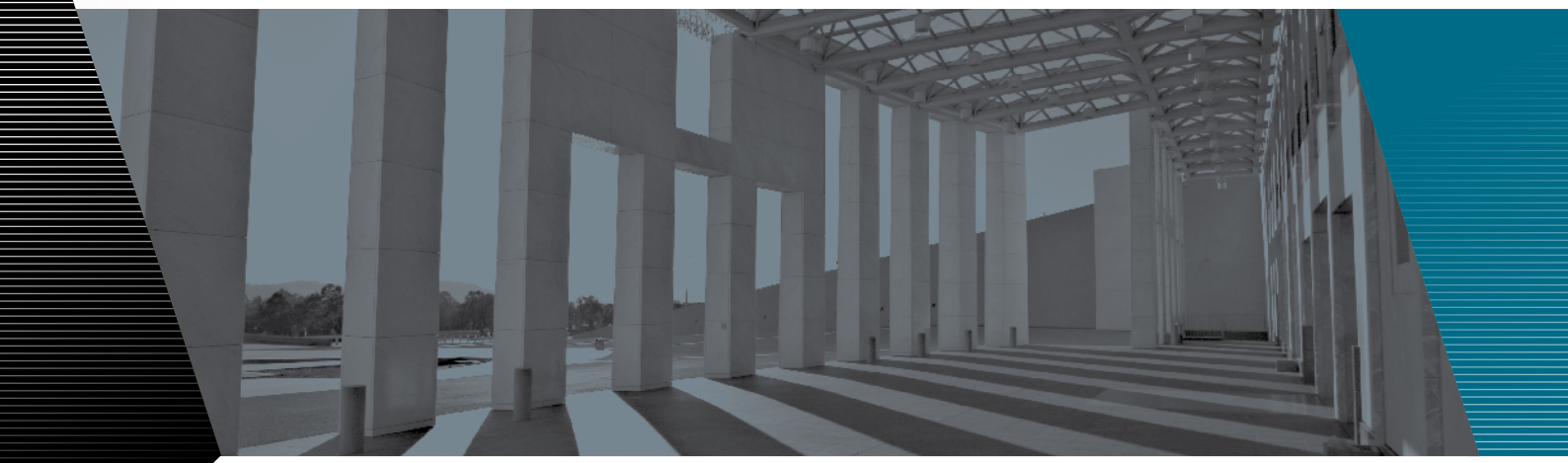
Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure



No.11 2011–2012

www.asio.gov.au

Contents

Figures

Tables

Scope of Review

The Australian Security Intelligence Organisation (ASIO) annual submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of Administration and Expenditure No. 11 provides a detailed account of ASIO's activities during the financial year.

For 2011–12, the PJCIS has requested a submission covering all aspects of administration, including:

- Any legislative changes that have had an impact on administration. The submission should cover the frequency and nature of use of these powers by an agency, 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 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 where applicable;
- 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, which 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 (PMV);
- the promotion of communal violence;
- attacks on Australia's defence system;
- acts of foreign interference; and
- serious threats to Australia's territorial and border integrity.

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 possible 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 issue and access to classified or controlled material and designated security-controlled areas.

Under the ASIO Act and other legislation, ASIO is authorised to use intrusive powers under warrant, including telecommunications interception, the entry and searching 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 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 the only agency in the Australian Intelligence Community (AIC) authorised to undertake security investigations into the activities of Australians, ASIO operates within a stringent oversight and accountability framework. The foundation of this framework is the ASIO Act, created to recognise the importance of individual rights, while safeguarding the public's collective right to be secure.

ASIO is subject to direction, with certain specific exceptions, from the Attorney-General and operates in accordance with guidelines issued by the Attorney-General.

ASIO is subject to strict accountability mechanisms, including, but not limited to:

- The tabling of an unclassified *Report to Parliament* and the provision of a highly classified Annual Report to members of the National Security Committee of Cabinet and a small number of senior Commonwealth officers;
- The review of ASIO's activities by the Inspector-General of Intelligence and Security, an independent statutory authority;
- Attendance at hearings of the Senate Standing Committee on Legal and Constitutional Affairs;
- The review of ASIO's administration and expenditure by the Parliamentary Joint Committee on Intelligence and Security via a classified submission and hearing; and, most recently;
- An additional mechanism, an Independent Reviewer, responsible for the review of ASIO adverse security assessments furnished in relation to eligible persons who remain in immigration detention.

Executive Overview

The security environment 2011–12 and outlook

Politically motivated violence

Australia's domestic security environment is dynamic, constantly changing in response to a range of factors— predominantly offshore influences. Australian interests overseas face a persistent threat in a number of international locations. The significant challenge to identify individuals and small groups inspired by, but not otherwise affiliated with, terrorist groups is an emerging security concern.

