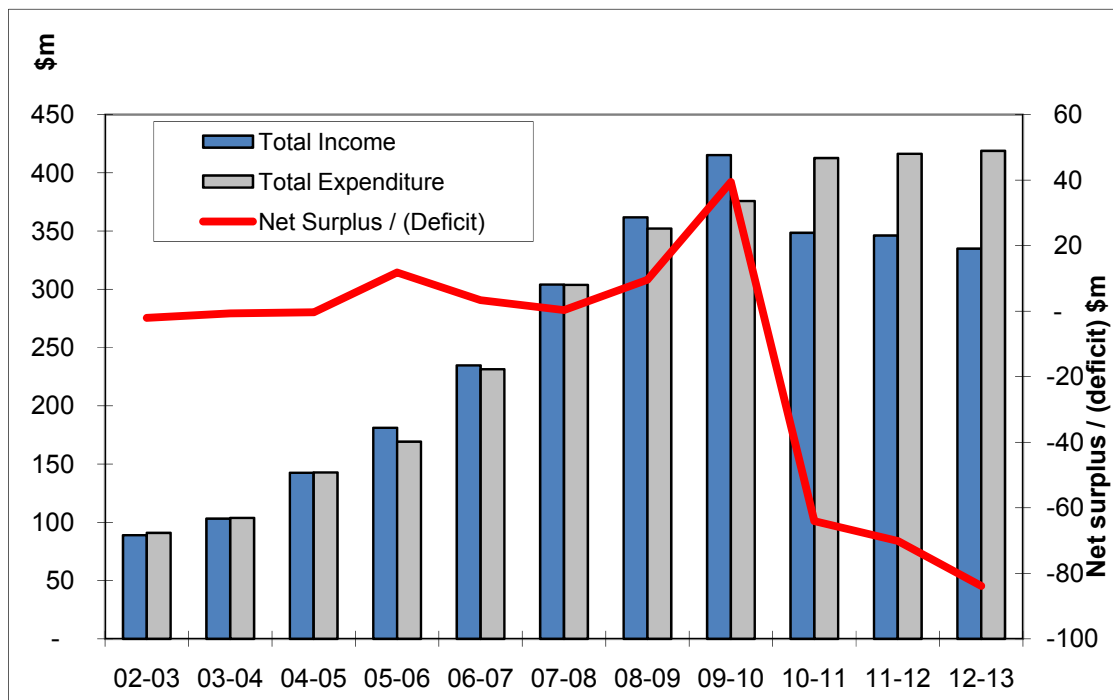
Note: The budgeted deficits commencing from 2010–11 are a consequence of the Government's introduction of Net Cash Funding and the removal of depreciation funding. Excluding depreciation expense, ASIO is budgeting for breakeven results from 2010–11 onwards.

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 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. The 2010–11 financial year will see ongoing resource allocation analysis to ensure ASIO continues to deliver outcomes to Government effectively.

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

In 2009–10, ASIO's organisational structure was reviewed to ensure ASIO was positioned to meet future challenges. The review of the structure was driven by ASIO's response to an evolving security environment as well as recent changes to ASIO's legislation and occurred in parallel with work being undertaken as part of ASIO's strategic agenda.

The new structure will be implemented on 1 July 2010.

FIGURE 3: ASIO ORGANISATIONAL STRUCTURE AT 1 JULY 2009

Director-General of Security
David Irvine

Deputy Director-General

Deputy Director-General

Deputy Director-General (left branch)

First Assistant Director-General — Investigative Analysis & Advice
- Assistant Director-General — Middle East & Africa
- Assistant Director-General — Australia, Pacific, Asia, Europe & Americas
- Assistant Director-General — Terrorism Litigation Advice
- Assistant Director-General — Leads

First Assistant Director-General — Collection
- First Assistant Director-General — NSW
- Assistant Director-General — Victoria
- Assistant Director-General — Central
- Assistant Director-General — Counter-Terrorism Investigations

First Assistant Director-General — Support to Operations
- Assistant Director-General — Surveillance
- Assistant Director-General — Operational Services

First Assistant Director-General — Counter-Espionage & Interference
- Assistant Director-General — Counter-Espionage
- Assistant Director-General — Foreign Interference
- Assistant Director-General — Foreign Intelligence Support

First Assistant Director-General — Technical Capabilities
- Assistant Director-General — TI Capabilities
- Assistant Director-General — T&I Operations
- Assistant Director-General — Technical Operations

First Assistant Director-General — Legal
- Assistant Director-General — Litigation Branch A
- Assistant Director-General — Litigation Branch B
- Assistant Director-General — Legal Advice
- Assistant Director-General — Operations Counsel Group

Deputy Director-General (right branch)

First Assistant Director-General — Security
- Assistant Director-General — Counter-Intelligence & Security
- Assistant Director-General — Protective Security
- Assistant Director-General — Security Assessments

First Assistant Director-General — Strategic Intelligence & Liaison
- Assistant Director-General — National Threat Assessment Centre
- Assistant Director-General — Strategic Analysis
- Assistant Director-General — International Engagement & Reporting

Chief Information Officer — Information
- Assistant Director-General — IT Infrastructure Services
- Assistant Director-General — Business Information Systems
- Assistant Director-General — Information Services

First Assistant Director-General — Corporate Management
- Assistant Director-General — People
- Assistant Director-General — Training
- Chief Finance Officer — Finance

First Assistant Director-General — Property
- Assistant Director-General — Accommodation
- Assistant Director-General — New Building

First Assistant Director-General — Executive
- Assistant Director-General — Government Relations
- Assistant Director-General — Corporate Governance
- Assistant Director-General — Corporate Strategy

First Assistant Director-General — National Security Executive Development Program

FIGURE 4: ASIO ORGANISATIONAL STRUCTURE AT 1 JULY 2010

Director-General of Security
David Irvine

Deputy Director-General Operations and Assessments

Deputy Director-General Corporate and Strategy

COUNTER INTELLIGENCE

INTERNAL AUDIT

FIRST ASSISTANT DIRECTOR-GENERAL COUNTER TERRORISM CONTROL CENTRE

OPERATION EVALUATION

STATE AND TERRITORY MANAGERS

Security, Strategy and Engagement
FIRST ASSISTANT DIRECTOR-GENERAL SECURITY, STRATEGY AND ENGAGEMENT
- ASSISTANT DIRECTOR-GENERAL INTERNAL SECURITY
- ASSISTANT DIRECTOR-GENERAL GOVERNANCE STRATEGY
- ASSISTANT DIRECTOR-GENERAL STRATEGIC COMMUNICATIONS & ENGAGEMENT

Corporate Capability & Services
FIRST ASSISTANT DIRECTOR-GENERAL CORPORATE CAPABILITY & SERVICES
- ASSISTANT DIRECTOR-GENERAL PEOPLE STRATEGY AND SERVICES
- ASSISTANT DIRECTOR-GENERAL PEOPLE DEVELOPMENT
- ASSISTANT DIRECTOR-GENERAL RESOURCE MANAGEMENT
- ASSISTANT DIRECTOR-GENERAL PROPERTY MANAGEMENT AND PROTECTION
- ASSISTANT DIRECTOR-GENERAL NEW BUILDING

Information
CHIEF INFORMATION OFFICER INFORMATION
- ASSISTANT DIRECTOR-GENERAL INFORMATION SERVICES
- ASSISTANT DIRECTOR-GENERAL IT INFRASTRUCTURE SERVICES
- ASSISTANT DIRECTOR-GENERAL BUSINESS INFORMATION SYSTEMS

Legal
FIRST ASSISTANT DIRECTOR-GENERAL LEGAL
- ASSISTANT DIRECTOR-GENERAL LEGAL ADVICE & WARRANTS
- ASSISTANT DIRECTOR-GENERAL LITIGATION-GENERAL
- ASSISTANT DIRECTOR-GENERAL LITIGATION NSW
- ASSISTANT DIRECTOR-GENERAL OPERATIONS COUNSEL GROUP

Assessment
FIRST ASSISTANT DIRECTOR-GENERAL ASSESSMENT
- ASSISTANT DIRECTOR-GENERAL NATIONAL THREAT ASSESSMENT CENTRE
- ASSISTANT DIRECTOR-GENERAL PROTECTIVE SECURITY
- ASSISTANT DIRECTOR-GENERAL STRATEGIC ANALYSIS

Investigative Analysis
FIRST ASSISTANT DIRECTOR-GENERAL INVESTIGATIVE ANALYSIS
- ASSISTANT DIRECTOR-GENERAL MIDDLE EAST & AFRICA
- ASSISTANT DIRECTOR-GENERAL ASIA/PACIFIC, AUSTRALIA, EUROPE & AMERICAS
- ASSISTANT DIRECTOR-GENERAL SECURITY ASSESSMENTS
- ASSISTANT DIRECTOR-GENERAL LEADS
- ASSISTANT DIRECTOR-GENERAL INVESTIGATIVE ANALYSIS

Collection
FIRST ASSISTANT DIRECTOR-GENERAL COLLECTION
- ASSISTANT DIRECTOR-GENERAL CENTRAL
- ASSISTANT DIRECTOR-GENERAL VICTORIA
- FIRST ASSISTANT DIRECTOR-GENERAL NSW
- ASSISTANT DIRECTOR-GENERAL COUNTER-TERRORISM INVESTIGATIONS

Counter-Espionage & Interference
FIRST ASSISTANT DIRECTOR-GENERAL COUNTER-ESPIONAGE & INTERFERENCE
- ASSISTANT DIRECTOR-GENERAL CEI A
- ASSISTANT DIRECTOR-GENERAL CEI B
- ASSISTANT DIRECTOR-GENERAL CYBER ESPIONAGE

Technical Capabilities
FIRST ASSISTANT DIRECTOR-GENERAL TECHNICAL CAPABILITIES
- ASSISTANT DIRECTOR-GENERAL TELECOMMUNICATIONS INTERCEPT CAPABILITIES
- ASSISTANT DIRECTOR-GENERAL TECHNICAL OPERATIONS
- ASSISTANT DIRECTOR-GENERAL TELECOMMUNICATIONS INTERCEPT OPERATIONS
- ASSISTANT DIRECTOR-GENERAL DATA EXPLOITATIONS CAPABILITIES

