ASIO SUBMISSION TO THE

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

REVIEW OF ADMINISTRATION AND EXPENDITURE

No. 10: 2010–11

Contents

Figures

Tables

Scope of Review

The Australian Security Intelligence Organisation (ASIO) annual review to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into Administration and Expenditure No. 10 provides a detailed account of ASIO's activities during the financial year. For 2010–11, the PJCIS has requested a submission covering all aspects of administration, including:

- Any legislative changes impacting on administration, including the frequency and nature of use of these powers, the amount of time expended on particular areas, the implications for staffing, training, the role of legal officers, the need for specialist staff, the relationship with outside agencies such as the police or the judiciary;
- An update on human resource management: recruitment, retention and training, workplace diversity, language skills, staff complaints, separation rates and accommodation;
- Structure of the organisation and the distribution of staff across different areas of the organisation, the ratio of field and operational staff to administration staff, executive to middle and lower level staff, central office to outlying staff;
- Pressures of expansion;
- Security clearances – current procedures, timelines, delays and any associated outsourcing arrangements;
- Security breaches – e-security arrangements and enhancements;
- Public relations and/or public reporting, where relevant;
- Direction and strategic planning and the management of expansion; and
- Performance management and evaluation.

This report examines ASIO's activities and performance in the areas requested above to provide the PJCIS with visibility of the fiscal, administrative and operational performance of the Organisation.

ASIO’s Role and Functions

ASIO is Australia’s security service. Its role and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). ASIO’s primary function is to collect, analyse, assess and disseminate security intelligence. Security intelligence is concerned with a specific set of activities that might harm Australia, Australians or Australian interests here and abroad. Those activities are:

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

ASIO’s responsibility for security intelligence extends beyond Australia’s borders and includes Australia’s ‘security’ obligations to other countries. The ASIO Act also 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 in accordance with the Attorney-General’s Guidelines;
- assesses security intelligence and provides advice to Government on security matters;
- investigates and responds to threats to security;
- maintains a national counter-terrorism capability;
- provides protective security advice; and
- provides security assessments, including for visa entry checks and 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, including interception of telecommunications, enter and search of premises, and compelling persons to appear before a prescribed authority to answer questions relating to terrorism matters. ASIO is also responsible for collecting foreign intelligence under warrant within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence, and maintains specialist capabilities that can be deployed to assist in intelligence operations and incident response.

As ASIO is the only agency in the Australian Intelligence Community (AIC) authorised in the course of its normal duties to undertake security investigations into, and collect intelligence on, the activities of Australians, it operates within a particularly stringent oversight and accountability framework. The foundation of this framework is the ASIO Act, which was created to recognise the importance of individual rights, while also endeavouring to safeguard the public’s collective right to be secure. The Inspector-General of Intelligence and Security, an independent statutory authority, also plays an important role in overseeing ASIO’s activities as does the PJCIS.

Executive Overview

The Security Environment 2010–11 and Outlook

The threat posed by terrorism and Islamic extremism remained the most immediate and significant factor influencing the security of Australia and Australian interests and people here and overseas during 2010–11. This is despite a number of significant international counter-terrorism developments including the deaths of Usama bin Laden and other key al-Qa'ida identities and the arrest of senior South-East Asian extremist figures. Foreign conflicts continued to act as drivers and motivation for extremism and Australia remains a target for terrorism. The four potential mass casualty attacks within Australia disrupted in the past ten years were inspired by an ideology imported from overseas, but largely the individuals involved are Australians. Throughout 2010–11, ASIO continued to work closely with the Attorney-General's Department on countering extremist views and beliefs.

Stand-alone jihadists or small groups, often with tenuous or no links to established groups, are emerging with increasing frequency as a significant security threat.

Espionage remains an enduring risk to Australia's security. While the traditional methods of espionage continue to be the backbone of the threat, espionage through cyber means has emerged as a serious and widespread threat. In July 2010, a dedicated Cyber Espionage Branch was established in ASIO, reflecting the growing significance of this activity in regard to Australia's national security.

In support of the Government's intelligence-led approach to combating people smuggling and following legislative amendment, ASIO established a dedicated border integrity investigation function. ASIO's effort was focused on supplementing the work of lead agencies countering people smuggling.

The security challenges for Australia from terrorism, espionage and foreign interference will not diminish in the near term. While overseas developments and connections will remain a central factor in the overall threat to Australia, the phenomenon of home-grown extremism will continue, particularly given the increased technological sophistication of international extremists in distributing a message of radicalisation around the world which individuals can use to develop and pursue their own extremist agenda.

The drivers and influences on foreign powers to engage in espionage and foreign interference are enduring. Foreign powers will continue to engage in these activities in the future, seeking to achieve their policy goals and extend their national influence and capabilities at Australia's expense. Cyber-espionage is likely to become even more significant in the future, given the increasing reliance of the government and business sectors on information technology systems.

The task of responding to traditional and new security challenges has become considerably more complex. Against this backdrop, ASIO will need to continue to enhance its capabilities and foster close collaboration with key national and international partners in order to preserve Australia's security.

Reporting	ASIO investigations and liaison partnerships contribute to the production of security intelligence and threat assessment advice. In 2010–11, ASIO produced 2,967 reports and assessments, including 575 threat-related products covering topics such as the implications for the security of Australia and Australians of the 'Arab Spring', the deaths of senior terrorist figures like Usama bin Laden and Anwar al-Aulaqi, the G20 Summit in Korea and the Commonwealth Games in New Delhi. ASIO's intelligence reporting was distributed to 347 partners, both domestic and foreign.

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' as defined in the ASIO Act.

In 2010–11, ASIO recorded an operating deficit of $33 million, due to the introduction of Net Cash Funding. Excluding depreciation, ASIO achieved a small operating surplus of $6 million.

Funding and Expenditure	In 2010–11, ASIO's total program expenses were $386 million, representing a 3 per cent increase from a total of $376 million in 2009–10. Government provided funding of $345 million for cash expenditure only (following the introduction of Net Cash Funding), and an additional $8 million was received from independent sources. The estimated total cost for program expenses for 2011–12 is $403 million.

Structure of the Organisation

On 1 July 2010, ASIO implemented a new ten division structure, designed to better allocate resources while aligning skills and work group functions to enhance organisational performance and interconnectivity across divisions.

Corporate Direction and Strategic Planning

During 2010–11, the ASIO Strategic Plan 2011–13 was launched, which will ensure ASIO is better prepared to meet Australia's security intelligence challenges now and into the future. The plan highlights ASIO's strategic direction and sets out four key strategic goals to achieve by 2013: to strengthen intelligence collection and analysis capability; to enhance strategic impact; to build and manage the workforce of the future; and to improve business processes and practices. A range of projects were undertaken in the reporting period to address these areas of strategic change, including a change to the internal prioritisation of counter-terrorism investigations, a series of collaboration initiatives with AIC partners, including the establishment of the Counter Terrorism Control Centre (CTCC).

In the reporting period, ASIO introduced a uniform approach to business planning to ensure the optimal allocation of resources and to meet new challenges through continuous improvement, while addressing potential risks. ASIO also launched a new project management framework in 2011, establishing a single, consistent approach to initiating, running and governing projects across the Organisation.

In 2010–11, ASIO's internal audit team became an independent functional unit operating under the Office of the Director-General and Deputy Directors-General and reporting to the Chair of the Audit and Evaluation Committee. The committee also includes two external members, including representation from the Australian National Audit Office, reinforcing the independence of the internal audit role.

ASIO maintains a robust fraud detection and control strategy. During 2010–11, seven incidents of alleged fraud were reported within or against ASIO, with one found to be actual fraud against ASIO. These incidents were dealt with in accordance with the ASIO Fraud Control Plan.

Human Resource Management

ASIO's recruitment activity in 2010–11 was focused on positioning the Organisation to fulfill the target of 1,860 full-time staff by the 2012–13 budget cycle, to meet the recommendation in the Review of ASIO Resourcing conducted by Mr Allan Taylor AM in 2005.

ASIO launched a new People Capability Framework in October 2010, allowing the Organisation to more accurately describe the capabilities and behaviours required of its workforce to deliver broader and more complex outcomes to the Australian Government. The People Capability Framework is based on the Australian Public Service Integrated Leadership. ASIO also redesigned its performance management processes. The new Enhancing Performance Framework cultivates leadership skills, supports more effective performance management and places an emphasis on staff development.

Highlighting the need for national and international cooperation to ensure security intelligence outcomes, ASIO staff undertook a number of attachments to domestic and foreign partners throughout 2010–11, including at the operational and Senior Executive Service levels.

In February 2011, the Director-General launched ASIO's new anti-bullying and anti-harassment campaign, 'Silence Hurts'. The campaign aligns with ASIO's values and Code of Conduct and is designed to prevent and stop bullying and harassment in the workplace and to encourage staff to 'speak up' when they experience or witness inappropriate behaviour.

Recruitment / Separations

In 2010–11, 196 new staff were recruited to the ASIO workforce, resulting in net growth of 78 and total staff of 1769. ASIO continues to use the internet as well as print media to engage with prospective employees, with advertisements appearing across a range of online media.

During 2010–11, ASIO experienced a slight increase in the separation rate from 5 per cent in 2009–10 to 5.8 per cent in 2010–11, with this level still comparing favourably to the Australian Public Service average separation rate of 7 per cent.

Training

Training and professional development continued as a major focus for ASIO in 2010–11. Throughout the reporting period, streamlined training opportunities were available to staff covering investigative techniques, intelligence tradecraft, surveillance techniques and linguistic monitoring, as well as enhanced leadership and management programs.

In 2010–11, 42 officers graduated as Intelligence Professionals from ASIO's Intelligence Development Program, reflecting ASIO's significant investment to meet capability development requirements.

Accommodation

In 2010–11, the majority of external works were completed on ASIO's new central headquarters, and the fit out components of construction commenced, with over 500 contractors employed on the project overseen by ASIO project managers. The progress of the development, together with timelines for moving staff into the new building, continues to be tightly managed with a slight delay in occupation by ASIO staff anticipated. There will be no requirement to seek additional funding from the Government.

In the reporting period, the program which commenced in 2006 to accommodate growth in state and territory offices was completed, enhancing ASIO's operational capability throughout Australia.

Legislation and Litigation

Throughout the reporting period, ASIO provided contributions and input to several proposed legislative amendments and policy developments, including the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011*, the Intelligence Services Legislation Amendment Bill 2011 and the Telecommunications Legislation Amendment (Cybercrime Convention) Bill 2011.

ASIO continued to contribute actively to prosecutions in national security cases, with ASIO officers and information often required in evidence or in responding to requests or subpoenas from the prosecution or defence. The diverse nature of the legal proceedings ASIO is involved in – including criminal (particularly terrorism) prosecutions, judicial and administrative reviews of security assessments and a range of civil actions – continues to produce a significant and increasing workload within ASIO.

Involvement in Litigation

In 2010–11, ASIO was involved in over 59 litigation matters, including criminal (particularly terrorism) prosecutions, judicial and administrative reviews of security assessments, and a range of civil actions.

ASIO Security Assessments

ASIO security assessments continued to be a significant area of activity for the Organisation, with large numbers of visa, personnel and counter-terrorism security assessments undertaken in the 2010–11 period. ASIO's priority in these processes is ensuring Australia's national security is not compromised through an inefficient or inappropriate security assessment process.

In 2010–11, ASIO developed and implemented a security referral framework for irregular maritime arrivals (IMAs) which enabled a focus on complex IMA cases requiring investigation and streamlined the process for non-complex cases. This will assist ASIO's contribution to the whole-of-government border security arrangements.

Visa Security Assessments	ASIO completed 34,396 visa security assessments in 2010–11, including 3,586 for irregular maritime arrivals (IMAs). 45 adverse assessments were issued in relation to visas, including 40 on terrorism grounds, two on the grounds of involvement in people smuggling or other threats to Australia's border integrity and three on espionage or foreign interference grounds.
Counter-Terrorism Security Assessments	ASIO completed 109,166 counter-terrorism security assessments in the reporting period, 97,922 of which were Aviation Security Identity Card and Maritime Security Identity Card assessments. This represents an eleven per cent increase from 2009–10. Two adverse and two qualified assessments were issued during the reporting period.
Personnel Security Assessments	In 2010–11, ASIO completed 31,099 personnel security assessments, including 3,100 for Top Secret Positive Vetting, 7,512 for Negative Vetting Level 2 and 20,487 for Negative Vetting Level 1. Two qualified personnel security assessments were issued in 2010–11. This is consistent with statistics from the previous financial year.
Protective Security	In the reporting period, ASIO's protective security advice to both government and the private sector assisted with the protection of classified information, premises and other assets. This included the provision of security advice for the Commonwealth Heads of Government Meeting (CHOGM) in October 2011 in Perth, as well as protective security and risk management training.

Security of ASIO

The protection of ASIO information and advice, staff identity, subjects of investigations and operations, and methodology is integral to the ongoing effectiveness of the Organisation. ASIO security policies meet or exceed the standards laid down in the Australian Government Protective Security Policy Framework. These policies support staff to uphold the highest standards of security practice. ASIO also invests heavily in staff security awareness and education.

In 2010–11, ASIO maintained a strong security culture and continued to work closely with other government agencies to provide advice to both the government and private sector to mitigate threats to security.

ASIO's information technology (IT) security program provides assurance that ASIO's information and communications systems are being used in an authorised, secure and appropriate manner, through audits, investigation of IT security incidents and IT security policy and advice. In the reporting period, the protection of ASIO externally connected IT systems from attempted cyber attacks was a particular focus of security attention. Another important body of work undertaken during the reporting period was the implementation of an information sharing business model to protect the security of ASIO information as the Organisation moves to a single information environment.

Management of Relationships and Public Reporting

Over 2010–11, ASIO continued to develop collaboration with domestic partners in support of ASIO's roles and functions. This included the development of closer operational partnerships, an expanded secondment and attachment program with key domestic partners and the introduction of more regular senior management meetings with key partner agencies.

Partnerships	On 21 October 2010, the Counter Terrorism Control Centre (CTCC) was officially launched in ASIO. As a joint agency team, the CTCC has strengthened the coordination and development of a strategic approach on counter-terrorism priorities while also improving interoperability and cooperation within the AIC. ASIO has also contributed to greater connections and cooperation with other agencies through the regular hosting of Senior Officer Partnership Forums and SES Officer Partnership Forums, bringing together officers to network and to increase familiarity with ASIO's roles and functions.
Business Liaison	ASIO's Business Liaison Unit (BLU) continued to provide appropriate unclassified security intelligence advice to domestic commercial partners with the aim of increasing awareness and responsiveness to threats to security. At the end of the reporting period there were more than 260 reports on the BLU website. As at 30 June 2011, there were 950 subscribers to the BLU website. There were 145 companies participating in the Register of Australian Interests Overseas, with over 1,270 facilities registered in 85 countries worldwide.