Espionage and foreign interference

ASIO continued substantial work to identify and investigate actual or attempted acts of espionage and foreign interference. ASIO's outreach to public and private sectors has helped to raise awareness of the espionage threat. This has also shaped both protective security and strategic policy responses and informed decision-making on public and private sector procurement of commercial platforms and engagement with foreign vendors.

Cyber-espionage remains a key concern. Ongoing work with the Defence Signals Directorate (DSD)-hosted Cyber Security Operations Centre (CSOC) facility was instrumental in identifying cyber threats and determining appropriate responses.

Harm is being done to Australian interests by espionage, including cyber-espionage. Determining the full extent of the harm remains complex and difficult.

ASIO's work across the spectrum of security issues enables a broad understanding of the security environment and the requirements for advice to government. Much of this advice and assessment is communicated through formal reports produced by ASIO.

Reporting	In 2011–12 ASIO produced 3 000 intelligence products, which were shared with over 350 partners in Australia and overseas. This included 593 threat assessments on topics such as the 2011 Commonwealth Heads of Government Meeting in Perth and visits by Her Majesty the Queen and the President of the United States of America.

Border integrity

In 2011–12 ASIO contributed to whole-of-government efforts to counter people smuggling, predominantly through the identification and investigation of onshore individuals facilitating international people-smuggling syndicates.

Expenditure

ASIO's budgetary situation will continue to place pressure on our ability to meet the expectations of Government and the Australian public. ASIO is continuing to examine options to manage the situation without a significant diminution of core operational work or capability.

Funding and expenditure	Revenue from Government in 2011–12 was $328.1 million, a decrease of $16.8 million from the 2010–11 financial year. In 2011–12, ASIO's operating result was a loss of $5.3 million against a Government approved operating loss of $6.2 million. This loss is a technical loss and is attributable to the accounting treatment required for employee provisions due to interest rate movements.

Structure of the Organisation

ASIO has continued to refine its structure in light of current and anticipated budgetary constraint. This, coupled with a more dynamic and challenging security environment, has necessitated innovative means to identify efficiencies.

Structure of the organisation	Since the conclusion of the reporting period, ASIO has implemented a revised structure. The new structure has shifted ASIO from 11 divisions to 8.

Corporate Direction and Strategic Planning

In 2011–12, ASIO business planning and investment activities continued to deliver against key programs. The reform and modernisation program has set the foundation for ASIO's move from a period of growth to a period of consolidation.

In January 2012 ASIO implemented a new, simplified and more accountable committee structure to support strategic resource and business planning, risk management and performance reporting.

Human Resource Management

The Taylor Review growth target of 1 860 has been deferred indefinitely. However, ASIO will continue to recruit new intelligence professionals and technical officers within budget allocations and increase the skill-set of existing officers to meet the increasingly diverse challenges of our security environment.

Revision of anticipated growth	In 2011–12 revisions to ASIO's budget resulted in an indefinite deferral of organisational growth. In February 2012 ASIO's approved staffing target was reduced from 1 860 to 1 760. However, in order to manage within its current budget, ASIO is maintaining a staffing level of 1 730.
Training	Two cycles of ASIO's Intelligence Development program took place over the reporting period, with 32 officers graduating to become Intelligence Professionals.

Accommodation

Delays in the construction of ASIO's new Central Office have led to the handover date slipping.

New Building budget	The project has experienced overruns to date of $41.6 million, which equates to seven per cent of the approved budget of $589.2 million set in 2008. ASIO's contribution to cost overruns is $24.3 million which is met within existing budgets.

Legislation and Litigation

Throughout 2011–12 further legislative amendments were developed to better meet the challenges posed by current and emerging technologies and modernise existing legislation.

In 2011–12, the trend of increased ASIO involvement in legal and judicial matters continued, with ASIO contributing actively to prosecutions in national security cases. ASIO remained involved in a number of civil matters arising from the discharge of statutory functions and indirectly in other proceedings where ASIO information was relevant.

Involvement in litigation	Over the reporting period ASIO was involved in 58 litigation matters including criminal prosecutions and judicial and administrative review of security assessments.

Security of ASIO

The secure and effective conduct of ASIO operations and investigations begins with strong personnel security supported by appropriate governance, policy and technological processes.

These elements, engaged in concert, serve to protect the information, people and business systems necessary to deliver on ASIO's mission—to protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government.