Operations Services & Surveillance
FIRST ASSISTANT DIRECTOR-GENERAL OPERATIONS SERVICES & SURVEILLANCE
- ASSISTANT DIRECTOR-GENERAL SURVEILLANCE
- ASSISTANT DIRECTOR-GENERAL OPERATIONAL SERVICES
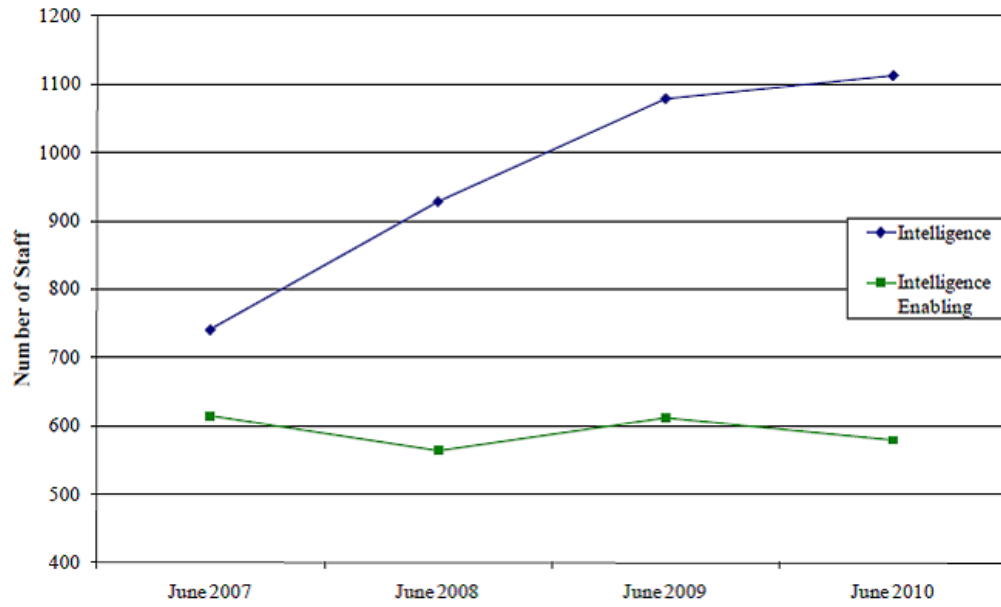
STAFFING LEVELS

FIGURE 5: WORKFORCE PROFILE BY FUNCTION

Graph 2 – Workforce Profile by Function

RATIO OF EXECUTIVE, MIDDLE AND LOWER LEVEL STAFF

At 30 June 2010, 3.4 per cent of ASIO staff were employed at the Senior Executive Service level, 24.6 per cent were engaged at the Senior Officer (Director, Assistant Director and equivalent) level, and 72.0 per cent were employed at the Officer (and equivalent) level.

TABLE 1: RATIO OF EXECUTIVE, MIDDLE AND LOWER LEVEL STAFF

Group	Total Staff	Female	NESB[1]	ATSI[2]	PWD[3]	Available EEO Data[4]
SES (excl. DG)	57	10	2	0	2	51
Senior Officers[5]	417	156	26	0	6	387
Officers[6]	1218	584	117	4	12	1131
Total	1,692	750	145	4	20	1,569

[1] Non-English speaking background
[2] Aboriginal and Torres Strait Islander
[3] People with a disability
[4] Provision of EEO data is voluntary.
[5] Translates to span the APS AEO1, AEO2, EL1 and EL2 levels.
[6] Translates to span the APS 1 to 6 classification levels.

DIRECTION AND STRATEGIC PLANNING

A highly capable security intelligence organisation heavily relies on the excellence and professionalism of its staff and current and future leadership. ASIO's preparation for the future focuses on building a strong organisational base to meet the demands of the current environment and to ensure it is suitably positioned to remain flexible and responsive to both an evolving security environment and the needs of the Government.

As part of ASIO's program of strategic business review and reform, during 2009–10 the ASIO senior management group reviewed the Organisation's structure to position ASIO to meet future challenges through improving efficiency and functional alignment. The new structure came into effect on 1 July 2010.

Some functions were redistributed on the basis that they better aligned with the investigative and assessment work of other divisions. In addition, key functional units, such as those focused on internal audits, operations evaluations and counter-intelligence, were placed outside the usual divisional structure to ensure these work areas operate with requisite autonomy.

The new structure will achieve a more efficient allocation of resources, with better alignment of staff skills and work unit functions resulting in an overall enhancement of organisational performance. Further, it is envisaged the new structure will better equip ASIO to contribute to a more broadly focused and interconnected national security community.

ASIO is reforming its recruitment framework to enhance efficiency and effectiveness following an independent review of its recruitment processes, and to improve return on investment at each stage of the process while maintaining standards. An internal taskforce has been established to assess and implement the recommendations from this review.

ASIO has also commenced a Strategic Workforce Plan to map capability supply and demand drivers. This Plan, to be implemented during 2010–11, will contribute to talent acquisition, management and retention strategies, with a view to ensuring ASIO is positioned to maintain a highly capable workforce.

CORPORATE GOVERNANCE

ASIO's corporate governance arrangements reflect the Organisation's sustained focus on risk management, accountability, performance measurement, building capability and managing growth. In 2009–10, during a period of accelerated growth and the expansion of the national security community, ASIO prioritised efforts to ensure and promote an ASIO culture which supports and drives the Organisation's work. ASIO implemented strategies to ensure its commitment to both building external partnerships and contributing strongly to national security priorities continues to be embedded firmly in ASIO's culture.

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.

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 embedding corporate governance principles at all levels of the Organisation.

The below figure illustrates ASIO's Corporate Committee structure as at 30 June 2010.

FIGURE 6: CORPORATE GOVERNANCE ARRANGEMENTS

Following the implementation of ASIO's new organisational structure on 1 July 2010, the ASIO Security Committee will be chaired by the Security, Strategy and Engagement Division Head.

The Organisational Development Committee will be superseded by the Strategic Workforce Design Committee in September 2010.

Revised ASIO Code of Conduct

In 2009–10, ASIO refined its Code of Conduct to enhance corporate governance arrangements. Refinements made to the Code of Conduct ensure it continues to articulate the professional and personal standards expected of ASIO officers while better reflecting the nature of the work undertaken and the challenges and complexity of ASIO's operating environment.

ORGANISATIONAL PERFORMANCE MANAGEMENT

Changes to ASIO's internal performance reporting mechanisms in 2009–10 provided the Organisation with an improved tool to measure its performance against pre-determined benchmarks. The new reporting format captures performance indicators, outcomes and risks centrally, which has resulted in more focused discussion and pro-active decision-making by ASIO's Corporate Executive.

STRATEGIC ALLOCATION OF RESOURCES

ASIO's resource allocation by percentage of the total reflects the Government's changing priorities between the four outputs. Resource allocation is reviewed formally and considered between February and May each year, with the Corporate Executive 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 Corporate Executive or the Director-General's Meeting. Divisional base budgets, internal projects and NPPs are monitored and driven by the Corporate Executive on a monthly basis.

AUDIT, EVALUATION AND FRAUD CONTROL

ASIO has an active and risk-based internal audit and evaluation program. Fourteen audits were completed in 2009–10. No loss of public monies was identified. At the end of the reporting period, three audits were ongoing, carrying over into 2010–11.

All internal audit reports, including recommendations arising, are reviewed by ASIO's Audit and Evaluation Committee. The Committee is chaired by a Deputy Director-General and includes two independent members, including a Senior Officer from the Australian National Audit Office. The Committee and relevant work areas accepted all audit recommendations with the exception of one, which was rejected on a sound operational basis and agreed to by the Committee and Internal Audit.

In 2009–10, ASIO's internal audit function received additional resources. This allowed internal audit to expand beyond compliance activities to include a broader range of performance audits focused on ASIO's high risk areas.

There were no suspected incidents of fraud reported in the reporting period. In 2010, ASIO's Fraud Risk Assessment was revised in line with Australian Government Fraud Control Guidelines, with a new Fraud Control Plan to be implemented in late 2010. In 2009, ASIO completed the Commonwealth Fraud Control Guidelines Annual Questionnaire.

Throughout their employment, ASIO staff participate in regular programs related to values and ethics, accountability, organisational oversight mechanisms, fraud prevention, legislative provisions, personal and professional security practices and occupational health and safety. Importantly, ASIO identifies strongly and aligns with the values and behaviours required of the public sector. In 2009–10, 71 new officers completed induction training and 488 new and ongoing staff completed ASIO's compulsory ethics and accountability workshops.

MANAGEMENT OF GROWTH

In 2009, ASIO implemented an enhanced approach to training and developing intelligence professionals that commenced in January 2010. The new approach supports greater engagement with partner agencies, academia, and the private sector; increases the level of skill and competence upon graduation; and provides access to modules for non-intelligence officer staff working in related areas.

In 2010, the ASIO People Capability Framework was developed to define key people capabilities required of staff at all levels across the Organisation to deliver on ASIO's outputs for the Government. The People Capability Framework, a key component of the overarching Human Capital Framework, will support better linkages with other Australian government agencies and underpin a number of people strategy programs, including career planning; informing the development of training initiatives; improving recruitment through consistent criteria and terminology; and informing performance management.

A leadership strategy was developed and implemented to enhance the quality of leadership, align the leadership group with the strategic agenda, support 'leadership behaviours' at all levels across the Organisation and build 'leadership bench strength' for the future. In addition to providing structure around the range of development opportunities offered for leaders in government (including from the National Security College), the strategy includes opportunities for all staff to engage with 'leaders' from Government, academia, and other agencies on strategic issues of relevance for ASIO; a program for Executive Level 1, Executive Level 2 and Senior Executive Service Band 1 officers to develop techniques to assist them drive the strategic agenda in the national security context; and forums for groups of leaders to advance ASIO's reform agenda.

Recognising that employment with the Organisation can at times impact on family life, during 2009–10 ASIO established a Staff and Family Liaison Office. This office is headed by a qualified social worker who manages a range of roles and functions designed to meet the situational needs of staff during their career with the Organisation.

To meet the challenges that come from substantial growth and identified gaps in organisation-specific experience, ASIO commissioned an independent review of the Organisation's approach to people strategy, frameworks and processes. The review focused on a more holistic approach to managing ASIO people capabilities, including the recruitment and retention of critical skills. Implementation of the recommendations from this review commenced in May 2010 and included the development of a Strategic Workforce Plan to map capability supply and demand drivers; talent acquisition, management and retention strategies; and recruitment reforms with a view to ensuring ASIO is positioned to maintain a highly capable workforce.

ASIO's HUMAN CAPITAL FRAMEWORK

One key output from the independent review of ASIO's people strategy, frameworks and processes was the formulation of the ASIO Human Capital Framework (see Figure 7). The Framework guides a detailed and strategically-oriented approach to workforce planning; better integrating ASIO's people management activities; aligning its people processes to deliver outcomes which support business requirements; and strengthening its recruitment and vetting pipeline.

The Framework is underpinned by guiding principles which drive behaviour in the development and execution of people activities, and continuous improvement across people programs. These principles are "focused on outcomes; owned by the Executive; unified across divisions; agile and progressive; and pragmatic and efficient".

The Framework integrates all people functions into a single, strategic system directed specifically at building people capability rather than a discrete set of fragmented administrative processes. The Framework recognises that the people service delivery model is based on the proposition that scarce and highly trained intelligence resources should not be diverted unnecessarily from the core business functions. The four key elements that provide the foundation of ASIO's Framework are people strategy and workforce planning; selection, evaluation and vetting; agility management, HR services and support; and capability management, learning and development.