In 2010–11, ASIO continued to expand the breadth and depth of its international engagement in recognition of ASIO's security mandate extending beyond the geographic boundaries of Australia. International liaison relationships are a potent force multiplier for ASIO, enabling the Organisation to draw on the information, expertise and capability of overseas partners to pursue security intelligence investigations that transcend national boundaries.

Foreign Liaison	In response to the global dimension of threats from terrorism and espionage activities, as at 30 June 2011, ASIO had 334 approved liaison relationships with security, intelligence and law enforcement agencies in 123 countries around the world with ASIO's program of engagement covering the full range of its functions and activities.
Technical Capability Expansion	Throughout the reporting period, ASIO's development of technical, surveillance and language capabilities supported both ASIO's work and that of ASIO's domestic and international partners. This included strengthened resource sharing of foreign language capabilities, the contribution of ASIO's technical expertise to support whole-of-government telecommunications interception policy development and the provision of support to the development and maintenance of national capability through the National Interception Technical Assistance Centre (NiTAC) pilot program.

During 2010–11, ASIO continued to engage publicly through speeches and appearances by the Director-General of Security. The Director-General spoke on numerous occasions throughout the year, including to community events, universities, research and private industry groups and at official government functions. The speeches covered a variety of topics, including the current security environment and cyber-security, and are uploaded to the ASIO website to increase public awareness of ASIO's roles and functions.

In 2010, ASIO re-launched its website to include a modern design interface and an emphasis on providing the Australian public with greater access to information about the Organisation, its people and its work.

ASIO continued active engagement with members of the Parliament and Senate, including through the highly classified Annual Report to Parliament 2010–11, which was made available to members of the National Security Committee of Cabinet and a small group of senior Commonwealth officials. ASIO also produced an unclassified Report to Parliament, which provides a publicly available source of information on ASIO's activities throughout the reporting period, and is available on the ASIO website.

Parliamentary Oversight

In March 2011, ASIO appeared before the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to respond to questions on administration and expenditure, and appeared again in June 2011 at a public hearing to respond to questions on security assessments. ASIO attended two hearings of the Senate Standing Committee on Legal and Constitutional Affairs during the reporting period, responding to questions on a range of issues including security assessments, ASIO's new central office, budget and staffing. During the reporting period, ASIO responded in writing to 29 questions on notice. The Director-General of Security also appears before other committees of the Senate and Parliament as required, including the Joint Select Committee on Australia's Immigration Detention Network.

The Security Environment 2010–11 and Outlook

Terrorism

The threat posed by terrorism and Islamic extremism remained the most immediate and significant factor influencing the security of Australia and Australian interests and people here and overseas during 2010–11. Foreign conflicts continued to act as drivers and motivation for extremism in 2010–11, including the conflict in Afghanistan, which has energised and fuelled feelings of resentment towards the West, risking the manifestation of this resentment in acts of terrorism. The longstanding conflict between the Palestinians and Israel also continues to provide a source of extremism which can be reflected outside the Middle East in Western countries.

Australia remains a target for terrorism. In the past ten years, four potential mass casualty attacks within Australia have been disrupted only because of the work of intelligence and law enforcement agencies. While they have been inspired by an ideology imported from overseas, largely the individuals involved are Australians. Three of these planned attacks would have been the work of groups with little or no contact with international affiliates.

Stand-alone jihadists or small groups, often with tenuous or no links to established groups, are emerging with increasing frequency as a significant security threat. International extremist figures are specifically targeting English-speaking audiences in the West and encouraging individuals to take action using whatever means are at their disposal without seeking any further sanction. The distribution of these messages via the internet is of particular concern as it amplifies both the reach and the immediacy of the message. ASIO remains aware of the threat from these lone actors and has been working to increase the likelihood that such individuals can be identified.

A number of events occured in 2010–11 which had the potential to impact on the global counter-terrorism environment, most notably the deaths of Usama bin Laden and Anwar al-Aulaqi, Harun Fazul, a senior operative of al-Q'aida in East Africa. There were also significant arrests including Abu Bakar Ba'asyir, Emir of Jamaah Ansharut Tauhid (JAT) and Umar Patek, a Jemaah Islamiyah member, both alleged masterminds of the 2002 Bali bombings. While these events represent a setback for the affected terrorist groups, ASIO assesses the groups or their supporters maintain an active intent and, in some cases, the ongoing capability to pose a threat to Australia or Australian interests.

Withholding passports is an important means of preventing Australians from travelling overseas to train, support or participate in terrorism. It may also be used to help prevent an Australian already overseas from participating (or further participating) in activities that are prejudicial to the security of Australia or another country. Under the Australian Passports Act, ASIO may request the cancellation of an existing Australian passport, as well as the refusal of an application for a new Australian passport, on security grounds. Under the Foreign Passports (Law Enforcement and Security) Act, an adverse ASIO security assessment can also be grounds for the Minister for Foreign Affairs to demand the surrender of a foreign travel document.

At the conclusion of the reporting period, ASIO was investigating more than 150 active counter terrorism investigations.

Communal Violence and Violent Protests

The past twelve months have seen a number of politically motivated protests in Australia covering a wide range of issues. In accordance with the ASIO Act, ASIO's investigative interest in protest is limited to that which is unlawful or violent. The only exceptions to this are demonstrations or other protest activities against internationally protected persons or other persons specified by the Attorney-General. ASIO may prepare threat assessments in relation to any demonstration or protest activity on the basis of information that it already has or that is passed to the Organisation by other agencies, for the purpose of advising authorities responsible for law enforcement and the protection of designated persons. Many of the conditions conducive to communal violence are present in Australia, including tensions arising from conflicts overseas and a small number of people who actively promote hate between segments of society. Fortunately, the number of people involved and the scale of violent protest has been relatively low.

Espionage and Foreign Interference

Espionage is an enduring threat to Australia's security. While the traditional methods of espionage, suborning Australians and others to obtain information or provide support for foreign intelligence agencies and using technology to access communications or conversations, continue to be the backbone of the threat, espionage through cyber means has emerged as a serious and widespread threat. This is likely to continue to gain prominence with the increasing reliance of the commercial, government and military sectors on digital technology. In July 2010, a dedicated Cyber Espionage Branch was established in ASIO, reflecting the growing significance of this activity in regard to Australia's national security.

Proliferation

Australia has existing legislative obligations to ensure compliance with the various United Nations Security Council Resolutions aimed at preventing the spread of Weapons of Mass Destruction (WMD) capabilities.

In 2010–11, ASIO contributed to Australia's support for international counter-proliferation efforts by investigating cases of possible access to WMD technology and materials by countries or individuals of proliferation concern.

Border Security

The ASIO Act was amended in June 2010 to provide ASIO with a new function to investigate serious threats to Australia's territorial and border integrity. ASIO is consequently able to use its capabilities to support the whole-of-government effort to combat people smuggling. In the previous twelve months, ASIO's contribution was focused on onshore elements of international maritime people-smuggling networks facilitating the passage of people to Australia. ASIO investigations identified several groups and individuals of security concern targeting Australia for irregular migration.

During the reporting period, ASIO worked closely with partner agencies to ensure our efforts are focused on preventing harm to Australian interests by identifying people seeking to enter Australia who are assessed to be a threat to security.

In 2010–11, ASIO completed 34,396 visa security assessments, including 3,586 assessments for irregular maritime arrivals (IMAs). 45 adverse assessments were issued in relation to visas, including 40 on terrorism grounds, two on the grounds of involvement in people smuggling or other threats to Australia's border integrity and three on espionage or foreign interference grounds.

Outlook for the Security Environment

The security challenges for Australia from terrorism, espionage and foreign interference will not diminish in the near term. The terrorism challenge is driven by ideas and radicalisation processes, which will continue to be attractive to some. It only requires relatively few individuals, or in the case of a lone actor, one individual, to carry out a mass casualty attack which would cause serious loss of life, economic harm or damage to our social cohesion. Overseas developments and connections remain a central factor in the overall threat to Australia, so the security environment in the future will continue to be shaped by broader international political and security-related developments. Despite this, it is likely the phenomenon of 'home-grown extremism' will remain in the future, particularly given the increased technological sophistication of international extremists who seek to distribute a message of radicalisation around the world which individuals can use to develop and pursue their own extremist agenda.

The drivers and influences on foreign powers to engage in espionage and foreign interference are enduring. Foreign powers will continue to engage in these activities, seeking to achieve their policy goals and extend their national influence and capabilities at Australia's expense. Technological developments continue to present foreign states and non-state actors with increased opportunities to access and exploit electronic information systems remotely and an increased reliance on integrated systems in government and business sectors will be a key vulnerability if not properly addressed.

As the international political environment continues to change rapidly, issue motivated groups in Australia will continue to pursue peaceful and non-violent means of protest. However, it remains likely that only a small number of activists will pursue violent protest as a method to attempt to influence government and business leaders. ASIO, through ongoing close cooperation with law enforcement agencies and other partners, will continue to assess possible threats that may arise through violent protest.

The task of responding to traditional and new security challenges has become considerably more complex. Against this backdrop, ASIO will need to continue to enhance its capabilities and foster close collaboration with key national and international partners in order to preserve Australia's security.

Expenditure

Budget Growth

ASIO's budget is set out in the Portfolio Budget Statements, with the audited outcome published in ASIO's annual *Report to Parliament*. Portfolio Budget Statements are prepared annually, consistent with the Government's budgeting requirements, with Portfolio Additional Estimates Statements also prepared if new measures are approved by the government post-Budget.

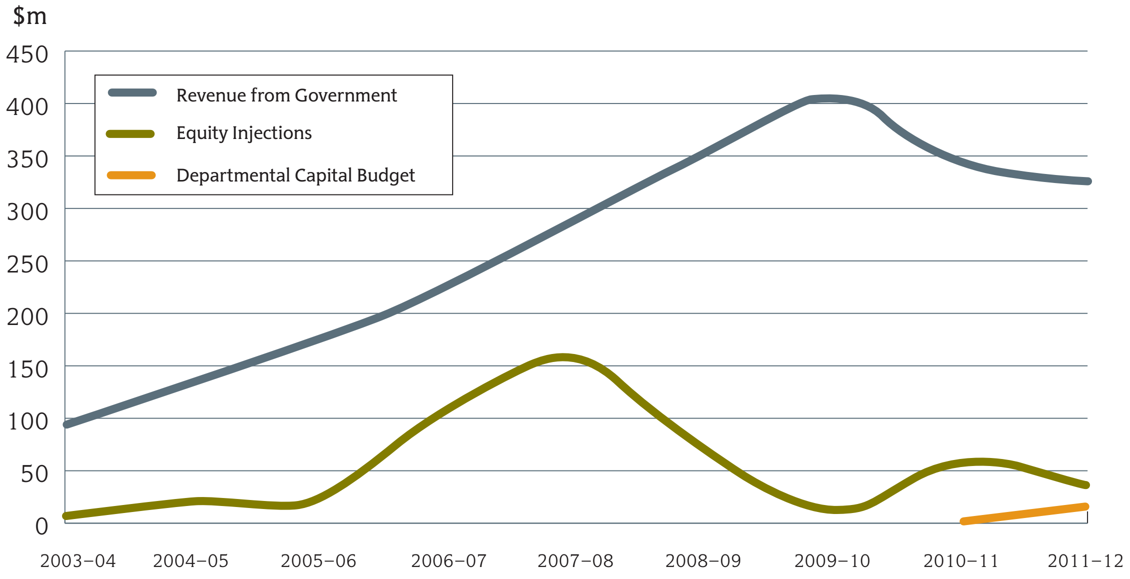
The Australian Government introduced Net Cash Funding in 2010–11, resulting in two significant funding changes:

- agencies are no longer funded for depreciation; and
- asset replacement will be funded by a departmental capital budget.

ASIO's funding in 2010–11 expressed in terms of total price of outputs was $353 million, a decrease of $62 million (15 per cent) from 2009–10. Revenue from government decreased by $61 million (15 per cent) to $345 million from $406 million in 2009–10.

ASIO received an equity injection in 2010–11 of $61 million towards the ASIO New Building Project. The Departmental Capital budget for 2010–11 was $5 million for ASIO's ongoing asset replacement. Two similar capital appropriations will be received in 2011–12 – an equity injection of $42 million towards the ASIO New Building Project, and a departmental capital budget of $19 million for asset replacement.

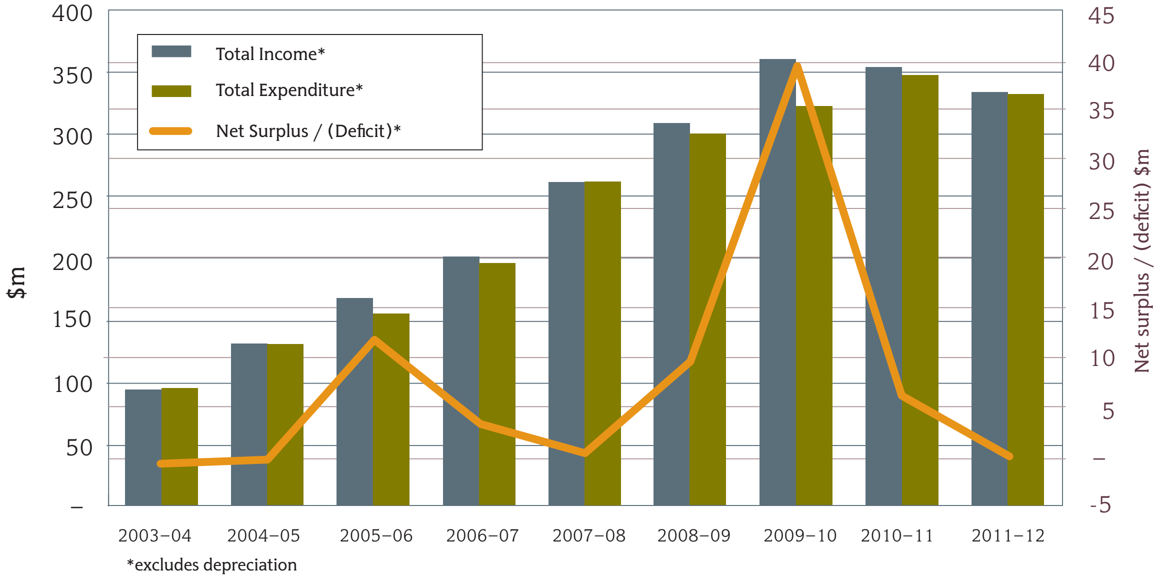
Figure 1: Revenue from Government: 2003–04 to 2011–12



Financial Performance

ASIO recorded an operating deficit of $33 million in 2010–11 due to the introduction of Net Cash Funding. Excluding depreciation, ASIO achieved an operating surplus of $6 million. This adjusted surplus represents 2 per cent of revenue, with recruitment challenges making the most significant contribution to the variance.