Management of relationships and public reporting

A particular focus during 2011–12 has been for ASIO to enhance awareness of the work of the organisation amongst the public, and across government and industry partners. This approach to domestic engagement has included an increase in the number of public addresses by the Director-General, regular senior officer partnership forums with state and federal government and the provision of security reporting to industry via the Business Liaison Unit (BLU).

Over the reporting period ASIO's international relationships with key partners were further strengthened with the preparation and conduct of secure large scale events such as the London Olympic and Paralympic Games.

Foreign Liaison	At the end of the reporting period the Attorney-General had authorised ASIO to liaise with 340 authorities in 125 countries.

The Security Environment 2011–12 and Outlook

Terrorism

The challenge of terrorism is real and persistent, with the greatest threat continuing to be terrorism motivated by a violent jihadist ideology. The security threats facing Australia are constantly evolving in response to a range of drivers, which mostly occur in, or originate from, other countries.

The Syrian conflict continues to present a range of interconnected and enduring security challenges and will fuel a now mature extremist landscape. There is a growing number of Australians expressing an intention to travel to Syria, Turkey and/or Lebanon to participate in the conflict.

Australian interests overseas face a persistent threat in a number of regions across the globe, although the decreased relevance of group membership across the board, such as to al-Qa'ida, represents an increasing intelligence collection challenge to identify individuals and small groups inspired by the ideology.

External sources of radicalisation continue to be of concern. Over the reporting period, al-Qa'ida in the Arabian Peninsula (AQAP) released four new issues of *Inspire* magazine via the internet. Australia has previously been mentioned in *Inspire* as a legitimate terrorist target.

Communal violence and violent protests

The ongoing violence in Syria has provoked and will continue to provoke a broad response from the Australian community and has created tensions between pro and anti-Syrian Government supporters.

Although outside the reporting period, it is worth noting the protests which occurred in Sydney on 15 September 2012 against the film *Innocence of Muslims*. These protests represent one of the most public examples of individuals willing to use violence in defence of Islam seen in Australia, and the first time we have seen it as a protest tactic. However, condemnation from local Islamic community leaders, the police response, and public outcry have combined to diminish the likelihood of similar violence at protests in the absence of significant provocation, at least in the short term.

The term issue-motivated groups (IMGs) covers a diverse range of legitimate protest and advocacy activities from environmental, anti-capitalism and animal rights through to indigenous affairs, industrial relations, rights for disabled people and local community issues.

The nature of IMG protests is generally not of security significance except where the protest methods attempt to influence political discourse through the use or threat of violence. Traditionally within Australia, most violent protest activity by IMGs has been undertaken by extremist left-wing groups, especially those linked to the anarchist movement. These groups and individuals are on the fringes of political activity and have a history of using violence against the state to promote their political ideology and objectives.

Australian nationalist extremist or racist extremist (NERE) groups continue to operate within Australia. Australian NERE groups supporting the use of violence against ethnic or religious groups are of interest to ASIO. At the same time, ASIO must remain alert to the possibility of a right-wing racist acting alone—as happened in Norway in July 2011. The majority of NERE groups do not advocate the use of violence to achieve their objectives, which are primarily limited to the establishment of whites-only communities removed from other ethnic groups and/or the promotion of white supremacy through race-hate music.

Other major issues which continue to resonate with the potential for protest activity are the environment, immigration and anti-globalisation. These have a general appeal and an existing support base, but protest activities remain largely non-violent. In most cases, violence is perpetrated by splinter groups dissatisfied with peaceful protest. Social networking sites provide opportunities for overseas leaders to generate influence and action here and for locally-based individuals to seek guidance or inspiration from abroad.

Espionage and Foreign Interference

In 2011–12 ASIO continued substantial work to identify and investigate actual or attempted acts of espionage and foreign interference. ASIO has reinvigorated its outreach to public and private sectors to raise awareness of the espionage threat. ASIO reporting on this activity has also helped shape both protective security and strategic policy responses and informed decision-making on public and private sector procurement of commercial platforms and engagement with foreign vendors.

Cyber-espionage remains a key concern. Ongoing work with the DSD-hosted CSOC facility was instrumental in identifying cyber threats and determining appropriate responses.

Harm is being done to Australian interests by cyber-espionage, although determining the full extent of harm done remains complex and difficult. ASIO's investigations, coupled with an expanding program of private and public sector outreach to raise awareness of the security threats, are yielding examples of the cost to Australian entities from cyber-espionage.

Proliferation

In 2011–12 ASIO worked in concert with other Australian government agencies to prevent and disrupt attempts to exploit Australian materials, technology and knowledge for the development of weapons of mass destruction (WMD).