Central to each element in the ASIO Human Capital Framework are the relationships between the Organisation and outcomes for Government, and what people capabilities are required.

LEGISLATION AND LITIGATION

LEGISLATIVE AMENDMENTS

In 2009–10, ASIO continued to work collaboratively with other Commonwealth departments and agencies on policy development and proposed legislative amendments to ensure the legislative framework supports ASIO's functions and capabilities. Legislative developments relevant to ASIO are detailed below.

Anti-People Smuggling and Other Measures Act 2010

The *Anti-People Smuggling and Other Measures Act 2010* (Cth) received Royal Assent on 31 May 2010. The Act strengthens the Commonwealth's anti-people smuggling legislative framework through amendments to:

- the *Criminal Code Act 1995* (Cth) and the *Migration Act 1958* (Cth) to create and harmonise offences and penalties in relation to people smuggling;
- the *Migration Act 1958* (Cth), the *Proceeds of Crime Act 2002* (Cth), the *Surveillance Devices Act 2004* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) to make consequential amendments;
- the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), to enable ASIO to carry out its intelligence functions in relation to territorial and border security issues; and
- the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) to enable foreign intelligence to be collected in certain circumstances and clarify that only the Minister for Defence and the Minister for Foreign Affairs can advise the Attorney-General on the need to issue a warrant for the collection of foreign intelligence.

The amendments to the ASIO Act introduced provision for the protection of Australia's territorial and border integrity from serious threat. This amendment enables ASIO to contribute to the Commonwealth's response, including people smuggling.

The Act also amended the definition of 'foreign intelligence' in the *Telecommunications (Interception and Access) Act 1979* (Cth) to align it with the concept of foreign intelligence currently contained in the *Intelligence Services Act 2010* (Cth).

Crimes Legislation Amendment (Serious and Organised Crime) Act 2010

The *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010* received Royal Assent on 19 February 2010. The Act amended, amongst other matters, Part IAC of the *Crimes Act 1914* (Cth) to implement the new national model laws regime for assumed identities endorsed by the Standing Committee of Attorneys-General in 2004.

The new assumed identities regime provides a more detailed process for issuing, using and obtaining evidence in support of assumed identities used by ASIO, other intelligence agencies and law enforcement.

Tax Laws Amendment (2010 Measures No.3) Act 2010

The *Tax Laws Amendment (2010 Measures No.3) Act 2010* received Royal Assent on 29 June 2010. Schedule 3 to the Act amends the *Taxation Administration Act 1953* to remove the possibility of conflict between Australia's national security interests and obligations imposed by Commonwealth tax laws. It does this by empowering the Director-General of Security and the Director-General of the Australian Secret Intelligence Service (ASIS) to declare that specified transactions are to be disregarded in determining tax liabilities, obligations or benefits under Commonwealth law. The Director-General of Security made no declarations in 2009–10.

When any declarations under this Act are made, tax liabilities, obligations and benefits will not apply in relation to the specified transactions. As a result there will be no obligation to provide information about these transactions to the tax authorities and no power to seek that information. This ensures that information that bears on the operational activities of Australia's security and intelligence agencies, which should remain secret in the interests of national security, will not be disclosed.

Declarations are subject to review by the Inspector-General of Intelligence and Security (IGIS), and also fall generally within the mandate of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its role to review the administration and expenditure of ASIO.

LITIGATION MATTERS

In the 2009–10 financial year, ASIO was involved in over 40 litigation matters, including criminal (in particular terrorism) prosecutions, judicial and administrative review of Security Assessments, and a range of other civil litigation matters.

ASIO information is often sought by Commonwealth prosecutors and subpoenaed by defendants for use as evidence. It can also form part of civil and administrative legal proceedings, often not involving ASIO directly (for example Freedom of Information applications to other agencies holding ASIO information). Demand for such material has continued to increase dramatically. Much of it is sensitive and some has been collected pursuant to special powers warrants. ASIO accordingly aims to balance protection of officer and source identities, collection methods and capabilities, and domestic and foreign relationships with the need to support prosecutions and other legal processes in the interests of open justice.

Consistent with the significantly higher level of activity experienced every year since 2005, ASIO's involvement in a large number of diverse and complex matters generated a significant work load. Sydney Pendennis, the longest-running terrorism prosecution in Australian history, concluded in 2009–10. On 16 October 2009, a jury found five defendants guilty of conspiring to do act(s) in preparation for a terrorist act or acts. On 15 February 2010, the New South Wales

Supreme Court sentenced them to terms of imprisonment ranging from 21 to 28 years. All have lodged appeals against conviction and sentence.

In August 2009, Melbourne Pendennis defendant Shane Kent, who had pleaded guilty to membership of a terrorist organisation and recklessly making a document connected with preparation for a terrorist act, was sentenced to five years' imprisonment. Along with fellow Melbourne Pendennis defendants Amer Haddara and Abdullah Merhi, Mr Kent has served his sentence and been released on parole.

ASIO continued to support Commonwealth terrorism prosecutions in Melbourne. In 2009–10, this included the prosecution of five Melbourne men charged with conspiring to do an act in preparation or planning for a terrorist act (Operation NEATH). It was alleged they were planning to conduct an armed attack on an Australian military base, and had conducted a reconnaissance of the Holsworthy Barracks.[1]

ASIO continued to support other criminal prosecutions. In January 2010, ASIO worked closely with ASIS and the South Australian Police to prepare material for use in the prosecution of an individual charged with three counts of blackmail. The individual pleaded guilty.

ASIO was also involved directly in two legal matters initiated by Mr Mamdouh Habib[2]:

- Mr Habib's appeal to the High Court of Australia against the November 2007 decision of the Administrative Appeals Tribunal (AAT) upholding an adverse Security Assessment and denying him an Australian passport. In May 2010 the High Court remitted this matter, with the parties' consent, to the AAT for re-hearing[3]; and
- his Federal Court of Australia compensation claim alleging that the Commonwealth defamed him and was complicit in his alleged mistreatment while he was detained overseas between 2001 and 2005[4].

ASIO was involved in challenges to a number of its Security Assessments. Significant legal and operational resources were required to identify, assess and produce material relevant to the proceedings. On 30 September 2009, the Federal Court of Australia in Melbourne dismissed three applicants' notices of motion seeking production of ASIO documents. One of these applicants has since discontinued his application, and the remaining two are listed for hearing in February 2011.

---

[1] The Victorian Supreme Court jury trial commenced on 13 September 2010, and on 23 December 2010 resulted in conviction of three of the defendants. All three were remanded in custody to await sentencing hearings, expected to commence in April 2011.

[2] The Inspector-General of Intelligence and Security is conducting an inquiry into the actions of Australian intelligence agencies in relation to the arrest and detention overseas of Mr Habib from 2001 to 2005.

[3] The AAT has since dismissed the appeal because Mr Habib has sought merits review of a subsequent adverse Security Assessment and passport refusal decision.

[4] This claim was settled in December 2010.

To ensure both its management of legal issues across the Organisation and its support to Commonwealth litigation, ASIO continued to invest in its legal capability. It has legal teams in Sydney and Melbourne, and has integrated lessons learned from prosecutions and other legal proceedings into its policies and procedures.

USE OF ASIO'S SPECIAL POWERS

The ASIO Act and 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.

RELATIONSHIPS WITH EXTERNAL AGENCIES

ASIO has increased engagement significantly with legal counterparts in Commonwealth, state and territory law enforcement bodies, so as to strengthen its support to criminal prosecutions. This has included formal inter-agency meetings, increased informal dialogue and a commitment to more collaborative work. Similarly, ASIO has increased engagement with external stakeholders to support civil litigation matters, notably legal challenges to Security Assessments.

Following the Sydney Pendennis trial, the Sydney Office of the Commonwealth Director of Public Prosecutions (CDPP) hosted a review of the conduct of the prosecution. ASIO, the Australian Federal Police (AFP) and New South Wales Police participated in the review, held in November 2009. The review examined issues that presented particular challenges in the prosecution, such as maintaining effective and efficient information flow across multiple agencies, consistency between agencies in the preparation of evidence and protection of sensitive information and procedures for disclosure of material relevant to the defence. The resulting report made 38 recommendations for consideration in future complex counter-terrorism matters. The recommendations were largely accepted by ASIO, which noted that a number of developments (including extensive Joint Counter-Terrorism Taskforce governance arrangements, prosecution guidelines involving AFP, the CDPP and ASIO, and ASIO training initiatives to better prepare its officers for future counter-terrorism prosecutions) have occurred since 2004 and 2005 which independently address many of the recommendations in the report.

SECURITY OF ASIO AND ASIO SECURITY ASSESSMENTS

VETTING OF ASIO STAFF

ASIO employees require a Top Secret (Positive Vetting) (TSPV) national security clearance.

For the reporting period, the *Australian Government Protective Security Manual* (PSM) was the authority document in regard to vetting considerations for ASIO staff. On 11 June 2010, the Attorney-General endorsed the *Protective Security Policy Framework* (PSPF) which now co-exists with the PSM to outline requirements for protective security across the Commonwealth. As such, both terms have been referenced in the context of ASIO's vetting and other protective security programs.

ASIO initiated over 362 TSPV security clearances as a result of recruitment activities in 2009–10. A further 192 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.

Except for its own staff (and in a limited number of cases where ASIO is the clearance sponsor), ASIO is not the issuing authority for security clearances and it is up to individual departments and agencies to consider ASIO's advice.

REVALIDATION AND RE-EVALUATION PROGRAM

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

The revalidation/re-evaluation program continues throughout the life of the clearance. Clearance holders must be re-assessed as remaining honest, loyal, trustworthy, mature and

tolerant through a process of psychological testing, police, financial and other checks, multiple referee appraisals and workplace assessments.

In the reporting period ASIO conducted 244 probation revalidations, 8 revalidations and 185 full re-evaluations. ASIO also conducted five full re-evaluations for external agencies.

SECURITY BREACHES

ASIO security policies meet or exceed the standards laid down in the Australian Government Protective Security Policy Framework. ASIO's *Security Plan 2009–12* and *Security Breach Policy* provide strategies to mitigate security risks and provide a framework for staff to ensure sound security is practiced in daily business.

ASIO's senior executive is briefed on security breaches every quarter, and senior managers are notified of breaches occurring within their divisions and branches.

E-SECURITY ARRANGEMENTS AND ENHANCEMENTS

Electronic interference is a growing security concern. In 2009–10, ASIO expanded its engagement with industry on the threat of electronic espionage, particularly in the resources and energy sectors. ASIO liaised with a small number of private sector companies which were the targets of electronic intrusions. In June 2010, ASIO also sponsored a resource sector information technology forum to deliver high-level briefings on cyber security and espionage threats and mitigation strategies to a range of resource sector companies. The forum coincided with National Cyber Security Awareness Week.