Figure 2: Financial Performance: 2003–04 to 2011–12

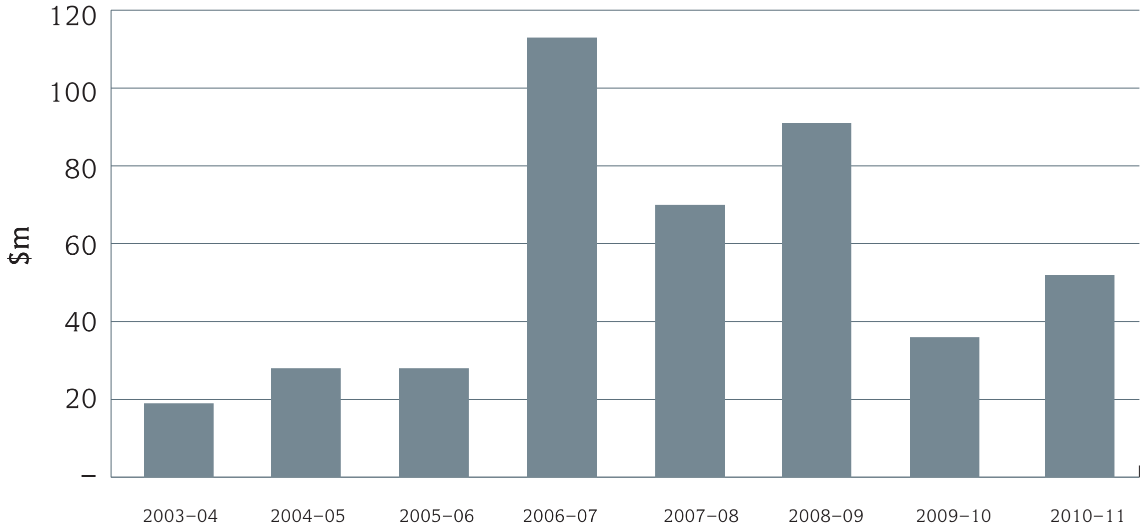


Strategic Allocation of Resources

Resource allocation is formally reviewed by ASIO's senior executive to ensure appropriate resources are directed to the functional areas of the Organisation. The 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 ASIO Corporate Executive, the main ASIO forum for managing strategic corporate resource issues. Divisional base budgets, the internal investment program and NPPs are monitored and driven by the Corporate Executive on a monthly basis.

Figure 3: Purchase of Capital Items 2003–04 to 2010–11



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. Reporting covers current and future Organisational financial performance matters and strategic financial management planning. Financial management practices are supported by a financial management information system with integrated internal controls aligned to the Organisation's financial framework.

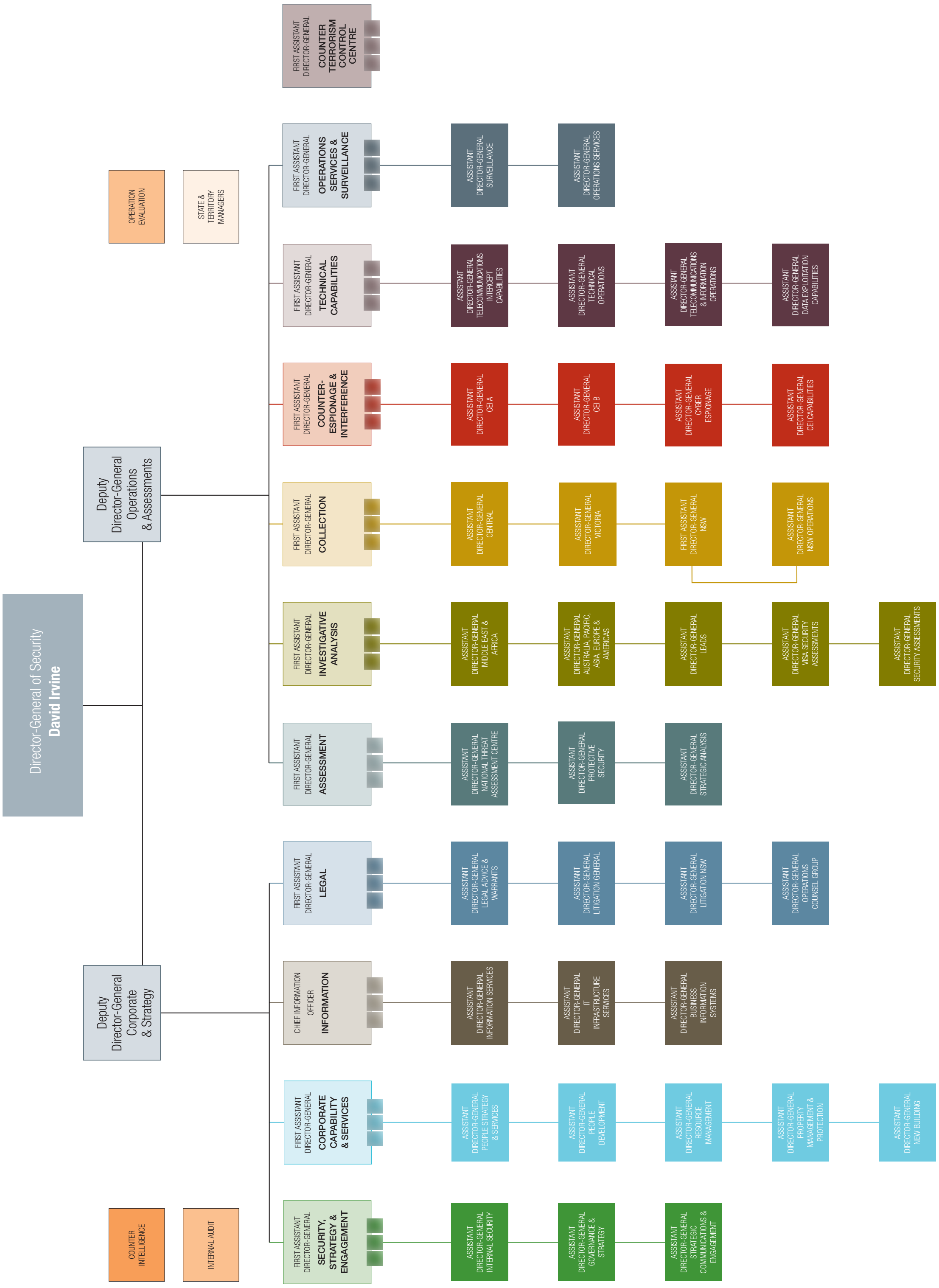
In addition to audits conducted by the ANAO and internal system controls, ASIO's internal auditor also undertakes a range of financial audits.

Structure of the Organisation

Organisational Structure

During the reporting period, ASIO's new ten division structure was implemented. This was designed to better allocate resources, aligning skills and work group functions to enhance organisational performance and interconnectivity across divisions. The ASIO Senior Management group continues to review ASIO's structure to ensure the most appropriate allocation of resources and matching of skills to duties, with a focus on ensuring ASIO's structure maintains sufficient fluidity to respond rapidly to any emerging thematic issues of security concern. The ASIO Structure, current as of 30 June 2011, is included at Figure 5.

Figure 4: ASIO organisational structure at 30 June 2011 [1]


Director-General of Security
David Irvine
Deputy Director-General Operations & Assessments
Deputy Director-General Corporate & Strategy
OPERATION EVALUATION
STATE & TERRITORY MANAGERS
COUNTER INTELLIGENCE
INTERNAL AUDIT
FIRST ASSISTANT DIRECTOR-GENERAL COUNTER TERRORISM CONTROL CENTRE
FIRST ASSISTANT DIRECTOR-GENERAL OPERATIONS SERVICES & SURVEILLANCE
ASSISTANT DIRECTOR-GENERAL SURVEILLANCE
ASSISTANT DIRECTOR-GENERAL OPERATIONS SERVICES
FIRST ASSISTANT DIRECTOR-GENERAL TECHNICAL CAPABILITIES
ASSISTANT DIRECTOR-GENERAL TELECOMMUNICATIONS INTERCEPT CAPABILITIES
ASSISTANT DIRECTOR-GENERAL TECHNICAL OPERATIONS
ASSISTANT DIRECTOR-GENERAL TELECOMMUNICATIONS & INFORMATION OPERATIONS
ASSISTANT DIRECTOR-GENERAL DATA EXPLOITATION CAPABILITIES
FIRST ASSISTANT DIRECTOR-GENERAL COUNTER-ESPIONAGE & INTERFERENCE
ASSISTANT DIRECTOR-GENERAL CEI A
ASSISTANT DIRECTOR-GENERAL CEI B
ASSISTANT DIRECTOR-GENERAL CYBER ESPIONAGE
ASSISTANT DIRECTOR-GENERAL CEI CAPABILITIES
FIRST ASSISTANT DIRECTOR-GENERAL COLLECTION
ASSISTANT DIRECTOR-GENERAL CENTRAL
ASSISTANT DIRECTOR-GENERAL VICTORIA
FIRST ASSISTANT DIRECTOR-GENERAL NSW
ASSISTANT DIRECTOR-GENERAL NSW OPERATIONS
FIRST ASSISTANT DIRECTOR-GENERAL INVESTIGATIVE ANALYSIS
ASSISTANT DIRECTOR-GENERAL MIDDLE EAST & AFRICA
ASSISTANT DIRECTOR-GENERAL AUSTRALIA, PACIFIC, ASIA, EUROPE & AMERICAS
ASSISTANT DIRECTOR-GENERAL LEADS
ASSISTANT DIRECTOR-GENERAL VISA SECURITY ASSESSMENTS
ASSISTANT DIRECTOR-GENERAL SECURITY ASSESSMENTS
FIRST ASSISTANT DIRECTOR-GENERAL ASSESSMENT
ASSISTANT DIRECTOR-GENERAL NATIONAL THREAT ASSESSMENT CENTRE
ASSISTANT DIRECTOR-GENERAL PROTECTIVE SECURITY
ASSISTANT DIRECTOR-GENERAL STRATEGIC ANALYSIS
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
CHIEF INFORMATION OFFICER INFORMATION
ASSISTANT DIRECTOR-GENERAL INFORMATION SERVICES
ASSISTANT DIRECTOR-GENERAL IT INFRASTRUCTURE SERVICES
ASSISTANT DIRECTOR-GENERAL BUSINESS INFORMATION SYSTEMS
FIRST ASSISTANT DIRECTOR-GENERAL CORPORATE CAPABILITY & SERVICES
ASSISTANT DIRECTOR-GENERAL PEOPLE STRATEGY & SERVICES
ASSISTANT DIRECTOR-GENERAL PEOPLE DEVELOPMENT
ASSISTANT DIRECTOR-GENERAL RESOURCE MANAGEMENT
ASSISTANT DIRECTOR-GENERAL PROPERTY MANAGEMENT & PROTECTION
ASSISTANT DIRECTOR-GENERAL NEW BUILDING
FIRST ASSISTANT DIRECTOR-GENERAL SECURITY, STRATEGY & ENGAGEMENT
ASSISTANT DIRECTOR-GENERAL INTERNAL SECURITY
ASSISTANT DIRECTOR-GENERAL GOVERNANCE & STRATEGY
ASSISTANT DIRECTOR-GENERAL STRATEGIC COMMUNICATIONS & ENGAGEMENT

[1] ASIO's structure was subsequently re-organised on 4 November 2011 to strengthen linkages between the operational/assessments and corporate and strategy areas of the Organisation. Technical Capabilities Division and Assessment Division now report to the Deputy Director-General, Corporate and Strategy, and Legal Division now reports to the Deputy Director-General, Operations and Assessments.

Corporate Direction and Strategic Planning

ASIO Strategic Planning

In December 2010, the ASIO Strategic Plan 2011–13 was launched. The plan embeds and builds upon the Organisation's strategic reform program, which commenced in 2009, to ensure ASIO is prepared to meet Australia's security intelligence challenges now and into the future.

The plan highlights ASIO's strategic direction and sets out four key strategic goals to achieve by 2013. These goals will guide ASIO to meet the expectations of government, domestic and international partners and the Australian public. The four goals are:

- strengthen intelligence collection and analysis capability;
- enhance strategic impact;
- build and manage the workforce of the future; and
- improve business processes and practices.

The plan guides business and project planning in ASIO, including performance and development agreements. It also provides a sound basis for the evaluation of Organisational performance both internally and through feedback sought from key stakeholders through the annual stakeholder satisfaction survey. A copy of the ASIO Strategic Plan 2011–13 is at Attachment 1.

During 2010–11, ASIO continued a range of change management programs designed to ensure ASIO remains well-positioned to respond to and proactively engage with threats to Australia's national security. Projects completed during 2010–11 included a change to the internal prioritisation of counter-terrorism investigations, a series of engagement initiatives with AIC partners, legislative reform to enhance interoperability and communication, the establishment of the Counter Terrorism Control Centre, implementation of the new Human Capital Framework and Strategic Workforce Plan, and the reform of the security assessment process for irregular maritime arrivals.

Management of Growth and Expansion

In 2010–11, ASIO continued to work towards its workforce growth program, as recommended by the Review of ASIO Resourcing, conducted by the late Mr Allan Taylor AM in 2005 (the Taylor Review). ASIO has also recently experienced significant growth in roles and functions, with the inclusion of border and territory sovereignty under the definition of security in the ASIO Act. These factors, coupled with the fast-pace investigative work required in the areas of counter-terrorism and counter-espionage, have placed a considerable demand on ASIO to effectively manage the growth of the Organisation and its duties.

ASIO's senior leadership has sought to manage this growth by focusing on developing the capabilities of ASIO staff, shaping an appropriate culture while actively managing change and engaging proactively with risks. The development of a modern, sophisticated senior committee structure, targeting recruitment to find the people with the right skills, characteristics and capabilities, and providing ongoing training and professional development for staff across all areas of ASIO will continue to assist the Organisation to manage growth experienced to date.

Corporate Governance

In 2009–10, ASIO commenced a comprehensive review and reform of its corporate governance framework, including key governance processes such as risk management, performance evaluation and enterprise resilience. In 2010–11, the focus of the review was ASIO's strategic and business planning and the corporate governance structure.

In the reporting period, ASIO introduced a uniform approach to business planning to ensure the optimal allocation of resources and to meet new challenges through continuous improvement, while addressing potential risks. Business plans closely align activity at divisional and branch levels with ASIO's strategic goals, as articulated in the ASIO Strategic Plan 2011–13, providing a sound basis for governance and performance evaluation. Business plans also provide staff with a shared understanding of the role, direction, work and priorities of the particular areas in which they work and are linked closely to staff performance measurement.

In 2011, ASIO launched a new project management framework, which establishes a single, consistent approach to initiating and running projects across ASIO. The framework ensures project and business planning processes are well integrated and underpins the annual investment program that determines which projects ASIO will undertake during the financial year, and the budget and staff resources which will be allocated to them.

ASIO is currently examining its corporate governance structure. A modified framework of high-level decision-making bodies and supporting corporate committees is expected to be introduced in early 2011–12. It is anticipated the improved corporate governance framework will further promote effective resource and risk management in ASIO and enhance accountability. The framework will ensure ASIO is preparing for the future by driving activity to meet agreed strategic objectives. The current structure of high-level committees is included at Figure 6 and a summary of the roles of the current committees is included at Table 2.

Table 1: Corporate Governance

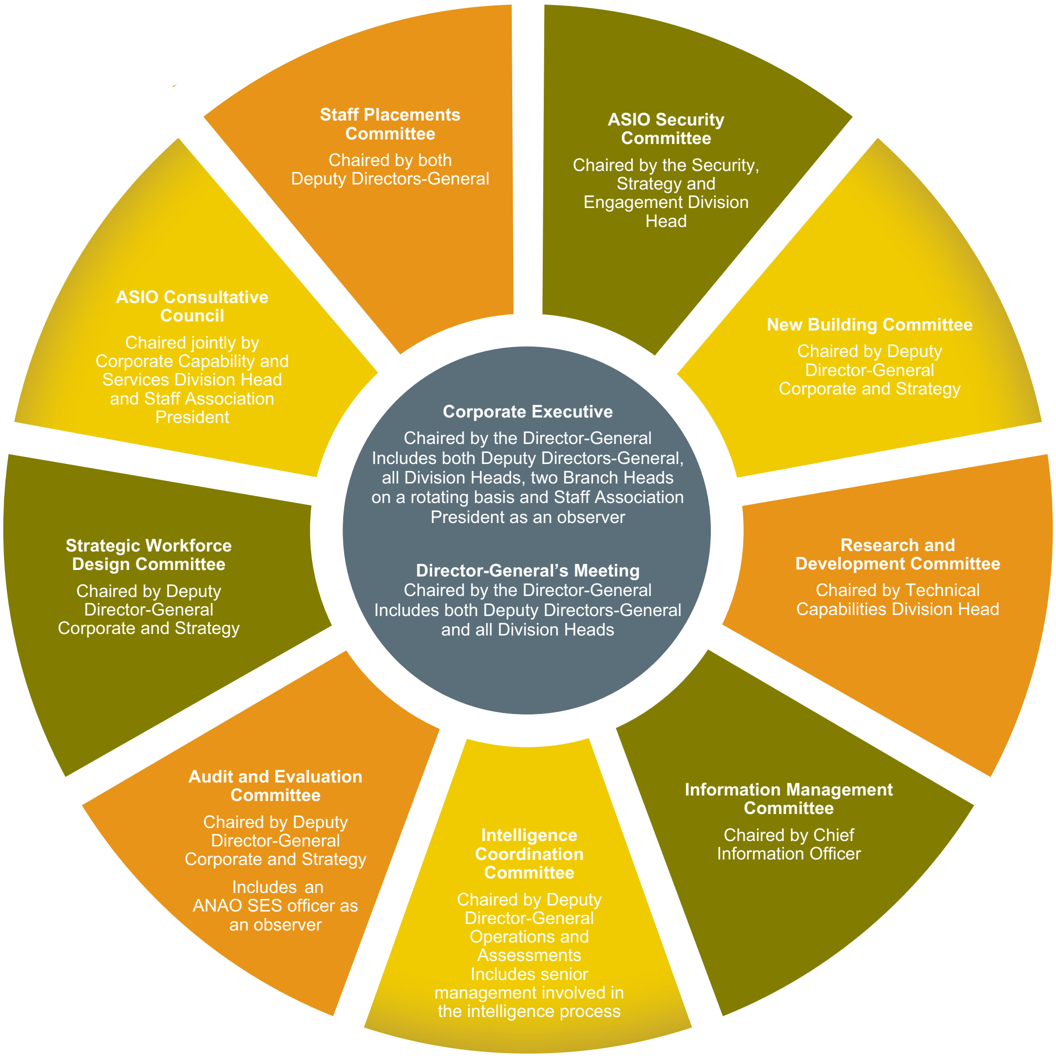
Director-General's Meeting	Comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. The DGM manages the day-to-day business of ASIO, including areas of ongoing corporate priority and urgent or emerging issues requiring consideration by the Executive.
Corporate Executive	Comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. A rotation of several Assistant Directors-General and the Staff Association President attend as observers. The Corporate Executive sets ASIO's strategic direction and oversees resource management, providing the main forum for managing strategic corporate priorities and resource issues. It also conducts detailed quarterly reviews of performance across ASIO. The Corporate Executive files are reviewed by the ANAO on an annual basis.

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

Table 2: Corporate Committee Structure

Intelligence Coordination Committee	Chaired by a Deputy Director-General, and includes senior managers involved in the intelligence process. The Committee establishes security intelligence investigative priorities and allocates investigative resources on a risk management basis. It also performs quarterly reviews against strategic objectives and approves arrangements for ensuring the legality and propriety of ASIO's intelligence collection, analysis and advice.
Audit and Evaluation Committee	Chaired by a Deputy Director-General, and includes two officers external to ASIO, including a senior executive officer from the Australian National Audit Office. The committee facilitates the internal audit of ASIO in accordance with the Internal Audit Charter, by setting priorities for audit, fraud control and evaluation planning. It considers the findings of the internal audits and evaluations, and ensures management-endorsed recommendations are implemented.
Staff Placements Committee	Comprises the two Deputy Directors-General and the Assistant Director-General of People Strategy and Services. The Staff Placements Committee manages the strategic placement of staff across ASIO, addressing existing and longer-term priorities and capability gaps.
Security Committee	Chaired by the head of Security, Strategy and Engagement Division and includes the Staff Association President. The committee reviews and addresses key issues relevant to the security of ASIO's people, property and Information Technology systems, and also drives development of security policies and practices.
Research and Development Committee	Chaired by the head of Technical Capabilities Division and includes ASIO's Science Adviser and a representative from the Defence Science and Technology Organisation. It provides strategic oversight and direction to technical collection and analysis capability.
Information Management Committee (suspended)	Chaired by the Chief Information Officer, the Information Management Committee provided strategic oversight and direction to ASIO's Information and Communication Technology (ICT) work program. In 2010, the Information Management Committee was suspended and the Intelligence Coordination Committee assumed responsibility for oversight of ICT projects delivering security intelligence enhancements. The continued requirement for an Information Management committee will be examined as part of the broader corporate governance review currently underway.
ASIO Consultative Council	Co-chaired by the head of the Corporate Capability and Services Division and the Staff Association President, and comprising representatives from management and the Staff Association. The committee is an advisory board which makes recommendations to the Director-General on human resource policies and practices. It facilitates management and staff discussion and resolution of issues of mutual interest and concern.
Strategic Workforce Design Committee	Chaired by a Deputy Director-General, this committee provides strategic focus on developing ASIO's workforce in alignment with the ASIO strategic plan. The four components of the ASIO Human Capital Framework (Strategic Workforce Planning, People Sourcing, People Policy and People Development) provide the supporting framework for committee deliberations.
New Building Committee (non-ongoing)	Provides strategic guidance on the new building project, including direction on significant design milestones, review of significant risk issues and oversight of project budget and program.

Figure 5: Corporate Committees Chart



Staff Placements Committee
Chaired by both Deputy Directors-General

ASIO Security Committee
Chaired by the Security, Strategy and Engagement Division Head

New Building Committee
Chaired by Deputy Director-General Corporate and Strategy

Research and Development Committee
Chaired by Technical Capabilities Division Head

Information Management Committee
Chaired by Chief Information Officer

Intelligence Coordination Committee
Chaired by Deputy Director-General Operations and Assessments
Includes senior management involved in the intelligence process

Audit and Evaluation Committee
Chaired by Deputy Director-General Corporate and Strategy
Includes an ANAO SES officer as an observer

Strategic Workforce Design Committee
Chaired by Deputy Director-General Corporate and Strategy

ASIO Consultative Council
Chaired jointly by Corporate Capability and Services Division Head and Staff Association President

Corporate Executive
Chaired by the Director-General
Includes both Deputy Directors-General, all Division Heads, two Branch Heads on a rotating basis and Staff Association President as an observer

Director-General's Meeting
Chaired by the Director-General
Includes both Deputy Directors-General and all Division Heads

Organisational Performance Management

ASIO's senior leadership group rigorously assesses its performance against specific benchmarks on a quarterly basis, utilising a 'traffic light' evaluation system. Underperformance against particular outputs or goals can impact on decisions and resourcing; operational or corporate priorities may need to be changed and specific strategies may need to be implemented to address the situation.

In 2010–11, ASIO mapped the relationship between strategic risks identified in the Strategic Risk Management Framework and performance reporting benchmarks to assess the extent to which performance reporting informs ASIO's management of strategic risks. The project has produced greater alignment between these two critical governance mechanisms.

Another important initiative during the period was the creation of an Organisational statistics library to collate, in a single coordinated space, statistical data reflecting ASIO performance and output over the last ten years. This will serve as a valuable platform for past and future trend analysis and inform ASIO's strategic planning.

Audit and Evaluation

In 2010–11, ASIO's internal audit team became an independent functional unit operating under the Office of the Director-General and Deputy Directors-General, reporting to the Chair of the Audit and Evaluation Committee (AEC). This structural adjustment reinforces the independence of the internal audit role. The AEC includes two external members, both senior executives from other agencies. The Australian National Audit Office Signing Officer also attends as an observer.

The AEC facilitates the internal auditing of ASIO in accordance with the Internal Audit Mandate, approves the annual audit work program and supports fraud control and evaluation planning. The effectiveness of the AEC was enhanced during the reporting period through the training of members by the Institute of Internal Auditors in governance, roles and procedures.

During the reporting period, compliance audit requirements were broadened to take into account changes to assumed identity legislation, and strict compliance requirements were incorporated into agreements for ASIO access to data belonging to other agencies. Seventeen internal audits were completed in the period, and three management-requested reviews were completed, along with the facilitation of an evaluation. The audit activity focused on improving performance beyond basic compliance to gain efficiencies in effective service delivery. Specific audits of ASIO assumed identities were conducted in January and July 2011 and found no discrepancies or instances of fraud.

An expanded internal audit capacity enabled broader performance audit activity covering a range of ASIO's administrative and operational practices. Performance audits conducted in 2010–11 included ASIO's processes for planning and approving capital projects and ASIO's stakeholder engagement, as well as audits leading to improved support mechanisms for operational activity. ASIO also seeks to undertake broader system evaluations to assist in the assessment of service delivery as well as the efficiency and effectiveness of the Organisation. Two major reviews were undertaken in 2010–11, relating to ASIO's engagement with another Commonwealth department and the integration of a risk management framework in organisational processes for priority setting in respect of counter-terrorism investigations and assessments.

Fraud Control

Following the release in March 2011 of the revised version of the Fraud Control Guidelines (2011) by the Attorney-General's Department, ASIO updated both the ASIO Fraud Risk Assessment and the ASIO Fraud Control Plan (2011–13). A new requirement of the 2011 Fraud Control Guidelines is the establishment of a fraud policy statement endorsed by the Director-General of Security. ASIO remains committed to minimising the incidence of fraud including through the mandatory requirement for all new staff and contractors to complete fraud and ethics training. Refresher ethics training is mandatory for all staff every three years. Ongoing training and familiarisation is provided via an e-learning module, which is available to all staff.

ASIO has a robust fraud control and detection strategy in place. Central to this is the commitment of all staff to report any suspected instances of fraud. During 2010–11, seven incidents of alleged fraud were reported within or against ASIO, with one found to be actual fraud, involving an external contact in private industry who misrepresented their association with the Organisation to derive improper personal benefits. All of these incidents have been dealt with in accordance with the ASIO Fraud Control Plan.

Human Resource Management

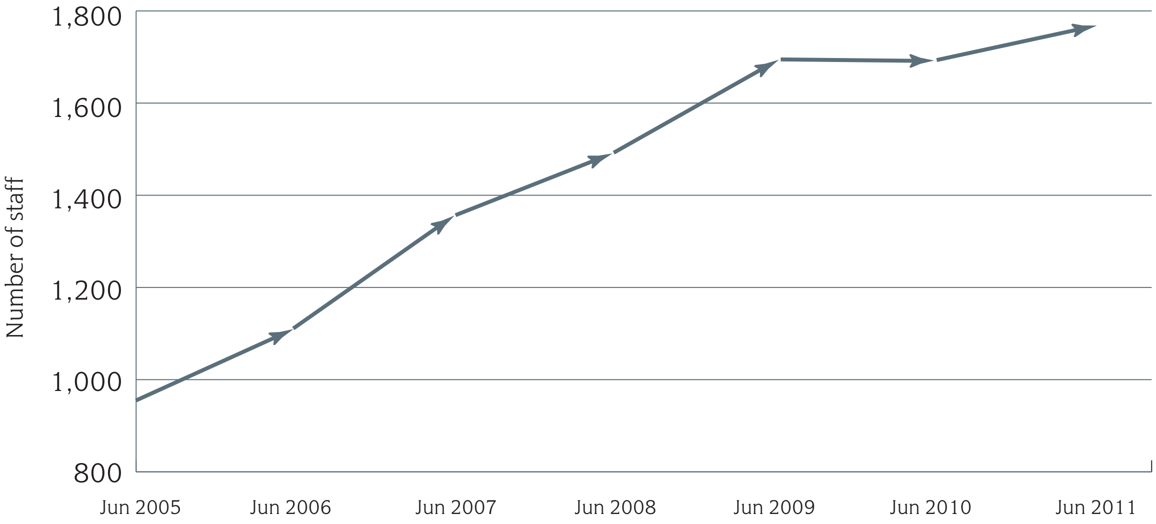
Recruitment

ASIO's recruitment activity in 2010–11 was focused on positioning the Organisation to fulfill the target of 1,860 full-time staff by the 2012–13 budget cycle, to meet the recommendation in the Review of ASIO Resourcing conducted by Mr Allan Taylor AM in 2005. Recruitment strategies and initiatives to attract new staff will remain a priority for ASIO to ensure the Organisation can meet the challenges of the current and future security environment.

As at 30 June 2011, ASIO employed 1,769 staff (representing 1,684 full-time equivalents), an increase of 78 during 2010–11. In 2010–11, ASIO appointed 196 employees, with 74 per cent engaged on an ongoing basis. ASIO remains committed to recruiting the people we need with skills in intelligence analysis and collection and technical specialist areas, while not compromising the stringent security vetting required of all ASIO employees.

In 2010–11, ASIO continued to utilise the internet to engage with prospective employees, placing recruitment advertisements across a range of online media, including social networking sites as well as traditional media. Prospective applicants were also attracted through the ASIO website, which was updated throughout the year with vacancies and information about positions available within the Organisation.