In January 2010, a multi-agency initiative was established to coordinate work against e-security threats. The Cyber Security Operations Centre (CSOC) was established in the Defence Signals Directorate (DSD) in 2009 as an initiative of the *Defence White Paper* to coordinate work against this threat. Personnel from ASIO, the Attorney-General's Department and the Australian Federal Police (AFP) are embedded within the Centre. ASIO's close cooperation with the CSOC and Computer Emergency Response Team (CERT) Australia extends to providing support and advice to private and government-owned critical infrastructure. In close consultation with these agencies, ASIO identifies developing cyber threats to critical infrastructure and determines appropriate responses.

The role of ASIO's IT Security directorate is to ensure ASIO's Information Communication Technology (ICT) systems are designed, installed, maintained and operated in a secure fashion, and to respond to threats. The directorate identifies and implements methods to mitigate risks to ASIO systems, including its externally connected systems. These include:

- an established, 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 providing recommendations for improvement;

- sharing ICT threat advice within the Australian Intelligence Community;
- developing and reviewing internal ICT Security Policies;
- providing targeted ICT security education programs for ASIO staff, ICT staff and ICT contractors; and
- providing ICT security advice, including advice in response to general enquiries and design, development, and implementation advice to ICT projects.

Maintaining information technology systems that have the necessary controls and security to communicate at the TOP SECRET level is expensive, both in the cost of security and the associated resource costs in people. Considerable personnel, security infrastructure and policy is required, which can present a significant barrier to new members of the national security community in building and maintaining these capabilities.

In 2009–10, in order to seek efficiencies of scale, ASIO built and continues to support a TOP SECRET environment (TS Enclave) on behalf of the Department of the Prime Minister and Cabinet, the Australian Customs and Border Protection Service and the AFP. This environment will allow those agencies to communicate and collaborate at the TOP SECRET level and also provide broader access to AICNET. It is anticipated that the TS Enclave, when fully populated, will support 200 users from these three agencies at less cost-per-user to each agency.

SECURITY ASSESSMENTS

ASIO's security assessment function is an important component of Australia's national security defenses. It provides a mechanism for 'security' (as defined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act)) to be considered in certain regular government decision-making processes (defined as 'prescribed administrative actions' in the ASIO Act). For example, in the issuing of passports, granting of visas, granting of access to sensitive government information (security clearances), and access to restricted areas such as ports and airports and sensitive goods such as ammonium nitrate.

Consistent with ASIO's role as an intelligence agency, they are a means by which ASIO provides advice. Security Assessments only consider factors related to 'security', which in practice is usually terrorism, other forms of politically motivated violence, espionage and foreign interference, and threats to Australia's territorial and border integrity. Security Assessments are not criminal or character checks and factors such as criminal history, dishonesty or deceit are only relevant to ASIO's advice if they have a bearing on security considerations. Character is not itself sufficient grounds for ASIO to make an adverse security finding.

Most ASIO Security Assessments are made at the request of another department or agency, though ASIO can, and particularly in relation to passports does, issue assessments as a consequence of an ASIO intelligence investigation. Security Assessments can include a simple check of personal details against ASIO's intelligence holdings, or an in-depth intelligence investigation to determine the nature and extent of an identified threat to Australia's national security. Each Security Assessment is handled on a case-by-case basis.

Upon making an assessment ASIO may provide:

- non-prejudicial advice, which means that ASIO has no security-related concerns about the proposed 'prescribed administrative action';
- a qualified assessment, which generally means that ASIO provides to the agency concerned information about the assessment subject relevant to security, but is not making a prejudicial recommendation in relation to the 'prescribed administrative action'; or
- an adverse assessment in which ASIO recommends that a 'prescribed administrative action' be taken (cancellation of a passport, for example), or not taken (declining access to a security controlled area, for example).

The consequence of an ASIO Security Assessment depends on the purpose for which it is made and the associated legislation, regulation or policy. In some cases decision-makers are obliged to take (or are prevented from taking) actions because of an ASIO Security Assessment — such as granting visas to travel to, or remain in, Australia. In other cases the assessment is only a single component to be considered among a range of other factors, for example, for granting access to national security information. In all cases, ASIO itself is not permitted by the ASIO Act to take any administrative action in relation to the assessment subject.

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

VISA SECURITY ASSESSMENTS

Any person applying for a visa to travel to, or remain in, Australia may have the application referred by the Department of Immigration and Citizenship (DIAC) to ASIO for a Security Assessment. Given the large volume of visa applications, it is not practical for each one to be assessed by ASIO. A risk managed referral framework has, therefore, been developed so that applications more likely to be of concern are drawn to ASIO's attention. Still, ASIO assesses many thousands of visa applications annually.

In most visa categories, a visa may not be issued (or must be cancelled) where ASIO determines the applicant to be directly or indirectly a risk to 'security' (as defined in the ASIO Act). The enabling legislation in this instance is the *Migration Act 1958*, specifically the *Migration Regulations 1994* and public interest criterion 4002.

Separately to visa application referrals from DIAC, ASIO's security intelligence investigations will from time to time determine that the holder of a valid visa to Australia (who is sometimes already in Australia, and other times overseas) presents a risk to Australia's security. In such circumstances ASIO may provide to the Minister for Immigration and Citizenship an adverse Security Assessment, which would lead the Minister to cancel the visa.

ASIO completed 38,438 visa Security Assessments in 2009–10. Nineteen adverse assessments were made in relation to visas. Fourteen of these adverse assessments were issued on counter-terrorism grounds and five were issued on counter-espionage or foreign interference grounds.

In 2009–10, ASIO diverted resources to undertaking security assessment of Irregular Maritime Arrivals (IMAs) for DIAC. Consequently, the resources available to assess protection visa and other refugee referrals were limited and this caseload experienced delays. ASIO continued to work very closely with DIAC to ensure visibility of the overall visa Security Assessment caseload and agreed priorities.

TABLE 2: VISA SECURITY ASSESSMENTS 2009–10

Type of entry	Number of assessments completed
Temporary visas	24,208
Permanent Residence	8,624
Onshore Protection	989
Offshore Refugee/Humanitarian	1,795
Irregular Maritime Arrivals	2,822
Total	38,438

TABLE 3: VISA SECURITY ASSESSMENTS 2003–10

Type of entry	2003–04	2004–05	2005–06	2006–07	2007–08	2008–09	2009–10
Temporary visas	30,841	39,015	39,973	44,197	56,126	46,896	24,208
Permanent Residence	13,881	13,402	13,174	9,190	16,562	12,988	14,230
Total	44,722	52,417	53,147	53,387	72,688	59,884	38,438

During the reporting period, ASIO engaged an independent assessor to review ASIO's visa security checking processes. Subsequently, and in close consultation with DIAC, ASIO implemented a number of recommendations designed to improve efficiency of the visa Security Assessment process and better manage risk.

The reduction in the total number of visa Security Assessments by ASIO compared with 2008–09 is a result of improved focus on a smaller number of visas, and represents an attempt to target ASIO's resources in this area. This is reflected in the fact that, despite assessing fewer total visa applications, ASIO has issued an increased number of adverse Security Assessments since the major changes to the referral guidelines (introduced 9 May 2009).

Delays in Visa Security Assessments

ASIO works closely with DIAC to prioritise caseloads, with an emphasis on detention cases (including IMAs) and compassionate or compelling cases, including individuals identified by DIAC as vulnerable.

During 2009–10, ASIO had to divert significant resources to undertaking security assessment of IMAs for DIAC. Protection visa assessments and other refugee assessments were most significantly affected, as the work area which manages these assessments was required to absorb the IMA workload rapidly. Given these resource pressures, ASIO has implemented measures to ensure all security assessment cases receive attention, including quarantining resources in the form of a dedicated team responsible for protection visas and other complex non-IMA visa cases; and working very closely with DIAC to ensure visibility of the overall visa security assessment caseload and agree priorities.

Complaints to the Inspector-General of Intelligence and Security

ASIO works closely with the Office of the Inspector-General of Intelligence and Security (IGIS) to address complaints regarding delays in processing visa Security Assessments. During 2009–10, the IGIS made 811 administrative inquiries to ASIO.

- The number of inquiries of ASIO is less than the number of complaints received by the Office of the IGIS as, based on their knowledge of ASIO processes, the Office of the IGIS declines a significant minority of complaints without referral to ASIO.
- The increase in complaints does not indicate an increase in issues with, or failings by, ASIO.
- The majority of these visa-related complaints to the IGIS appear to be attempts to accelerate visa processing times and do not indicate problems in ASIO's processes or significant levels of delay in reaching assessments.
- The majority of these complaints come from a defined group of visa applicants (with one specific nationality and one specific visa type prevailing).
- Across other nationalities and visa types, complaints to the IGIS have not increased significantly.

Of the 811 enquiries, the IGIS found that:

- Only two complaints related to administrative error by ASIO – both of these were acted on immediately and processes were reviewed to avoid similar errors from re-occurring.

- 26 per cent of cases had already been completed by ASIO, or had not yet been referred to ASIO by DIAC;
- The number of complaints relating to skilled visas (identified by the IGIS as 48 per cent of all complaints to the Office) is likely to be driven by changes in government policy around skilled migration rather than any issue with ASIO's handling of these visas.
- The IGIS has noted that the increase in complaints may reflect increased awareness by applicants and migration agents of the option to refer matters to the IGIS.

PERSONNEL SECURITY ASSESSMENTS

The Protective Security Policy Framework sets out Australian government policy and guidance on protective security, including policy for the granting of clearances for access to national security classified information. In almost all circumstances a department or agency must request security assessment advice from ASIO as part of its overall consideration of whether or not to grant a national security clearance. In making the assessment, ASIO reviews any intelligence it may hold, as well as considering known security risk factors.

ASIO completed 22,343 personnel Security Assessments in 2009–10. ASIO issued one adverse and one qualified personnel Security Assessment in 2009–10 (see Table 4).

TABLE 4: PERSONNEL SECURITY ASSESSMENTS 2009–10

Type of assessment	Number
Confidential	3,052
Secret	11,929
Top Secret	4,931
Top Secret Positive Vet	2,431
Total	22,343

From 1 October 2010, all Commonwealth security clearances for access to national security classified information will (except for a few exempt agencies) be undertaken by a single security vetting agency — the Australian Government Security Vetting Agency (AGSVA). The AGSVA will be located in the Department of Defence and will consequently become ASIO's primary client for Security Assessments for national security clearances.

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 will undertake further investigative actions.

COUNTER-TERRORISM SECURITY ASSESSMENTS

ASIO conducts counter-terrorism checks at the request of AusCheck and the AFP. ASIO completed 98,086 counter-terrorism Security Assessments in 2009–10, 99 per cent of which were completed within five days.

AusCheck refers applicants for Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC) for a counter-terrorism check. ASICs and MSICs ensure that those with access to sensitive air and maritime port areas undergo appropriate background checking. ASICs are administered under the *Aviation Transport Security Act 200*4 and associated regulations. MSICs are administered under the *Maritime Transport and Offshore Facilities Security Act 2003* and associated regulations.

ASIO's role in the ASIC and MSIC process is primarily to consider any terrorism concerns. AusCheck coordinates the larger suite of background checks (including criminal history) and assesses the applicant's overall suitability to hold an ASIC or MSIC. ASIO's advice may recommend against the issuance of an ASIC or MSIC if there are assessed security concerns.

ASIO completed 88,367 ASIC and MSIC checks in 2009–10. No adverse or qualified Security Assessments were made.

ASIO provides (via the AFP) counter-terrorism background checks for licensing by the Australian states and territories for access to security sensitive ammonium nitrates (SSANs — used as an explosive particularly by the mining industry and as a fertiliser in agriculture). Each state and territory has its own licensing regime, consistent with a set of principles agreed in 2005 by the Council of Australian Governments. ASIO may recommend against a license for access to SSANs. ASIO completed 7,803 SSAN checks in 2009–10.

ASIO also provides, via the AFP, security assessment advice on any terrorism concerns for individuals requiring access to the Australian Nuclear Science and Technology Organisation nuclear facility at Lucas Heights. In 2009–10, ASIO completed 1,371 checks. The AFP also requests counter-terrorism checks for people requiring accreditation for special events. During the reporting period, ASIO conducted 322 checks for people requiring accreditation for the Pacific Islands Forum in August 2009.

TABLE 5: COUNTER-TERRORISM CHECKS

Type of check	2003–04	2004–05	2005–06	2006–07	2007–08	2008–09	2009–10
Aviation/Maritime Security Identity Cards	58,147	38,466	71,733	118,118	70,084	56,266	88,367
Security Sensitive Ammonium Nitrate	-	1,634	7,428	6,419	4,502	7,948	7,803
ANSTO[1]	-	-	-	1,027	1,251	905	1,371
Special Events	-	-	-	9,417	13,453	-	322
Flight Crew	-	-	-	-	-	-	223
Total	58,147	40,100	135,310	134,981	89,290	65,119	98,086

[1] Australian Nuclear Science and Technology Organisation

HUMAN RESOURCE MANAGEMENT

RECRUITMENT

FIGURE 8: ASIO'S JOB FAMILY ADVERTISING 2009–10

As at 30 June 2010, ASIO employed 1,692 staff which represented 1,600 full time equivalent (FTE) staff. In 2009–10, ASIO appointed 117 employees, with 79 per cent engaged on an ongoing basis. As a consequence of the 2005 *Review of ASIO Resourcing* by Mr Allan Taylor AM (Taylor Review), ASIO's recruitment efforts have focused on achieving a substantial workforce growth program to culminate in staff numbers reaching 1,860 during 2011. Employment market conditions, combined with the necessarily stringent and lengthy security vetting of potential new staff contributed to ASIO not reaching its recruitment targets for the 2009–10 financial year. As a result of these shortfalls, ASIO will not reach this target until the 2012–13 financial year.

Throughout the year, recruitment activities focused on building intelligence and technical capabilities and essential enabling functions. Recruiting high-calibre staff suitable to work in ASIO's high security environment — particularly in the more specialised areas of intelligence analysis and collection — proved particularly challenging. Difficulties in finding suitable candidates to undertake work in these specialised areas, coupled with the rigorous and lengthy security vetting of potential new staff, were key contributing factors to ASIO not meeting its ambitious 2009–10 growth targets.

In 2009–10, ASIO introduced changes to the manner in which it engages with prospective applicants. This included a larger and broader online presence which appeals more effectively to

prospective employees. During the reporting period, recruitment media planning, coupled with online media (such as the placement of banner advertising on social networking site Facebook) assisted ASIO to attract and source suitable applicants. ASIO's expenditure on recruitment advertising was more cost effective than previously, decreasing from $1.962m in 2008–09 to $1.250m in 2009–10.

In 2009–10 ASIO's focus continued to be on building the intelligence-focused areas while maintaining capability in the enabling corporate functions. In particular, the recruitment of Intelligence Professionals, technical skill sets and professional skill sets such as psychologists and lawyers remained challenging.

Learning and Development

ASIO aims to build an adaptable, responsive and capable workforce to meet a wide range of challenges including rapidly shifting priorities in the security environment. ASIO invested $16.7m in people development during 2009–10, an increase of 38 per cent on the previous year. People capability development will continue to be central to the Organisation's strategic focus.

ASIO's core business of collecting, analysing and assessing information relevant to security generates a requirement for staff to develop and enhance specialist skills. This includes language skills and an increasingly wide range of skills relevant to professional disciplines such as information security, critical infrastructure protection, telecommunications and engineering, data analysis and information management. Investing in these skills has strengthened ASIO's ability to respond to the challenges of the security environment.

Corporate Development Programs

ASIO's internal professional development and leadership development programs are complemented by programs drawing on skills and experience from other parts of government and non-government sectors. Increasingly, ASIO is drawing on the resources of academia and elsewhere to provide programs that meet the particular needs of the Organisation in areas such as strategic analysis and cultural awareness.

In 2009–10, ASIO's programs were aligned with development programs across Government, notably the establishment of the National Security College at the Australian National University, as well as through the programs, seminars and other events sponsored by the Australian Public Service Commission. During the reporting period, approximately 100 ASIO officers attended orientation or senior officer courses run by the national security community designed to foster cooperation and mutual understanding of roles and functions within the community.

ASIO's learning culture aims to foster professionalism. During 2009–10, the Organisation provided assistance to 270 officers for external study programs across a range of disciplines. 18 officers undertook language development training that was fully, or partly, funded by ASIO. Assistance included additional leave to attend classes and examinations and financial assistance for continuation of study considered to be relevant to the needs of the Organisation. ASIO's

Study Assistance Program forms a key component of ASIO's people retention, rewards and recognition strategy. In addition to study assistance, the Director-General of Security awarded a number of study bursaries to officers who achieved excellence in their academic performance while continuing to make a valued contribution to ASIO's work.

MANAGEMENT AND LEADERSHIP SKILLS

ASIO's leadership programs are designed to build skills required for the public sector, not just for ASIO. ASIO's programs connect well to external programs and develop its leaders as individuals with the resilience and dexterity to manage and lead. In 2009–10, ASIO implemented a leadership program that challenges a 'vertical slice' of ASIO's leadership ranks to work across boundaries to undertake and implement projects that further the achievement of ASIO's strategic goals in the context of a larger national security community. These programs include participants from partner agencies.

ASIO's Leadership Strategy was launched in March 2010 and is a key initiative that aligns ASIO with the reforms related to providing strong leadership and strategic direction, flagged by *Ahead of the Game: BluePrint for Reform of Australian Government Administration.* The strategy focuses on three key platforms – programs, seminars and systems – and emphasises the importance of leadership by all ASIO staff to position the Organisation to meet challenges of the current and future operating environment.

The leadership program is building leadership capability and driving strategic direction to position ASIO for the future. This includes engagement with the Director-General of Security and ASIO's Senior Executive and culminates with the establishment of 'Think Nets' – a group of peers from across the Organisation working together on key leadership projects supporting the strategic direction of ASIO. All leaders in ASIO will participate in the program in the period to 2012.

ASIO's seminar series reaches out to Government and academia to source presenters who can challenge and contextualise ASIO's work with reference to broader government priorities, as well as providing insights and techniques for connecting within Government. The seminar series is a new initiative that commenced in May 2010 and will continue on a monthly schedule. The monthly seminars invite all staff to engage in topics related to leadership, national security and government issues. Speakers to date have provided insight into the global political landscape, the global security environment and broad public sector reform. The seminars are also attended by staff from other Australian Intelligence Community (AIC) agencies.

PERFORMANCE MANAGEMENT

In 2009–10 ASIO developed *Sustainable Excellence in ASIO,* a blueprint to deliver an integrated Performance Management Framework beyond people management and performance monitoring. The framework, to be implemented in 2010–11, augments linkages between formal and informal feedback systems, performance metrics, learning and development opportunities and workforce planning to foster and maintain short and long-term people capability. Senior

Executive Service (SES) performance agreements were reviewed to ensure clear connections with ASIO's strategic goals.

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 development programs.

ASIO is well integrated in the national exercise programs conducted under the auspices of the National Counter-Terrorism Committee. ASIO is also committed to supporting the programs of the National Security College. ASIO will continue to engage with the AIC, law enforcement and other partners to build its capability to respond collaboratively to the challenges the Organisation faces through joint training, exercises, secondments and attachments (both to and from ASIO).

LANGUAGE TRAINING

During the reporting period, ASIO continued to strengthen its foreign language capability, including by enhancing relationships with key domestic and foreign partners.

ASIO's commitment to developing its foreign language capability in 2009–10 included:

- full-time training in languages relevant to ASIO's investigative work;
- full-time language training for ASIO's 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.

In 2009–10, ASIO facilitated several short-term foreign language support activities with key domestic and foreign partners.

ATTACHMENTS

ASIO encourages staff exchanges with Australian and international partners. These exchanges improve ASIO's cooperation and interoperability with a range of other agencies and encourage the sharing of skills, capability, knowledge and information. The number of attachments to and from other agencies increased in 2009–10 as ASIO continued to build on its outreach and engagement strategy. During the reporting period, there were attachments to and/or from ASIO to:

- the Attorney-General's Department;
- the Australian Crime Commission;
- the Australian Federal Police;
- the Australian Government Solicitor;
- the Australian Secret Intelligence Service;
- the Defence Imagery and Geospatial Organisation;
- the Defence Intelligence Organisation;
- the Defence Security Authority;
- the Defence Signals Directorate;
- the Department of Defence;
- the Department of Foreign Affairs and Trade;
- the Office of Transport Security within the Department of Infrastructure, Transport, Regional Development and Local Government;
- the Department of the Prime Minister and Cabinet; and
- the Office of National Assessments.

WORKPLACE DIVERSITY

ASIO has implemented recruitment and people management strategies intended to create an inclusive working environment that recognises and utilises the diversity in the workforce, while seeking to recruit a range of people that reflect the Australian community as much as is practical. Generally, ASIO's staffing profile compares favourably with that of the broader Australian Public Service (APS).

- ASIO officers from non-English speaking background (people born overseas whose first language was not English) comprise 6.9 per cent of ASIO staff, an increase from 5.6 per cent in 2008–09.
- The *State of the Service Report 2009–10* notes that the proportion of APS employees who identified themselves as being from a non-English speaking background rose slightly to 6.3 per cent. Accordingly, ASIO's representation of 6.9 per cent is marginally higher.
- Women now make up 44 per cent of ASIO's workforce – an improving trend. However, they remain under-represented in the Senior Officer (37 per cent) and

SES (18 per cent) ranks compared with the APS norms (46 per cent and 37 per cent respectively).

- The proportion of part-time staff employed at 30 June 2010 was nine per cent. This has risen from eight per cent at 30 June 2009. Most of these part-time staff members (86 per cent, or 116) were women, with around half being in the 35-44 year age group.

- At 30 June 2010, 89 per cent of ASIO's total staffing of 1,692 was working on a full-time basis. This represented FTE of 1,600.