Figure 6: Staffing Growth, 2005–11



Training and Development

Intelligence Training

Throughout 2010–11, ASIO continued to invest heavily in Intelligence Training to meet capability development requirements. The revised Intelligence Development Program (IDP) ensures new intelligence officers are more capable and workplace ready at the completion of their initial training. Two IDPs were delivered in the year, with a total of 42 officers graduating from the programs into analytical or collection roles. In addition, many existing ASIO staff and officers from other agencies have accessed a range of ASIO intelligence training modules relevant to their work, developing their capabilities and diversifying the skill set of the ASIO, and Australian Intelligence Community, workforce. Advanced training courses were also provided to ensure intelligence officers have access to ongoing development to meet the requirements of a challenging and diverse security environment.

Corporate Training Programs

Corporate training programs are a specific mechanism used by ASIO to provide targeted development for officers in specific roles across the Organisation. This training ensures ASIO's staff members are appropriately skilled and underpins ASIO's Human Capital Framework. Corporate training activities include:

- an induction program for all new starters;
- wide-ranging administrative training, including training in – contract management, project management, staff selection skills, presentation skills, interviewing skills, strategic thinking, communication, finance and budgeting as well as trainer training;
- information technology training, including – basic and advanced training in the use of ASIO's computer systems;
- ethics and accountability training – all members of staff are required to attend at least once every three years; and
- discipline-specific courses covering subjects such as Islamic history and culture, and the political and social drivers of terrorism.

Management and Leadership Skills

ASIO officers have access to a range of leadership programs designed to build skills for ASIO, the national security community and the wider Australian Public Service, with programs designed to develop leaders with the resilience and dexterity to lead and manage in complex environments. In 2010–11, ASIO continued to implement 'Leading Edge', a program designed to engage all members of the leadership group with the organisational change required to deliver on ASIO's strategic imperatives.

ASIO's seminar series also continued throughout the reporting period. The series allows all ASIO officers to engage with presenters from government and academia on matters relevant to national security, providing different perspectives and contextualising ASIO's work with broader government priorities. During the reporting period, speakers to the series included representatives from the Department of Immigration and Citizenship, the Attorney-General's Department, the Department of the Prime Minister and Cabinet, the Lowy Institute, the Australian National University and ASIO's domestic and international partner agencies.

Language Training

In 2010–11, ASIO increased its foreign language capabilities and capacity to support the Organisation's counter-terrorism, counter-espionage and foreign interference investigations. Along with working with key domestic and international partners to strengthen resource sharing and benchmarking, ASIO streamlined procedures to process and disseminate foreign language product more efficiently.

ASIO also facilitated several short-term foreign language support activities with key domestic and foreign partners, including several secondments between ASIO and partner agencies. These short-term support activities filled critical language capability gaps and ensured agencies, including ASIO, were better placed to meet their foreign language requirements.

E-Learning

In the reporting period, ASIO continued to utilise e-learning, a computer-based training method which provides staff with increased access to various training packages to encourage professional development. ASIO developed and implemented 28 new e-learning modules during the year, with a focus on corporate and systems-based training.

Study Assistance

ASIO officers continue to have access to study assistance, which is designed to encourage continuing education and competency development relevant to ASIO's work. In 2010–11, ASIO provided assistance to 214 officers enrolled in external study programs across a range of disciplines, including international studies, law and education. ASIO also fully or partly funded the language development training of 17 officers during the reporting period. The Director-General's Study Bursaries also continued through 2010–11, supporting members of staff who achieve outstanding results in their studies while maintaining high levels of work performance.

Australian Intelligence Community Training

In 2010–11, ASIO provided ongoing support to a whole-of-government approach to intelligence training and partnerships, including providing presenters and participants for the AIC induction and senior officer development program and allocating places in ASIO development programs for participants from other agencies. Throughout the reporting period, ASIO also provided partnership forums – six for Executive Level 1 and 2 officers and three for Senior Executive Service officers – from a range of departments and agencies to increase awareness of ASIO's work and processes and provide an increased awareness of the roles and functions of the Organisation.

ASIO remains well integrated in the national counter-terrorism exercise programs conducted under the auspices of the National Counter Terrorism Committee, and continues to support the programs of the National Security College, including through providing presenters and students. ASIO is committed to ongoing capability development with AIC, law enforcement and other partners through joint training, exercises, secondments and attachments both to and from ASIO.

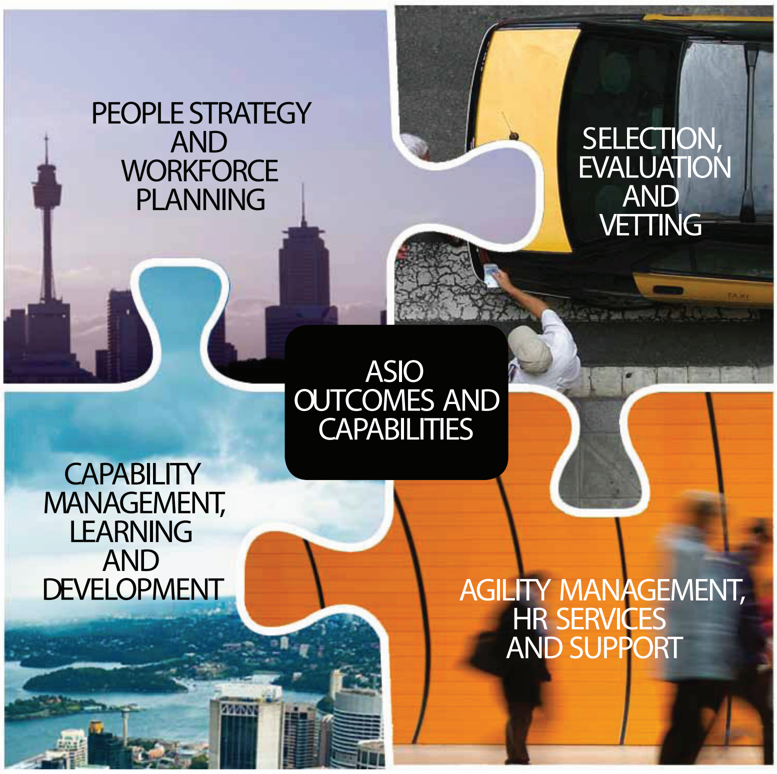
Performance Management

ASIO employs a highly competent and committed workforce and recognises the importance of harnessing its talent and continuing to foster and develop the capability of its people. Following the introduction of ASIO's Human Capital Framework, ASIO undertook to redesign its performance management framework. Enhancing Performance is a modern approach to managing, building and delivering capability within ASIO's workforce, while interconnecting with ASIO's mission and objectives to provide opportunities to improve employee engagement across the Organisation.

The Enhancing Performance framework and associated activities are supported by a range of interactive processes and tools. These aim to cultivate leadership skills and practices, assist managers to focus on managing for performance, support effective performance conversations and plan for individual and professional growth. This newly designed framework was implemented within ASIO in July 2011.

In October 2010, ASIO launched the new People Capability Framework, which allows ASIO to more accurately describe the capabilities and behaviours required of its workforce to deliver broader and more complex outcomes to the Australian Government. The People Capability Framework is based on the Australian Public Service Integrated Leadership System. Future focused, the framework supports ASIO's strategic intent, reflects ASIO's unique role and frames the workforce required to achieve excellence.

Figure 7: ASIO's People Capability Framework


PEOPLE STRATEGY AND WORKFORCE PLANNING
SELECTION, EVALUATION AND VETTING
ASIO OUTCOMES AND CAPABILITIES
CAPABILITY MANAGEMENT, LEARNING AND DEVELOPMENT
AGILITY MANAGEMENT, HR SERVICES AND SUPPORT

Attachments

ASIO values and encourages staff exchanges with its 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, enhancing national security outcomes. The number of Senior Executive Service (SES) level staff seconded from ASIO to other agencies/departments and vice versa has increased, demonstrating ASIO's ongoing commitment to the development of its leadership team and enhanced integration and collaboration with other government departments. During the reporting period, ASIO continued to build on its outreach and engagement strategy with regard to secondments to other Australian Government agencies and departments. During 2010–11, there were attachments to and/or from the:

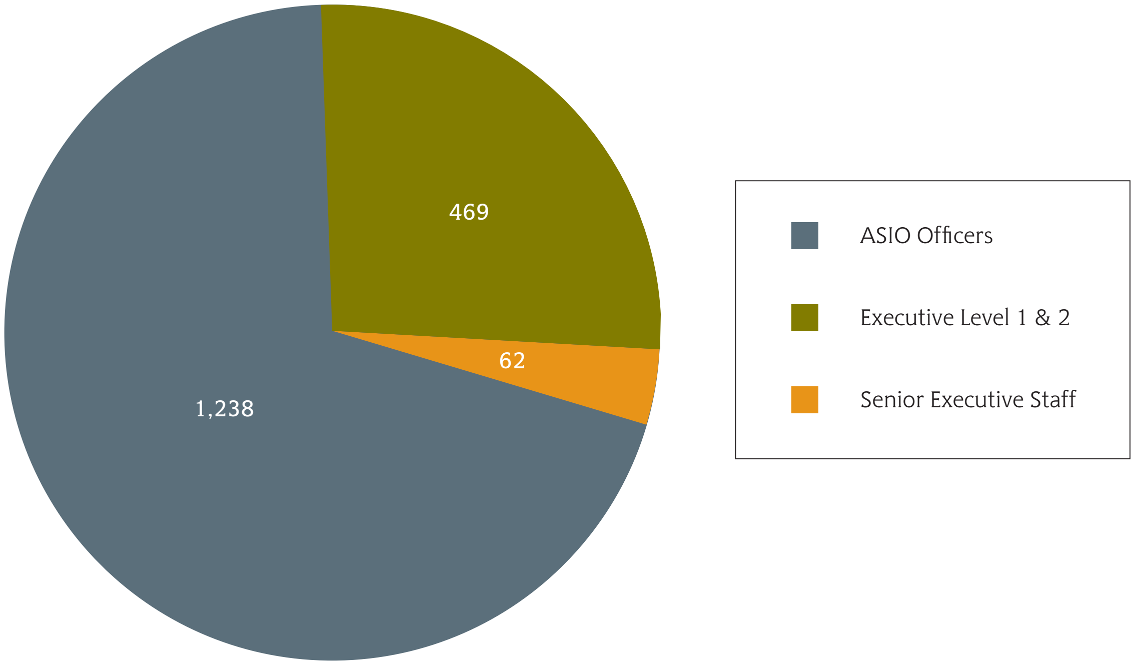
- Attorney-General's Department;
- Australian Customs and Border Protection Service;
- Australian Federal Police;
- Australian Government Solicitor;
- Australian Secret Intelligence Service;
- Department of Immigration and Citizenship:
- Defence Imagery and Geospatial Organisation;
- Defence Intelligence Organisation;
- Defence Security Authority;
- Defence Signals Directorate;
- Department of Defence;
- Department of Foreign Affairs and Trade;
- Office of National Assessments;
- Office of Transport Security within the Department of Infrastructure and Transport;
- Department of the Prime Minister and Cabinet;
- New South Wales Police; and
- Western Australian Police.

Staffing Ratios

Ratio of Senior Executive to Middle and Lower Level Staff

At 30 June 2011, there were 62 Senior Executive Service (SES) officers, 469 Executive Level 1 and 2 officers, and 1,238 other officers. These ratios are represented below in Figure 9.

Figure 8: Staff by Classification Group



Workplace Diversity

ASIO recognises and values equity and diversity and employs people from diverse backgrounds. During 2010–11, ASIO implemented recruitment and people management strategies designed to create an inclusive working environment that recognises and utilises the diversity in the workforce, seeking to recruit a range of people that reflect the Australian community. The diversity of ASIO's staff is reflected in Table 3 below.

Table 3: Diversity of Staff in ASIO[1]

Group	Total Staff	Women	Non-English Speaking Background	Aboriginal and Torres Strait Islander	People with a disability	Available EEO Data[2]
Senior Executive Service (excl DG)	62	12	0	0	1	60
Senior Officers[3]	469	170	17	0	7	436
AO5[4]	598	308	48	2	5	517
AO1 - 4[5]	539	279	25	3	5	521
Information Technology Officers Grades 1 and 2	92	14	8	0	1	88
Engineers Grades 1 and 2	9	0	0	0	0	8
Total	**1,769**	**783**	**98**	**5**	**19**	**1,630**

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

[2] Provision of EEO data is voluntary.

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

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

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

Additional information on the diversity of ASIO is included in Figure 9, which depicts the age distribution of ASIO staff; Figure 10, which depicts the length of service of ASIO staff; and Figure 11, which depicts gender representation across the various ranks of ASIO staff.

Figure 9: Age of Staff

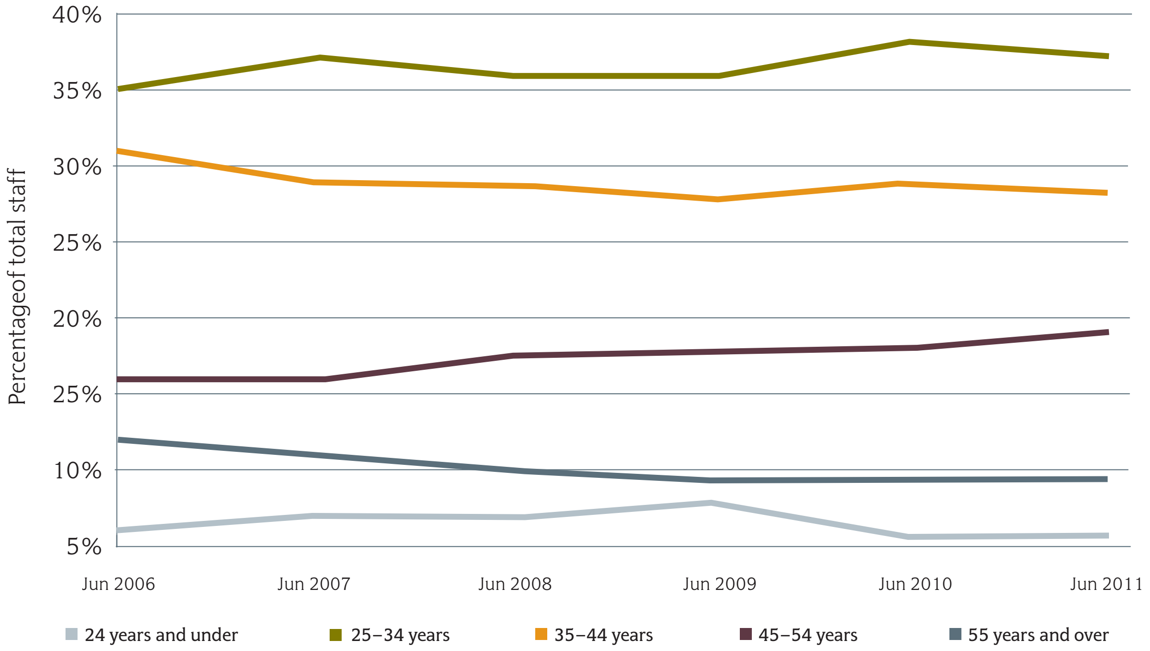


Figure 10: Length of Service of ASIO Staff

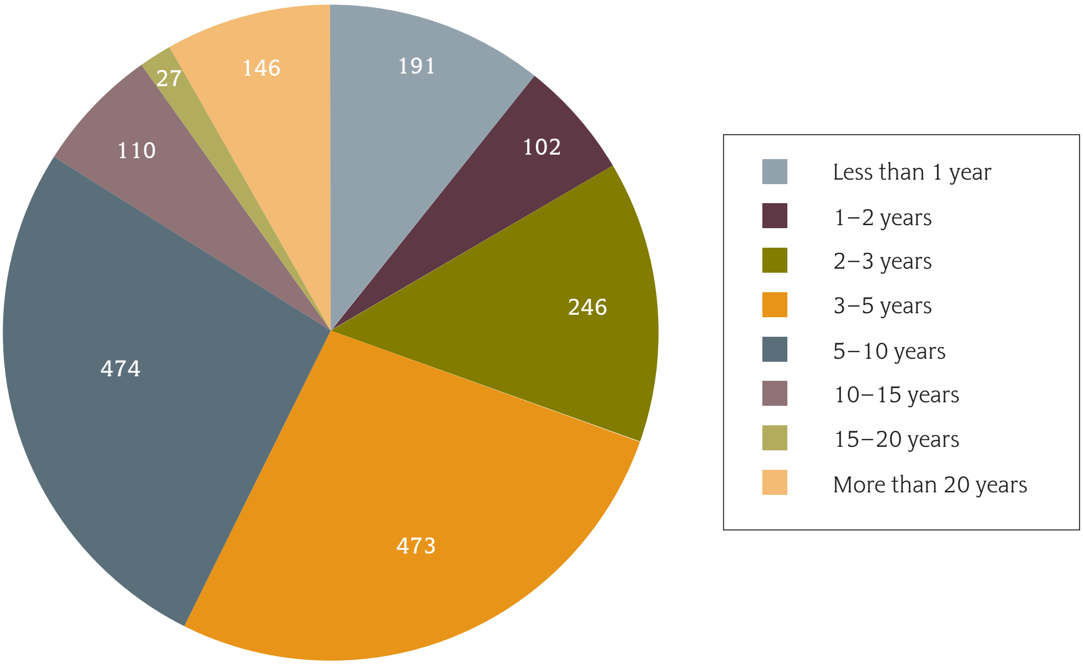
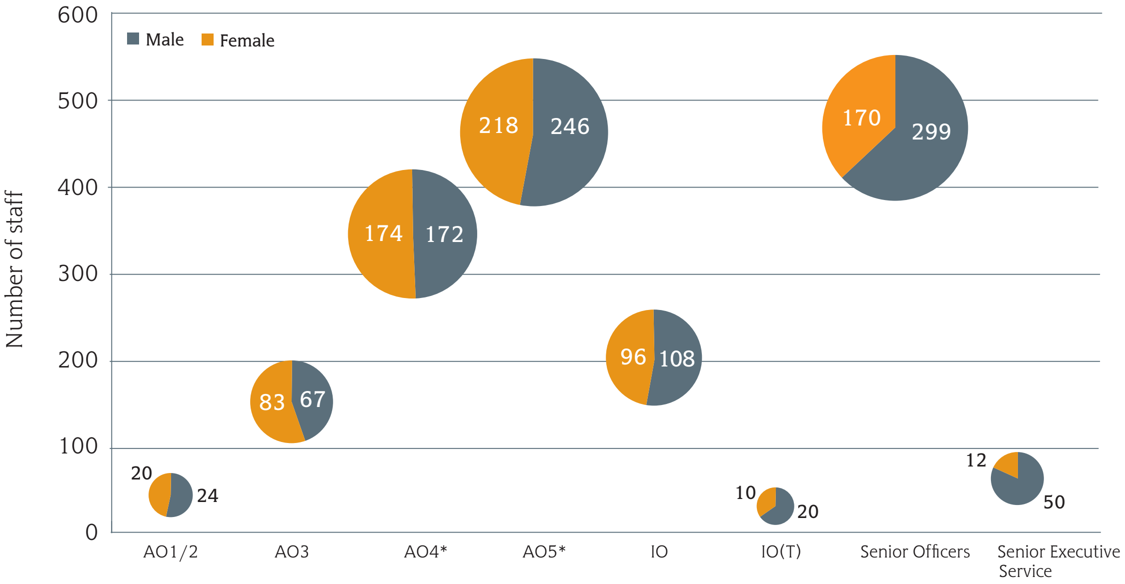


Figure 11: Gender Balance by Classification



* Includes equivalent staff in the Engineering and Information Technology Classifications

Staff Complaints

In February 2011, the Director-General launched ASIO's new anti-bullying and anti-harassment campaign, 'Silence Hurts'. The campaign aligns with ASIO's values and Code of Conduct and is designed to reinforce the need for a workplace culture free of inappropriate behaviour or where, if there is such behaviour, it is actively addressed. The Organisation-wide campaign included the launch of a bullying and harassment hotline, which provides information to staff members and managers on what to do if they experience or witness inappropriate behaviour, and provide support to those who have experienced bullying or harassment.

Twenty six requests for support or information were raised in the reporting period. The matters ranged from equity and diversity concerns to experiencing or witnessing inappropriate behaviour in the workplace. The increase in reporting in 2010–11, compared with eight cases reported in 2009–10, demonstrates the success of the 'Silence Hurts' campaign in promoting greater awareness and improving communication channels.

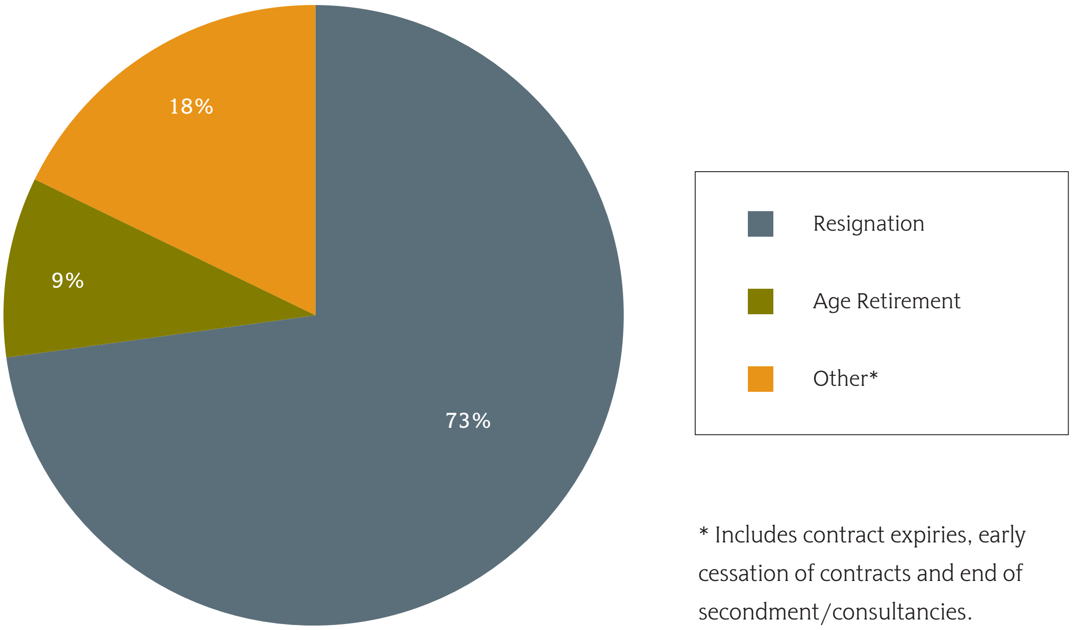
Since 2010, ASIO has employed an external ombudsman to assist in resolving issues raised by staff. As one of ASIO's review mechanisms, the ombudsman ensures concerns are considered impartially, informally and expediently, and the independent nature of the post provides an additional assurance of transparency and objectivity to the process. The ombudsman reports on a biannual basis on the general nature of his activities to ASIO's Corporate Executive and more explicitly to the Director-General as particular cases require.

In 2010–11, the ombudsman dealt with a range of matters including informal staff complaints, advice and support on workplace issues, and guidance on employment conditions. Additionally, the Director-General of Security also requested that the ombudsman undertake three formal investigations into workplace behaviour and interactions. The ombudsman reported that no issues suggesting systemic personnel problems within the Organisation were encountered.

Separation Rates

ASIO experienced a slight increase in the separation rate from 5 per cent in 2009–10 to 5.8 per cent in 2010–11, with this level still comparing favourably to the APS average separation rate of 7 per cent.

Figure 12: Separations by Percentage of Total Staff and Reason



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

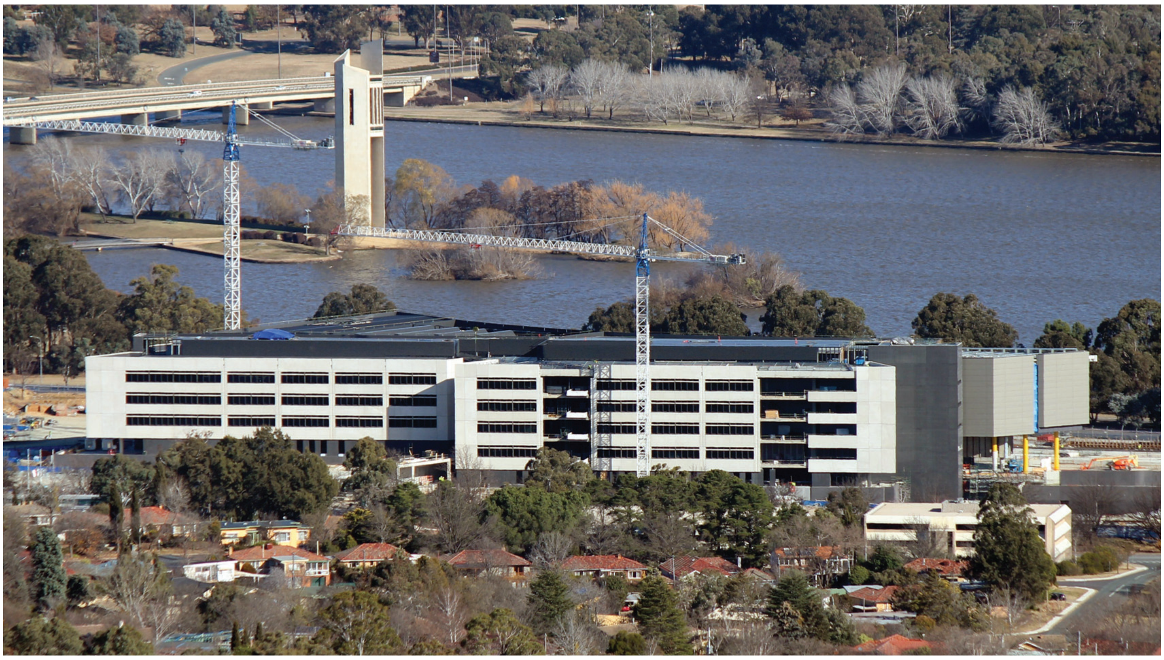
Accommodation

New Central Office, Canberra

During 2010–11, construction of ASIO's new Central Office continued. The pace of construction on the project has continued to increase, with over 800 contractors employed on site as at time of writing. At the close of the reporting period, construction was progressing to allow the building to be handed over to ASIO in mid-2012, with the main relocation of ASIO staff to commence from late 2012.

Close financial management against the project schedule by ASIO and the Department of Finance and Deregulation (through a jointly chaired steering committee) has ensured that cost and schedule pressures on the project are being managed in a way that there will be no requirement to seek additional funding from government for the project. 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.

Figure 13: ASIO's New Central Office



Legislation and Litigation

Legislative Amendments

ASIO works collaboratively with other Commonwealth departments and agencies to help ensure that Australia's legislative framework continues to support ASIO's capabilities and performance of its functions. This has included helping facilitate the Independent National Security Legislation Monitor's reviews of the effectiveness of, and appropriate safeguards relating to, Australia's counter-terrorism and national security legislation. During 2010–11, ASIO contributed to several proposed legislative amendments and policy developments, details of which are provided below.

Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011

Commencing in March 2011, these amendments enhance cooperation, assistance and information sharing between Australia's security, intelligence and law enforcement agencies in support of key national security priorities. For ASIO, the legislation provides greater flexibility to share intelligence and information with the national security community, within strict guidelines. The legislation also enables cooperation with law enforcement agencies in relation to telecommunications interception and other areas in which ASIO has expertise, including technical support, logistics and analytical advice.

Intelligence Services Legislation Amendment Bill 2011

Introduced into Parliament in March 2011, this Bill was passed on 4 July 2011. The legislation will enhance interoperability within the AIC and includes measures to:

- align the definition of 'foreign intelligence' in the *Australian Security Intelligence Organisation Act 1979* with the concept of foreign intelligence contained in the *Intelligence Services Act 2001* and the *Telecommunications (Interception and Access) Act 1979*;
- expressly confirm that computer access warrants under the ASIO Act authorise ongoing access over the life of the warrant; and
- exclude advice concerning AIC employment from the security assessment provisions of the ASIO Act.

Telecommunications Legislation Amendment (Cybercrime Convention) Bill 2011

This Bill was introduced into the House of Representatives on 22 June 2011 and remained under consideration by the Australian Parliament at the end of the reporting period. The Bill proposes a regime to allow interception agencies to request the preservation of telecommunications until a warrant can be sought to authorise the agency's access to the content of those communications.

ASIO will continue its support for a coordinated whole-of-government approach to further reforms to the ASIO Act and Intelligence Services Act to enhance operational capability, and of the telecommunications interception legislation regime to ensure effective ongoing telecommunications interception.

Litigation Matters

ASIO continues to contribute actively to prosecutions in national security cases, with ASIO officers and information often required in evidence or in responding to requests or subpoenas from the prosecution or defence. ASIO has also been involved directly in a number of civil matters arising from the discharge of its statutory functions and indirectly in other proceedings where ASIO information is relevant in cases involving third parties. ASIO takes seriously its obligations to the judicial process, while remaining aware of the need to bring to the attention of the courts and tribunals any issues which may imperil the effectiveness of future security efforts through the exposure of sensitive capabilities or information.

In the 2010–11 financial year, ASIO was involved in over 59 litigation matters, including criminal (particularly terrorism) prosecutions, judicial and administrative reviews of security assessments, and a range of civil actions. The diverse nature of these proceedings continues to produce a significant and increasing workload within ASIO.