- The median age of the Organisation's workforce is currently 36 years, compared with the median age of the APS of 42 years (as reported in the State of the Service Report 2009–10). The average age of the Organisation's workforce at 30 June 2010 was 38.4 years and, while this remained unchanged relatively compared to the last reporting period, the figure has been trending down since 2003 when it was 40 years.

AGE OF ASIO STAFF

The profile across age groups remains the same since 1 July 2006 onwards.

LENGTH OF SERVICE OF ASIO STAFF

The percentage of staff members with less than five years of service has decreased slightly from the same time last year to 62.2 per cent (down from 68.6 per cent). At the end of the reporting period 16.6 per cent of staff members had ten or more years experience in ASIO. The increase in five years or more length of service can be attributed to fewer external commencements and the transition of staff recruited in 2005 and 2006 into a new reporting category.

The below graph illustrates the length of service for staff members at 30 June 2010 with comparisons from June 2007.

FIGURE 9: LENGTH OF SERVICE OF ASIO STAFF
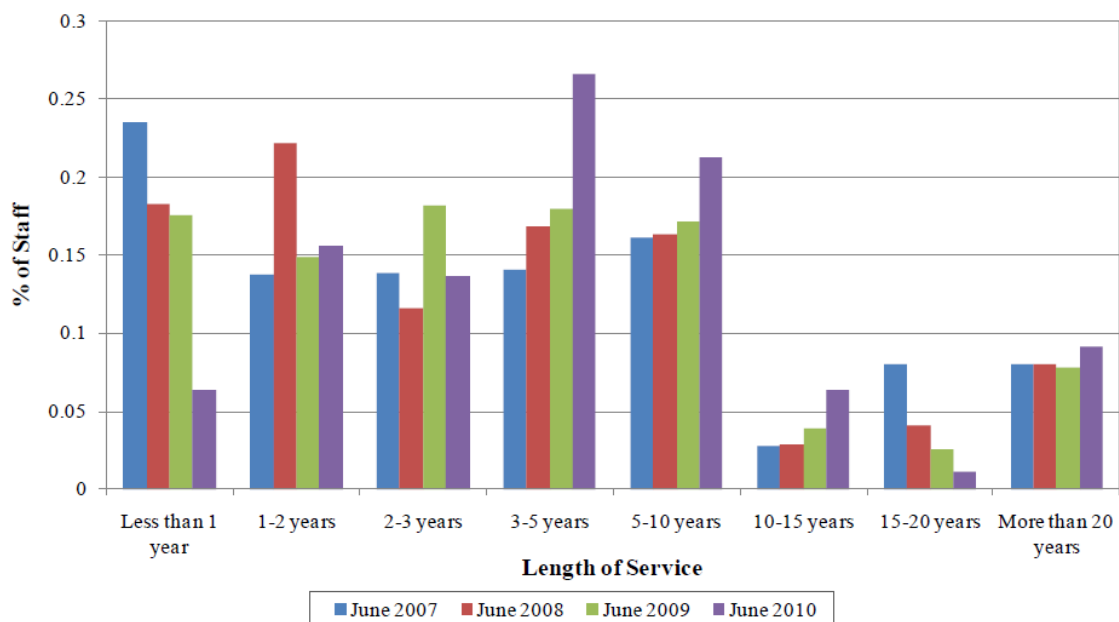
GENDER BALANCE BY CLASSIFICATION

At 30 June 2010, the Organisation's workforce consisted of 56 per cent males and 44 per cent females. This ratio has observed an increase in the number of females from 42 per cent in June 2003 – this trend is consistent with the broader labour market where there has been greater participation by females.

The following graph provides a breakdown of gender by classification and shows females outnumber males at the AO3, AO4 and AO5 classification, while the number of males continues to be larger in the ITO1/2 and IO classifications. The gender ratio difference is more pronounced at the Senior Officer and SES levels with females constituting 37 per cent of Senior Officers and 18 per cent of SES. This pattern is consistently lower than the APS figures of females constituting 46 per cent of ongoing staff at the Executive level and 37 per cent at the SES level (*State of the Service Report 2009–10*).

FIGURE 10: GENDER BALANCE BY CLASSIFICATION

AO1–5 - ASIO Officer 1–5
IO - Intelligence Officer
IO(T) - Intelligence Officer (Trainee)
AEO1–3 - ASIO Executive Officer 1–3
ADG – Assistant Director-General
SES - Senior Executive Service
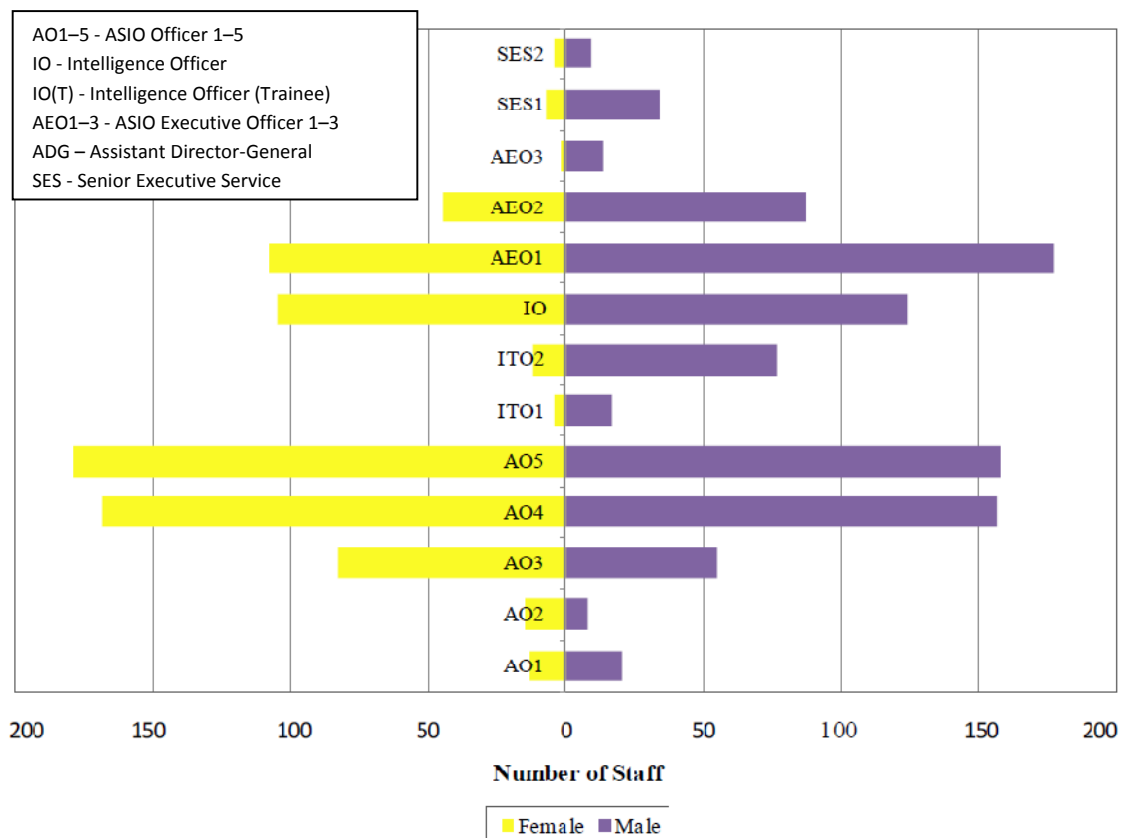
* Includes equivalent staff in the Engineering and Information Technology classifications.

REPRESENTATION OF DESIGNATED GROUPS

Based on staff salary classifications recorded in ASIO's human resource information system.

TABLE 6: REPRESENTATION OF DESIGNATED GROUPS

Group	Total Staff	Women	Non-English Speaking Background	Aboriginal and Torres Strait Islander	People with a disability	Available EEO Data[1]
Senior Executive Service (excl DG)	57	10	2	0	2	51
Senior Officers[2]	417	156	26	0	6	387
AO5[3]	570	284	41	0	5	335
AO1–4[4]	521	283	36	4	6	684
Information Technology Officers Grades 1 and 2	108	15	10	0	1	95
Engineers Grades 1 and 2	19	2	2	0	0	17
Total	1,692	750	117	4	20	1,569

[1] Provision of EEO data is voluntary.

[2] Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications.

[3] ASIO Officer Grade 5 group translate to APS Level 6.

[4] Translates to span the APS 1 to 5 classification levels.

The trend over the last four financial years shows a slight decrease in the percentage of Aboriginal and Torres Strait Islander (ATSI) people and people with a disability (PWD) in the Organisation. The decrease in representation of people with disabilities is consistent with the situation in the APS.

FIGURE 11: PERCENTAGE OF REPRESENTATION OF DESIGNATED GROUPS
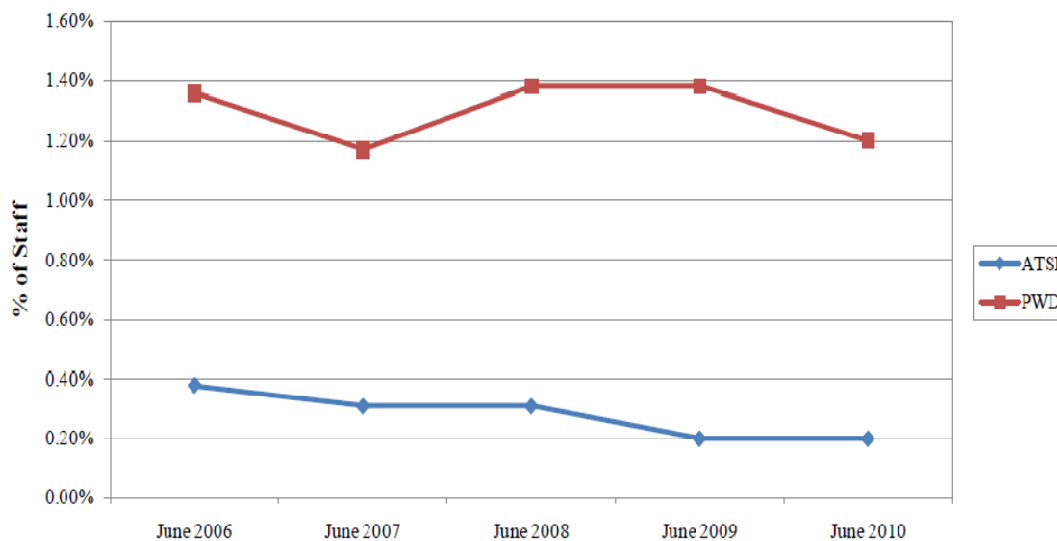
In accordance with the *Reconciliation Action Plan 2009–2012* on indigenous affairs, the Organisation attends the Attorney-General's Portfolio Reconciliation Network Meeting. The purpose of this meeting is to view indigenous affairs matters from a whole-of-portfolio perspective and to assist in identifying processes and procedures that are preventing agencies from attracting and retaining indigenous employees.