The prosecution arising from a complex and lengthy joint counter-terrorism investigation involving the prosecution of five Melbourne men charged with conspiring to do an act in preparation or planning for a terrorist act, continued in Melbourne during 2010–11. On 23 December 2010, three men were found guilty in the Victorian Supreme Court of conspiring to undertake acts in preparation for a terrorist act – namely, planning an armed assault on Australian Defence Force personnel. Two group members were found not guilty and released. At the end of the reporting period, the three convicted men were awaiting sentencing by the court.[2]

During the reporting period, ASIO officers also gave evidence in other cases, including an attempted murder case in New South Wales.

Throughout 2010–11, ASIO was involved in challenges to a number of its security assessments. In December 2010, the Administrative Appeals Tribunal held that it did not have jurisdiction to hear applications for merits review of adverse security assessments for three irregular maritime arrivals (IMA). In a separate matter, in March 2011 the Federal Court dismissed two applicants' challenges to their adverse security assessments, noting there was insufficient evidence to support grounds for appeal.

In 2010–11, ASIO was involved directly in two legal matters initiated by Mr. Mamdouh Habib:

- Mr. Habib's compensation claim in the Federal Court of Australia alleging the Commonwealth defamed him and was complicit in his alleged mistreatment while he was detained overseas from 2001 to 2005 – the matter was settled on a confidential basis in December 2010; and
- Mr. Habib's application in the Administrative Appeals Tribunal to review an adverse security assessment and passport refusal decision.

[2] On 16 December 2011, Wissam Fattal, Saney Aweys and Nayef El Sayed were each sentenced to 18 years' imprisonment, with non-parole periods of 13 years and six months each.

Use of ASIO's Special Powers

Subject to a warrant approved by the Attorney-General, ASIO is empowered under the ASIO Act and the Telecommunications (Interception and Access) Act 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.

Role of Legal Officers

Given the increasing requirement for ASIO's involvement in legal and judicial matters, throughout 2010–11 ASIO continued to invest in its legal capability, ensuring management of legal issues across the Organisation and support to Commonwealth litigation. ASIO has legal teams based in Sydney and Melbourne and has integrated into its policies and procedures the lessons learned from prosecutions and other legal proceedings. The integration of legal officers into state offices has been a fundamental step towards more effective coordination and consideration of litigation and legal issues throughout the investigative process.

Visa, Personnel and Counter-Terrorism Security Assessments

ASIO's Role in Security Assessments

ASIO provides security assessment advice to appropriate areas of government concerning risks to security, including links to politically motivated violence, promotion of communal violence, espionage, foreign interference and border security. ASIO security assessments provide a mechanism for 'security' (as defined in section IV of the 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, the granting of visas and the 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.

ASIO security assessments are not an end in themselves. Consistent with ASIO's role as an intelligence agency, they are a means by which ASIO provides advice, covering factors related to 'security' as defined in the ASIO Act. 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 issued at the request of another Commonwealth agency, though ASIO does initiate reviews of security assessments as a consequence of ASIO intelligence investigations. Security assessments can include a simple check of personal details against ASIO's intelligence holdings or an in-depth intelligence investigation to determine, based on the nature and extent of the threat to security, the suitability of a person to have access to information, resources, materials or areas that are restricted on security grounds, or as it relates to a person's visa assessment. Each security assessment is handled on a case-by-case basis.

Upon making an assessment, ASIO may provide:

- a non-prejudicial assessment – ASIO has no adverse security advice to provide to the decision maker, not that ASIO has favourable advice regarding the suitability of the person;
- a qualified assessment – ASIO provides the decision maker with advice which they may take into consideration about the assessment subject but is not an adverse assessment in relation to the 'prescribed administrative action'; or
- an adverse assessment – ASIO provides the decision maker with advice which they may take into consideration about the assessment subject and 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 secure areas or to official or classified information. In all cases, ASIO itself is not permitted by the ASIO Act to take any administrative action in relation to the assessment subject.

In relation to security assessment for access to information, resources, materials or areas that are restricted on security grounds, all people subject to an adverse or qualified security assessment have the right to appeal to the Administrative Appeals Tribunal, regardless of their residence status. In regard to visa assessment matters, the subject only has a right to appeal 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 of an adverse security assessment.

Immigration-related policy and issues relating to the processing of irregular maritime arrivals, community detention and security assessments have been the focus of intense political, media and public interest in recent years. This has resulted in a number of recent reviews and inquiries involving significant contributions from ASIO, including an Inspector-General of Intelligence and Security inquiry into Community Detention Security Assessments, a Joint Select Committee review of Australia's Immigration Detention Network and also an Australian National Audit Office audit of ASIO's visa, personnel and counter-terrorism security assessment processes.

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 practicable for each one to be assessed by ASIO. A risk-managed referral framework has been developed with applications more likely to be of concern 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 may already be in Australia or who may be 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 34,396 visa security assessments in 2010–11. 45 adverse assessments were made in relation to visas, with 40 of these adverse assessments issued on counter-terrorism grounds, two on the grounds of involvement in people smuggling and three on the basis of counter-espionage or foreign interference.

In December 2010, the government directed that only irregular maritime arrivals (IMAs) found to be owed protection obligations, such as refugee status, would be referred to ASIO for a security assessment to determine any threat to security from the granting of permanent residence in Australia. As a result, in

January 2011, ASIO developed a referral framework which commenced operation in April 2011. This new framework has enabled ASIO to focus on complex IMA cases requiring intelligence investigation and to streamline the security process for non-complex cases in accordance with the risk to security they present.

Table 4: Visa Security Assessments 2010–11

Type of Entry	Number of Assessments Completed
Temporary Visas	16,223
Permanent Residence	11,724
Onshore Protection	957
Offshore Refugee/Humanitarian	1,906
Irregular Maritime Arrivals	3,586
Total	**34,396**

Delays in Visa Security Assessments

An ASIO security assessment forms part of the overall consideration by DIAC of whether to issue a permanent Australian visa. DIAC is responsible for determining the refugee status of all IMAs and assessments regarding an individual's identity and health prior to making a decision. At 30 June 2011, there were 5,738 IMAs in immigration detention, of which 456 had been found to be refugees and were awaiting security assessment. This represented 9 per cent of those in detention at that time. It is not a requirement under the ASIO Act that IMAs remain in detention during the security assessment process. The detention of IMAs is managed by DIAC, in accordance with Australian Government policy.

Passport Cancellations

Withholding passports is an important means of preventing Australians from travelling overseas to train, support or participate in terrorism. It may also be used to help prevent an Australian already overseas from participating (or further participating) in activities that are prejudicial to the security of Australia or another country. Under the Australian Passports Act, ASIO may request the cancellation of an existing Australian passport, as well as the refusal of an application for a new Australian passport, on security grounds. Under the Foreign Passports (Law Enforcement and Security) Act, an adverse ASIO security assessment can also be grounds for the Minister for Foreign Affairs to demand the surrender of a foreign travel document.

In the reporting period, ASIO issued adverse security assessments which resulted in the cancellation or denial of seven passports or passport applications. ASIO's adverse security assessments and the subsequent passport cancellations or denials by the Department of Foreign Affairs and Trade prevented the travel of several individuals who ASIO assesses were planning to travel overseas to engage in terrorism-related activities.

Personnel Security Assessments

Under changes to Australian Government policy in 2010–11, the new national security clearance levels are Baseline, Negative Vetting Level 1 (encompassing the previous levels of Confidential and Secret), Negative Vetting Level 2 (Top Secret Negative Vetting) and Top Secret Positive Vetting. The non-national security clearance levels of Protected and Highly Protected were abolished. ASIO personnel security assessments are mandatory for all persons requiring security clearances, except Baseline clearances. Agencies should refer Baseline clearances to ASIO where they identify a genuine link to security.

On 1 October 2010, the Australian Government Security Vetting Agency (AGSVA) was established. Since January 2011, all security access assessment referrals have come to ASIO electronically from AGSVA, except for a small percentage received by ASIO from AGSVA-exempt agencies. In 2010–11, ASIO completed 31,099 security access assessment referrals, which represents a 39 per cent increase in the number of security access assessment referrals completed by ASIO in 2009–10.

ASIO issued two qualified personnel security assessments in 2010–11. The majority of ASIO's security assessments are resolved based on material provided by the requesting agency. If there are issues of potential security concern, ASIO may conduct interviews or make other inquiries.

Table 5: Personnel Security Assessment 2010–11

Type of Assessment	Number
Top Secret Positive Vetting	3,100
Negative Vetting Level 2	7,512
Negative Vetting Level 1	20,487
Total	**31,099**

Counter-Terrorism Security Assessments

ASIO undertakes counter-terrorism security assessments to assist in granting:

- maritime security identification cards (MSIC);
- aviation security identification cards (ASIC);
- access to the Australian Nuclear Science and Technology Organisation (ANSTO) facility at Lucas Heights, Sydney;
- access to dangerous goods; and
- accreditation for individuals to work at special events, such as CHOGM.

ASIO conducts counter-terrorism security assessments to determine whether an individual has any known links of relevance to security. In 2010–11, ASIO completed 109,166 counter-terrorism security assessments, 97,922 of which were ASIC and MSIC assessments. This represents an 11 per cent increase from 2009–10. During the reporting period, ASIO issued two adverse counter-terrorism security assessments – one was for access to dangerous goods and the other was for an ASIC. This was the first time ASIO has issued adverse security assessments for these purposes.

In 2011, ASIO undertook counter-terrorism security assessments for MSIC renewals for the first time and also provided security assessments for access to restricted areas in relation to CHOGM 2011.

Figure 14: Personnel Security Assessment Process

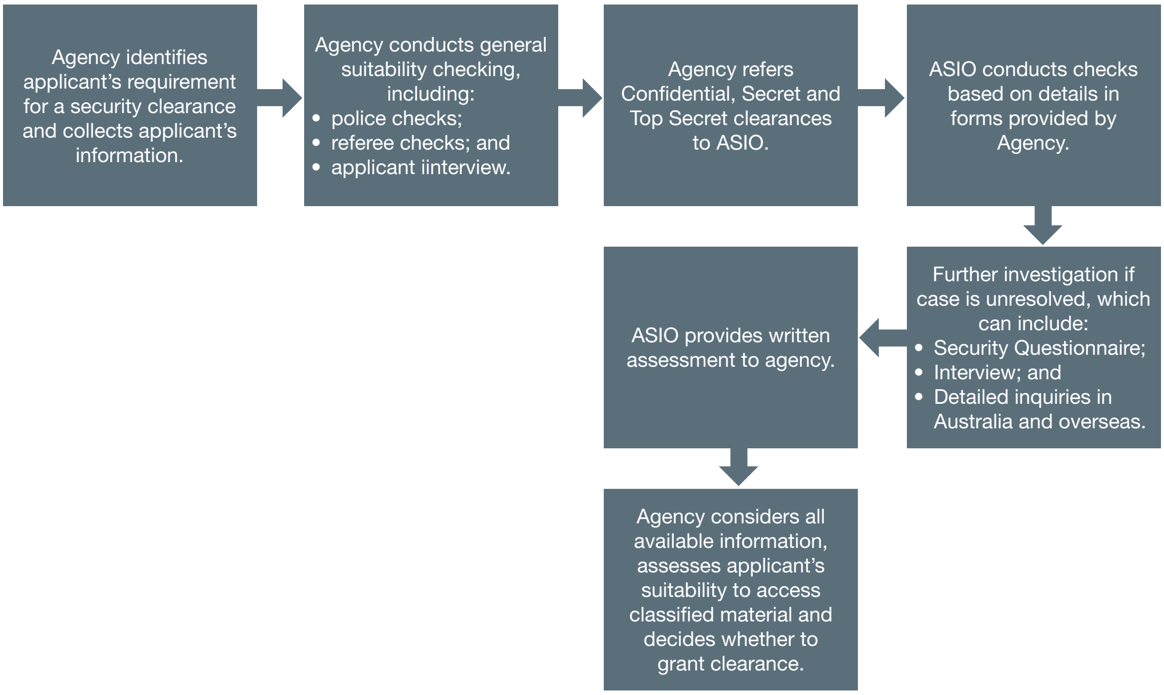
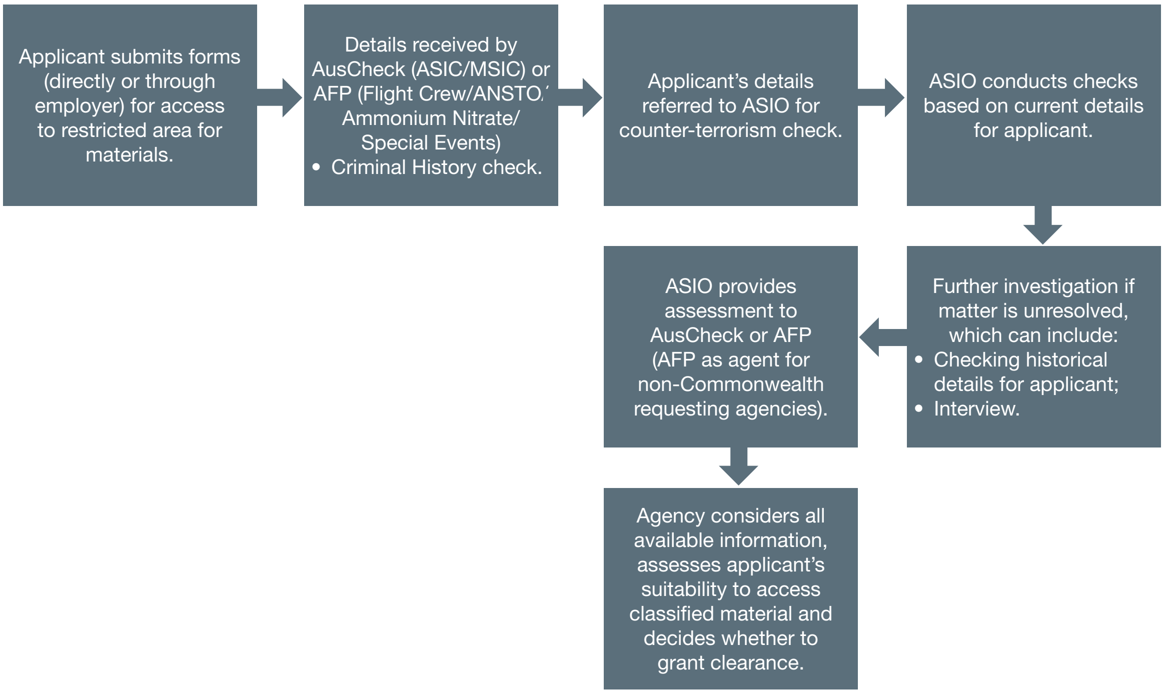

Agency identifies applicant's requirement for a security clearance and collects applicant's information.
Agency conducts general suitability checking, including: • police checks; • referee checks; and • applicant iinterview.
Agency refers Confidential, Secret and Top Secret clearances to ASIO.
ASIO conducts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

Figure 15: Counter-terrorism Security Assessment Process


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

Security of ASIO

The protection of ASIO information and advice, and knowledge of ASIO staff, sources, subjects of investigation, operations and methods, is integral to the ongoing effectiveness of the Organisation. The Australian Government looks to ASIO to exemplify best security practice. Accordingly, the Organisation reviews and develops corporate security policies and procedures regularly and seeks to shape appropriate security practices and culture to protect staff, premises and information from compromise.