REPRESENTATION OF DESIGNATED GROUPS: FEMALE AND RACE/ETHNICITY

The below graph shows the percentage of females and staff with non-English speaking backgrounds has remained relatively steady over the last four financial years.

FIGURE 12: PERCENTAGE OF REPRESENTATION OF DESIGNATED GROUPS
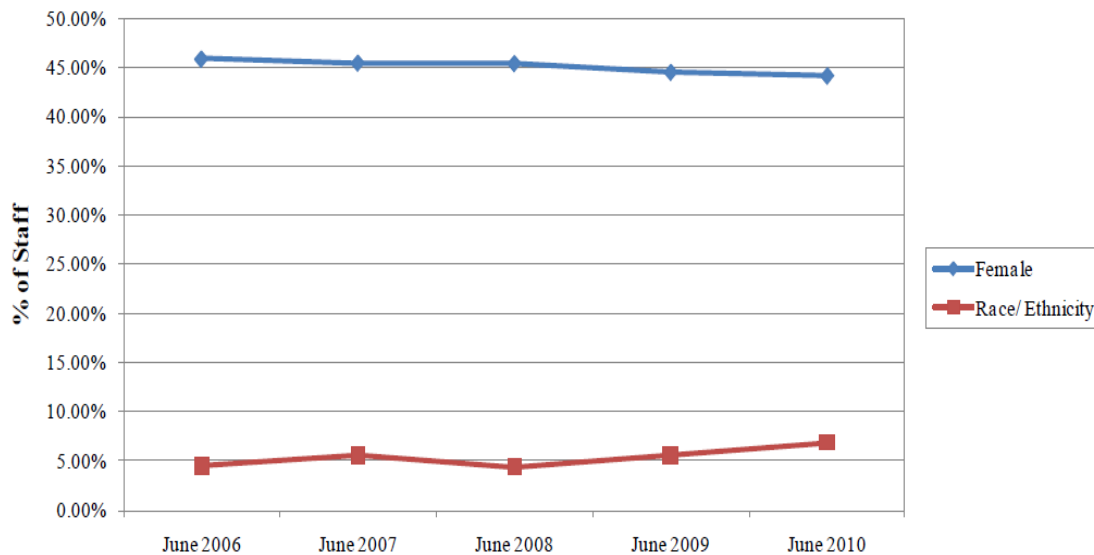
The provision of information by staff on recognition as a member of a designated group is voluntary.

STAFF AND FAMILY LIAISON OFFICE

The Staff and Family Liaison Office (SFLO) came into service in November 2009, as one of the first implemented initiatives under ASIO's strategic agenda. Its purpose is to provide an integrated model of wellbeing services that meets the needs of staff and families while supporting the Organisation's requirements.

Since implementation, the SFLO has introduced a range of highly successful products and services, including:

- Family Information Evenings – these events aim for greater inclusion, providing family members with the opportunity to increase their understanding of ASIO as an Organisation and the support services that are provided to assist them. In 2009–10, Family Information Evenings were held at ASIO's Canberra, Sydney, Melbourne, Adelaide and Perth Offices.
- Transition support – the SFLO provides briefings and individual appointments for officers and their families who are undertaking a geographical move. "Welcome" and "Transition" packs are also available to staff.

- Briefings at Intelligence Assessment Centres, aimed at alleviating some of the uncertainty potential officers may face concerning a move to Canberra and/or the Organisation.
- Information briefings to staff members and their families commencing an overseas posting. The primary purpose of these briefings is to articulate the services available to Australia-based family members and to ensure emergency contact arrangements are known to facilitate immediate assistance, if necessary.
- Supportive counseling, crisis support and referral services for staff members and their families, including bereavement support.
- An Organisational play group for children of staff members on maternity or parental leave. The play group has a current uptake of 90 per cent of all officers on maternity leave and encourages ongoing links with the Organisation.

The SFLO also commenced coordination and management of the Employee Support Officer (ESO) Program in March 2010, which has been broadened to include officers within the Intelligence Development Program. The ESO Program links new officers with staff of at least twelve months experience, to assist them to develop networks within the Organisation and their understanding of ASIO's culture.

STAFF COMPLAINTS

In 2009–10, ASIO staff lodged two formal grievances. Both complaints were resolved with appropriate action taken. Eight matters were raised informally with Harassment Contact Officers and the Human Resource Management Section for the 2009–10 year. Three staff contacted either a Harassment Contact Officer or a member of the Human Resource Management Section for information on bullying, harassment or discrimination. This is comparable with the previous year.

As part of maintaining a harassment and discrimination free work environment, ASIO established a Complaints and Appeals Framework to ensure the timely and effective resolution of staff concerns. The framework includes the appointment of ASIO's first external, independent Ombudsman to resolve issues impartially, informally and in a timely manner.

During 2009–10, the Harassment Contact Officer Network was reviewed to ensure appropriate coverage across ASIO. All Harassment Contact Officers undertook specialist training with an external provider.

The Organisation's *Workplace Diversity Program*, *Disability Action Plan* and *Reconciliation Action Plan 2009–12* continued to ensure ASIO promotes an inclusive work environment for all staff. Throughout 2009–10, ASIO continued to meet its responsibilities under the Commonwealth Disability Strategy.

SEPARATION RATES

ASIO's separation rate for 2009–10 increased to five per cent compared with 4.5 per cent in 2008–09. However, ASIO still experienced a relatively low separation rate during the reporting period which compared favourably with the APS rate of seven per cent.

Separating staff members can participate in a voluntary exit interview in order to identify reasons for departure from the Organisation and address concerns requiring a management response. Approximately half of all separating staff in 2009–10 chose to participate in the exit interview. Reasons cited by separating staff include promotion and career opportunities, work/life balance issues, job satisfaction issues, retirement and a range of personal reasons. While the exit interview process did not reveal any systemic concerns requiring management response, it is expected that the Human Capital Framework programs and initiatives being developed such as career management, leadership development and a contemporary employment framework will facilitate the retention of staff.

ACCOMMODATION

New Central Office, Canberra

In July 2009, a sod-turning ceremony held on the site of ASIO's new central office on Constitution Avenue in Parkes, Canberra marked a significant project milestone. As at 30 June 2010, the base building architectural design work had been completed and the fit-out design was 85 per cent complete. Excavation work, which required the removal of 90,000 tonnes of rubble for the main building and structured car park facility, was completed.

Construction of the building commenced in September 2009 with construction of levels one, two and three well underway at the end of the reporting period. During 2010–11, construction activity will include the completion of the erection of the facade and continuation of the interior fit-out. Construction is progressing on schedule for the building to be handed over to ASIO in mid-2012, with the main relocation of ASIO staff to commence from late 2012.

The building is located within the Parliamentary Triangle in close proximity to key national security and intelligence partners. It will provide a flexible working environment that meets ASIO's operating requirements whilst fostering a culture that works closely within the broader international and national security community.

The building is being designed and constructed in partnership with the Department of Finance and Deregulation (Finance) and will accommodate up to 1,800 people. It will operate 24 hours per day, with a level of security commensurate with ASIO's intelligence functions. In the 2008–09 Budget the Australian Government approved $606m for the new building. This was reduced to $589m in the 2009–10 Budget when the proposed subtenant, the Office of National Assessments, withdrew from the project to pursue alternative leased accommodation.

Close financial management against the project schedule by ASIO and Finance (through a jointly chaired Steering Committee), has ensured the project is proceeding on time and within budget and scope. Given the nature of the security environment and the pace of technological change, it is inevitable that additional capabilities will need to be added to the new building to maintain ASIO's capability to provide sound advice to Government on issues of national security.

ASIO has developed an asset management plan to align the replacement of furniture and information and communication technology assets with the relocation to the new building, and to maximise the re-use of furniture and equipment where possible.

The building is being designed in close consultation with the National Capital Authority (NCA) to maintain adherence with the National Capital Plan and sympathy to the Griffin Legacy. The NCA has determined the development is consistent with the Plan and has provided works approvals for site establishment works, site works and building works (structural).

The project is being delivered in accordance with the Implementation Guidelines for the National Code of Practice for the Construction Industry and the requirements of the Office of the Federal Safety Commissioner.

In May 2010, a project update was provided to the Parliamentary Standing Committee on Public Works. The project team also provides regular briefings to government and commercial stakeholders and distributes newsletters to local residents advising of current and future site activity.

Surveys of the site for the new central office identified it was formerly used as a landfill area revealing a small percentage of soil was contaminated by bonded asbestos sheeting. The majority of soil that contained the sheeting has now been removed successfully from the site. The remainder of the material lies under the existing engineering service lines and will be removed progressively as these services are upgraded during construction. The removal process was approved by the ACT Environmental Protection Authority and the work practices were endorsed by WorkCover ACT. Chilean Needle Grass, which is a noxious weed in the Australian Capital Territory, was also removed from the site in accordance with the legislative requirements of the Australian Capital Territory and New South Wales.

The size and footprint of the building required the removal of most of the existing trees on the site. The trees removed were recycled as mulch and donated to the local community for the regeneration of school gardens. A landscape master plan has been prepared for the site which includes significant new plantings.

Management plans have been established for the preservation of a significant row of oak trees along Constitution Avenue.

EXEMPTION FROM THE PUBLIC WORKS COMMITTEE

The Governor-General granted the New Building Project an exemption from scrutiny by the Public Works Committee (PWC) 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.

The PWC was provided with a confidential progress report in May 2010. Further confidential briefings have been, and will continue to be offered to the Committee as the Project progresses.

STATE AND TERRITORY OFFICES

As a result of funding received in 2006–07 and 2007–08 following the *Review of ASIO Resourcing* by Mr Allan Taylor AM (Taylor Review) in 2005, ASIO established an integrated property upgrade program. The program was designed to meet ASIO's need to accommodate additional staff, undertake increased operational activities and refresh ageing facilities. ASIO finalised its funded reconfiguration and relocation program on 30 June 2010.

In addition to providing additional space for staff, ASIO's new and upgraded accommodation has enabled the Organisation to increase operational capability in the states and territories. These

projects have delivered quality accommodation that is flexible, multi-functional and meets the operational needs of the Organisation.

ASIO has developed considerable expertise in managing high security accommodation projects with complex infrastructure requirements. Each project has been delivered on time and within budget. The lessons learned from each project have passed to the next project and where practical are applied to the much larger new central office project in Canberra.

PUBLIC RELATIONS AND REPORTING

ASIO has introduced initiatives in recent years to improve accessibility and contact points into ASIO. This will remain an enduring priority and focus. In 2009–10, The Director-General of Security decided, under the provisions of the ASIO Act, to reveal publicly the identity of one of ASIO's Deputy Directors-General, Mr David Fricker.

In addition to ASIO's public statements through parliamentary accountability processes, ASIO also provides information to the public in a number of ways, including:

- the publication of ASIO's *Report to Parliament*;
- the ASIO website;
- responding to enquiries from the media; and
- public statements by the Director-General of Security and Deputy Director-General of Security, Mr David Fricker.

ASIO's REPORT TO PARLIAMENT 2009–10

ASIO produces a highly classified *Annual Report* which examines ASIO's operational and corporate activities for the financial year in some detail. The classified *Annual Report* is made available to members of the National Security Committee of Cabinet and a small group of senior Commonwealth officials. ASIO also produces an unclassified *Report to Parliament*, which provides a publicly available source of information on ASIO's activities during the reporting period, and is available on the ASIO website (www.asio.gov.au). ASIO is the only agency within the Australian Intelligence Community (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

ASIO is subject to scrutiny and oversight by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), and appears publicly in Senate Standing Committee on Legal and Constitutional Affairs hearings.

Parliamentary Joint Committee on Intelligence and Security

The PJCIS reviews ASIO's administration and expenditure, and may also conduct inquiries into matters relating to the intelligence agencies that have been referred to the PJCIS by the responsible Minister or by a resolution from either House of Parliament. The PJCIS is also responsible for reviewing the listing of an organisation as a terrorist organisation under the *Criminal Code Act 1995* (Cth) and reviewing ASIO's questioning and detention powers. The

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

In 2009–10, ASIO provided a classified report on its administration and expenditure to the PJCIS (*Review of Administration and Expenditure No. 8: 2008–09*). An unclassified version of this report is available on the ASIO (www.asio.gov.au) and PJCIS website (www.aph.gov.au/house/committee/pjcis/reports.htm). In addition to written reporting, ASIO appeared in front of a PJCIS hearing to respond to questions on administration and expenditure.

During the reporting period, ASIO provided other classified briefings to the PJCIS, including on the construction of ASIO's new central office. Members of the PJCIS also met with a group of ASIO's Intelligence Officer trainees. ASIO used these outreach activities to provide the PJCIS with further insight into ASIO's operating environment and to introduce the Committee to a broader range of ASIO staff.

Senate Standing Committee on Legal and Constitutional Affairs

ASIO was called to the Senate Standing Committee on Legal and Constitutional Affairs hearings twice in 2009–2010 (Additional Estimates on 8 February 2010 and Budget Estimates 24 May 2010). At both hearings the Director-General of Security was accompanied by ASIO's Deputy Director-General, Mr David Fricker.

ASIO responded to questions on a range of issues including:

- ASIO's detention powers under warrant;
- Security Assessments;
- the Counter-Terrorism White Paper;
- national security legislation;
- ASIO's new central office;
- budget and staffing;
- complaints to the Inspector-General of Intelligence and Security;
- the Counter Terrorism Control Centre; and
- the 2011 Intelligence Review.

ASIO also responded in writing to 22 Questions on Notice.

PUBLIC STATEMENTS

Throughout the reporting period, ASIO engaged in outreach activities to promote understanding of ASIO's unique role, to highlight challenges in the security environment, and to contribute to broader policy considerations and debate. The audience included Commonwealth and state and territory partners through initiatives such as Partnership Forums; academia through seminars; as well as the wider community through ASIO's new website.

Public comments about the activities of ASIO may be provided by the Attorney-General, as ASIO's Minister, the Director-General of Security, Deputy Director-General of Security, Mr David Fricker, or ASIO's Media Liaison Officer.

ENHANCEMENTS TO PUBLIC RELATIONS AND REPORTING

The ASIO website is the primary source of public information about ASIO. On 12 March 2010, a redeveloped modern website (www.asio.gov.au) was launched by the Attorney-General, the Hon. Robert McClelland MP. The website has a contemporary design and provides easy-to-access information across a range of topics, including broad details on the nature of ASIO's work. The careers section of the website provides information about roles within the Organisation and what applicants may expect from the recruitment process. Short videos provide an understanding of a range of roles within ASIO.

The website also provides publications such as ASIO's *Report to Parliament* and previous submissions to the PJCIS, and links to related sites including the Attorney-General's website and other members of the AIC.

A number of journalists from the Parliament House Press Gallery attended the launch, which provided an opportunity for journalists to enter ASIO headquarters and meet ASIO staff.

INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office holder who reviews the activities of the agencies of the AIC (ASIO, the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate and the Office of National Assessments). The IGIS's mandate is to ensure the Australian intelligence agencies act legally, with propriety, comply with ministerial guidelines and directions and respect human rights.

The IGIS is a core component of the rigorous oversight and accountability framework within which ASIO operates. In respect of ASIO, the IGIS has both an inspection and an inquiry role.

Inspection

The IGIS conducts ongoing inspection and monitoring of ASIO activities (particularly operational activities), which include regular reviews of:

- investigation authorisation and warrant documentation;
- the conduct of counter-terrorism, counter-espionage and counter-intelligence investigations, including special powers operations;
- engagement with other Australian agencies, and ASIO's access to their data;
- interactions with international liaison partners and ASIO's communications on Australian citizens and residents to those partners; and
- compliance with legislation, Attorney-General's Guidelines, and internal policies and procedures.

Inquiry

The IGIS has the authority to inquire into public complaints, conduct inquiries referred by Government, and initiate 'own motion' inquiries. At the conclusion of an inquiry, the IGIS reports conclusions and recommendations. While there is no legal obligation for the Director-General of Security to comply with the recommendations, ASIO works collaboratively with the IGIS to resolve issues.

Regular engagement with ASIO's Senior Executive

ASIO coordinates a regular monthly senior meeting with the IGIS that allows an exchange of views on strategic issues of common interest, and provides an opportunity to elevate issues arising out of inspections or inquiries, or for the IGIS to be provided with specific briefings if requested or considered useful by ASIO.

Where appropriate and relevant to issues of legality, propriety and human rights, ASIO consults the IGIS on the development of policy guiding its activities. ASIO, on an ongoing basis, also seeks to provide the IGIS with early advice of emerging issues impacting on the Organisation, to assist understanding of the environment ASIO is operating in and challenges faced. In 2009–10, ASIO consulted with the IGIS in drafting internal policy documents including on ASIO communication with foreign authorities, and the consolidation of ASIO's internal policies and practices prohibiting use or involvement in torture and other cruel, inhuman or degrading treatment or punishment.

Complaints

The IGIS made 811 administrative inquiries to ASIO during the reporting period, an increase from 153 in the previous financial year. The IGIS has confirmed that the increase in complaints does not indicate an increase in issues with, or failings by, ASIO. Of the 811 enquiries, the IGIS found that only two complaints related to administrative error by ASIO – both of which were acted on immediately to avoid similar errors from occurring. Twenty-six per cent of the enquiries made were not with ASIO at the time of enquiry, having already been completed, or had not yet been referred to ASIO by DIAC.

Based on the various monitoring, inspection and inquiry activities undertaken by the Office of the IGIS in 2009–10, the IGIS was satisfied that there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety or the law. Further details can be found in the IGIS's *Annual Report* at www.igis.gov.au.

INDEPENDENT NATIONAL SECURITY LEGISLATION MONITOR

When appointed, the Independent National Security Legislation Monitor will have jurisdiction to review the effectiveness of, and appropriate safeguards relating to, Australia's counter-terrorism and national security legislation. With respect to ASIO's work, this relates to Division 3 of Part III of the ASIO Act dealing with special powers relating to terrorism offences (questioning and questioning and detention powers), and the provisions of the *National Security*

Information (Criminal and Civil Proceedings) Act 2004, insofar as ASIO is involved in litigation. The Prime Minister and/or the PJCIS may also refer matters relating to counter-terrorism or national security to the Monitor.

INTEROPERABILITY

ASIO engages closely with counterparts both in Australia and overseas to develop and share technical, analytical and investigative capability. ASIO is committed to the principles of sharing information and integrating capability to ensure there is a single focused strategic effort on national security at the Commonwealth level. ASIO is partnering with a number of agencies in the national security community to ensure that its leading edge capabilities and capacity are deployed effectively to deliver the best outcomes for Australia and its partners. ASIO has also expanded its program of national and international exchanges and secondments, and will continue its successful Partnership Forum series and the program of attachments, which enable direct interaction between partner agencies and ASIO.

THE STREET REVIEW OF INTEROPERABILITY

On 22 November 2007 the Commissioner of the Australian Federal Police (AFP) appointed a National Security Operations Review Committee chaired by Sir Laurence Street AC KCMG QC, and including retired New South Wales Police Commissioner, Mr Ken Moroney AO APM, and the former Director of the Defence Signals Directorate (DSD), Mr Martin Brady AO. The Terms of Reference for the *Review of Interoperability between the Australian Federal Police and its National Security Partners* (Street Review) included an examination of the adequacy of existing practices, policies and inter-agency governance and frameworks.

The Review delivered ten recommendations designed to significantly improve the way joint agency counter-terrorism investigations are managed in the future. The recommendations cover four broad areas including operations decision making processes, joint task force arrangements, information sharing, and training and education.

MAJOR INITIATIVES 2009–10

During 2009–10, a major initiative to enhance ASIO's interoperability with the national security community was the establishment of the multi-agency CTCC. Announced in the February 2010 *Counter-Terrorism White Paper,* the CTCC became operational in May 2010. Although the CTCC is a small unit (of senior and experienced officers), it represents a major shift in the way counter-terrorism has been managed in Australia at the Commonwealth level. ASIO leads the CTCC, which will ensure that the Commonwealth's counter-terrorism intelligence and investigative activities are fully coordinated and draw as appropriate on the full range of capability that resides within Australia's national security community.

ASIO is also working in partnership with the AFP and other Commonwealth agencies to provide coordinated technical assistance to other Australian intercepting agencies. In 2010–11 ASIO will conduct a pilot study for the establishment of a National Interception Technical Assistance Centre (NiTAC). The NiTAC is planned to provide a central point of reference from which agencies can receive technical assistance to help keep pace with the rate and scale of technical change.

FURTHER ENHANCEMENTS TO INTEROPERABILITY

ASIO is working to ensure its capabilities and capacity are deployed effectively to help its partners through a range of initiatives. These include the establishment of the NiTAC; enhanced client focus, responsiveness, and accessibility; an expanded program of ASIO Partnership Forums across the national security community; and development of Stakeholder Engagement Plans to enhance the Organisation's outreach and influence within the national security community, Parliament, media, private sector and academia inter alia.

ASIO also collaborates with other agencies in the area of capacity building. In 2009–10, ASIO worked with the AFP to develop the Commonwealth Technical Response Capability (CTRC), effective from 1 July 2010. The CTRC will provide state and territory law enforcement agencies with the ability to draw on the technical resources of ASIO and the AFP at short notice in circumstances of urgency (such as a terrorist incident) or during peak requirements (such as a major event).

The formalisation of relationships with other agencies has also been important in ensuring a shared understanding, and effective employment, of agency capabilities.

ACCOMMODATION ARRANGEMENTS AND INTEROPERABILITY

ASIO's new central office will facilitate interoperability with the national security community through specialised facilities. These facilities incorporate Top Secret classified conference rooms, auditorium, operational taskforce accommodation, technical facilities and the capacity to host Top Secret Information and Communication Technology equipment within the data hall.