Vetting of ASIO Staff

Revalidation and Re-evaluation Program

ASIO staff are required under government policy to periodically undergo a revalidation and re-evaluation program (where clearances are reviewed) to ensure they remain suitable to access classified material. The program monitors changes in the circumstances of staff to identify any areas where they may benefit from professional counselling or support or where a formal investigation might be required. This is to prevent security vulnerabilities arising out of financial, personal or work-related problems that could lead to the compromise of ASIO information.

Security Breaches

ASIO has a comprehensive suite of internal security policies to guide and support staff to uphold the highest standards of security practice. ASIO's Security Plan 2009–12 and Security Breach Policy provide strategies to mitigate security risks and provides a framework for staff to ensure sound security is practised in daily business.

In the reporting period, ASIO conducted a series of internal security focus groups, which were successful in identifying key security policies, priorities and policy gaps across the Organisation. ASIO also embarked on a strategic program of security policy reform, informed by the outcomes of the focus groups. In particular, work commenced to update the ASIO Security Plan, which provides a strategic overview for the management of security within ASIO, sets out strategies for achieving and maintaining security best practices and articulates how ASIO manages security risks. ASIO's Security Instructions, which document the practices, requirements and culture that ASIO staff are expected to adopt and embody, were also revised throughout the reporting period. ASIO Security Policies meet or exceed the standards laid down in the Protective Security Policy Framework.

ASIO places considerable emphasis on staff security awareness and education. Security briefings are factored into a range of training courses, including a dedicated e-learning module accessible to staff at any time. Presentations are provided to new staff to make clear the reasons for enhanced personnel, physical and information security within ASIO and the standards of professional and ethical behaviour expected of ASIO officers. All staff must participate in a security awareness workshop every five years to ensure ongoing security attentiveness.

E-Security Arrangements and Enhancements

With the increased threat to national security posed by cyber-intrusions, ASIO is working closely with other government agencies to provide advice to both the government and the private sector to mitigate these threats. Working collaboratively with others, ASIO identifies developing cyber-threats to critical infrastructure and determines appropriate responses, providing support and advice to private and government-owned critical infrastructure. In 2010–11, ASIO provided briefings to a range of private sector companies, often in conjunction with the Cyber Security Operations Centre (CSOC) and/or the Computer Emergency Response Team (CERT) Australia, focusing on the role cyber-security plays within the broader security landscape.

During the reporting period, ASIO contributed to whole-of-government cyber-security policy and crisis coordination arrangements. ASIO is engaged with the Attorney-General's Department and other Commonwealth departments and agencies to develop policy that aims for a more secure and resilient cyber-environment for critical infrastructure and across the public and private sectors more broadly.

ASIO's information technology (IT) security program provides assurance that ASIO's information and communications systems are being used in an authorised, secure and appropriate manner, through auditing, investigation of IT security incidents and IT security policy and advice. In the reporting period, the protection of ASIO externally connected IT systems from attempted cyber attacks was a particular focus of security attention. The implementation of an information-shared model to protect the security of ASIO information as the Organisation moves to a single information environment was another important body of work undertaken during 2010–11.

Management of Relationships and Public Reporting

As a security intelligence organisation, much of ASIO's work is necessarily conducted in secret, which can lead to erroneous speculation and commentary about ASIO's activities. ASIO is dependent on the support and cooperation of its partners and the Australian community. Without this support, ASIO cannot protect the security and safety of Australians effectively. Reaching out to partners has been increasingly important for ASIO, and a multifaceted strategy of outreach and engagement to build mutual trust and confidence with partners and the public has become a critical part of ASIO's work.

ASIO's Domestic Relationships

Over 2010–11, ASIO domestic liaison relationships were enhanced to better support ASIO's roles and functions. This included an expanded secondment and attachment program and the introduction of more regular senior management meetings with key partner agencies.

In 2011, ASIO introduced a new model for seeking feedback from stakeholders on their satisfaction with ASIO's engagement and performance. The new approach involves independently administered interviews with high-office holders in those agencies with whom ASIO most closely engages. Feedback is sought on partners' levels of satisfaction with their engagement with ASIO, their views on ASIO's collaboration, stakeholder focus, capabilities and people, and their evaluation of the quality, timeliness and accessibility of ASIO information and advice. Stakeholders reported high levels of satisfaction with their engagement with ASIO, with feedback centring on ASIO's contributions to whole-of-government outcomes, the sharing of capabilities, and collaboration. Partners considered their ASIO counterparts to be professional and capable interlocutors. Some issues of timeliness of advice in regard to ASIO security assessments were noted by some partners.

The survey also indicated collaboration with AIC partners has continued to improve over the reporting period, with most noting a desire for even greater integration and cooperation in the future. Federal, state and territory police services commended on the high quality of their partnerships and strong engagement with ASIO, with information sharing between ASIO and law enforcement partners seen as effective.

During the reporting period, ASIO continued its program of senior executive and senior officer partnership forums, a critical component of ASIO's broader outreach and engagement agenda. The forums provide participants with greater insights into the work and challenges facing the Organisation, while demonstrating the importance of interagency collaboration and cooperation in achieving security intelligence outcomes. The forums also provide a strong foundation for the increased sharing of perspectives, networking and the identification of areas for future partnership. In 2010–11, there was an increased focus on forums for senior officers as ASIO works to enhance relationships at that level. Participation was also extended to representatives of state and territory police forces and the offices of both premiers and chief ministers, demonstrating the ever-expanding range and nature of ASIO's partnerships.

During 2010–11, ASIO's Business Liaison Unit (BLU) provided intelligence-derived reporting to corporate security managers in private industry, enabling them to authoritatively brief executive management and staff for their risk management and continuity planning. ASIO actively built links with industry, business and research institutions and provided protective security advice in relation to the presence and activities of these businesses in Australia and overseas. ASIO also engaged in industry events, providing advice on corporate security, and the BLU coordinated five high-level meetings between company chief executive officers and the Director-General of Security. During the reporting period, ASIO expanded its industry engagement to include high-level briefings on espionage and cyber-issues to companies who have been, or are likely to be, victims of cyber-intrusions.

ASIO's International Relationships

ASIO's security mandate extends beyond the geographic boundaries of Australia. Security threats against Australians emanate from many different locations worldwide. The transnational nature of security threats and ASIO's global remit make engagement with, and support from, international partners essential to ASIO's work and effectiveness. International liaison relationships are a force multiplier for ASIO, enabling it to draw on the information, expertise and capability of overseas partners to pursue intelligence investigations that transcend national boundaries and make assessments of matters that affect the security of Australians and Australian interests.

In 2010–11, ASIO continued to expand its international liaison network. At 30 June 2011, the Attorney-General had authorised ASIO to liaise with 334 authorities in 123 countries. ASIO's program of engagement with these international partners covers the full range of its functions and activities, including:

- counter-terrorism;
- counter-espionage;
- cyber-threats;
- counter-proliferation;
- operational security and support issues;
- legal matters;
- training and corporate strategy; and
- technical exchanges.

ASIO engages with partners through liaison meetings, information and reporting exchanges, secondments or staff exchanges, and joint training and capabilities development initiatives, as well as through hosting or attending international visits and conferences. ASIO has a well-established and structured framework of accountability for its international engagement. As ASIO's investigations invariably touch on Australians, officers adhere to specific protocols regulating the exchange of information with overseas services. These include strict accountability and reporting measures, including regular auditing by the Inspector-General of Intelligence and Security.

The breadth and sensitivity of ASIO's functions also mean on-the-ground ASIO representation is an essential component of engagement in some countries, not just for ASIO but also more broadly for the AIC. The location of ASIO's overseas posts is reviewed regularly against changes to the global security environment and any shifts in budgetary position. ASIO coordinates its international engagement with other Australian intelligence agencies to ensure international relationships are pursued in accordance with broader government policy and to the maximum benefit of Australia's intelligence community as a whole while maximising resource use.

ASIO enjoys particularly strong and broad cooperation with key traditional North American, British, European and New Zealand partners and good relations with close allies in Asia and the Middle East. During the reporting period, ASIO also worked to enhance engagement with partners in parts of the world which are of increasing or emerging importance due to their links to security intelligence issues. ASIO's relationships with partners are not one way – partners seek ASIO support and assistance on matters affecting their own security.

One element of ASIO's international engagement is the Counter-Terrorism Intelligence Training Program (CTITP). The program, established in 2005, delivers training and capacity building to intelligence, security and law enforcement agencies in Asia, the Middle-East, Africa and the Pacific region. In 2010–11, CTITP delivered 87 training programs to more than 20 countries, involving more than 1,000 participants.

Public Reporting and Oversight

ASIO's Annual Report to Parliament 2010–11

ASIO produces a highly classified annual report which covers ASIO's operational and corporate activities 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 annual *Report to Parliament*, which provides a publicly available source of information on ASIO's activities throughout the reporting period, and is available on the ASIO website (www.asio.gov.au). ASIO is the only agency within the AIC that produces a publicly available report.

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

Public Statements

Throughout the reporting period, ASIO continued to engage publicly through speeches and appearances by the Director-General of Security. The Director-General spoke on numerous occasions throughout the year, including to community events, universities and research and private industry groups and at official government functions. The speeches covered a variety of topics, including the current security environment and cyber-security. These speeches are uploaded to the ASIO website to increase public awareness of these engagements by the Director-General.

The launch of the Counter Terrorism Control Centre (CTCC) was a significant media event for ASIO during the reporting period and involved the Prime Minister of Australia, the Attorney-General and the Director-General, along with a number of journalists accredited to the Parliament House Press Gallery. The launch, which occurred on 21 October 2010, received coverage across a wide range of print and broadcast media, reaching a potential audience of nearly two million people.

In 2010, ASIO relaunched its website to include a modern design interface and an emphasis on providing the Australian public with greater access to information about the Organisation, its people and its work. In 2011, in response to a query from the Law Council of Australia, ASIO completed a significant update of the Frequently Asked Questions (FAQ) section of the website as part of an ongoing effort to enhance communication channels with key stakeholders and members of the public. The FAQs are an important feature of the website and were revised to provide more detail across a broad range of areas, including ASIO's powers under legislation, ASIO's accountability framework, how ASIO officers interact with members of the community and information on matters of national security.

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 which collectively constitute the Australian Intelligence Community (AIC). The roles and functions of the IGIS are set out in sections 8, 9 and 9A of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act), providing the legal basis for the IGIS to conduct regular inspections of ASIO (and the other AIC agencies) and to conduct inquiries, of varying levels of formality, as the need arises.

ASIO works closely with the Office of the Inspector-General of Intelligence and Security to enable regular inspections of ASIO activities and to provide prompt responses with to IGIS inquiries. Throughout 2010–11, ASIO continued hosting monthly meetings with the IGIS to discuss issues arising from current inquiries as well as ongoing inspection activities. These regular meetings provide ASIO an opportunity to proactively brief the IGIS on emerging issues. ASIO senior officers provided numerous briefings and updates to IGIS during 2010–11 to discuss issues such as immigration-related security checking, the internal structure of ASIO, inter-agency cooperation, the revision of internal policies and procedures, the progress of legal actions in which ASIO has an interest, various inspection and inquiry tasks, and some specific operational matters.

In the reporting period, ASIO received more than 600 pieces of correspondence from the IGIS, and responded to about 98 per cent in less than 30 days. Forty one IGIS inspections took place during the 2010–11 period.

During 2010–11, IGIS initiated three new preliminary inquiries about the activities of ASIO, compared with the 12 preliminary inquiries initiated and/or concluded in the 2009-10 reporting period. One of these preliminary inquiries involved concerns about the processing of security assessments for an individual seeking a visa, while the other two revolved around the purported misconduct of ASIO officers in dealing with members of the public. All three of these inquiries have now concluded – an apology was issued by the Director-General of Security to the visa applicant for the delay in security assessment advice due to an administrative error, while the two cases of purported misconduct were not made out.

No full inquiries into ASIO were initiated by IGIS during the 2010–11 reporting period.

In December 2010, the Prime Minister requested that the IGIS conduct an inquiry into the actions of relevant Australian agencies in relation to the arrest and detention overseas of Mr. Mamdouh Habib from 2001 to 2005. ASIO provided considerable support and information to assist the IGIS in this inquiry.

In May 2011, at the request of the Prime Minister, the IGIS also commenced a full inquiry into allegations of inappropriate security vetting practices at the Defence Security Authority. ASIO will continue to provide information and assistance to the IGIS to support the inquiry, and work closely with the Defence Security Authority to identify any security issues.

During 2010–11, IGIS received 1,111 complaints from individuals who raised concerns about the timeliness with which ASIO processed immigration-related security checks; this compares to 1,015 such complaints received during 2009-10. The IGIS Annual Report 2010–11 notes "*While delay in the completion of security assessments has been a cause of genuine concern to me, I am satisfied that this has not been caused by error or improper processes by ASIO but has been largely a by-product of external factors over which it has limited control.*"

Parliamentary Oversight

Senate Standing Committee on Legal and Constitutional Affairs

ASIO attended two hearings of the Senate Standing Committee on Legal and Constitutional Affairs during 2010–11 (Supplementary Budget Estimates in October 2010 and Budget Estimates in May 2011). In both instances, the Director-General of Security was accompanied by ASIO's Deputy Director-General, Corporate and Strategy, Mr. David Fricker.

ASIO responded to questions on a range of issues, including:

- security assessments;
- ASIO's new central office;
- budget and staffing;
- cyber-espionage attacks on the Department of Parliamentary Services network;
- WikiLeaks;
- the Intelligence Services Legislation Bill 2011;
- the Inspector-General of Intelligence and Security's inquiry regarding Mr. Mamdouh Habib;
- Mr. Habib's Commonwealth compensation claim and settlement;
- counter-terrorism laws; and
- personnel security assessments and vetting procedures for Australian Government employees.

During the reporting period, ASIO also responded in writing to 29 questions on notice.

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* (Cwlth) 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.

This report constitutes ASIO's unclassified submission to the PJCIS on administration and expenditure covering the 2010–11 period. In addition to this written report, ASIO is due to appear in front of a PJCIS hearing to respond to questions on administration and expenditure. In 2010–11, ASIO provided the classified *Review of Administration and Expenditure (No. 9: 2009-10)* to the PJCIS, with an unclassified version of the review made available on the PJCIS website. In March 2011, ASIO appeared before the PJCIS to respond to questions on its administration and expenditure. In June 2011, ASIO appeared before the PJCIS in a public hearing to respond to questions on security assessments.