This activity included:

- cooperation with the Department of Foreign Affairs and Trade and the Defence Intelligence Organisation to deny individuals of concern access to Australia through vigilant visa screening and visa denials under Public Interest Criterion 4003(b); and
- provision of advice to the Minister for Foreign Affairs and Trade and the Minister for Defence in support of export and sanctions issues.

Border security

In 2011–12 ASIO contributed to whole-of-government effort to counter people smuggling, predominantly through the identification and investigation of Australians involved in maritime people-smuggling.

Outlook for the Security Environment

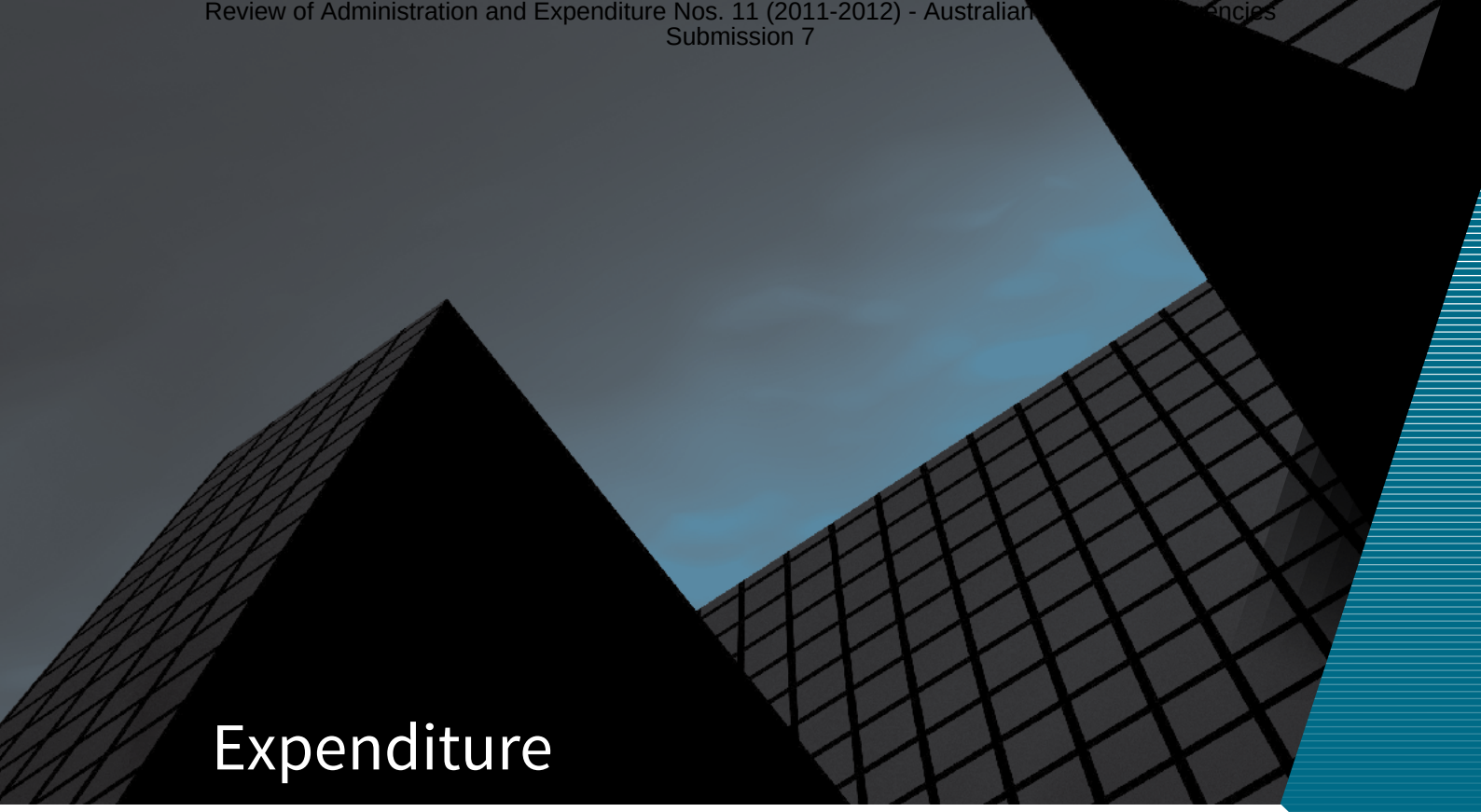
We are likely to see the emergence of new domestic extremists in 2013, either individually or in small groups. Many will likely be technologically savvy and security conscious, the latter facilitated by individuals learning the methods of authorities through ongoing court proceedings. This will make the detection and prevention of terrorist attack planning increasingly difficult.

Countries in North Africa caught up in the Arab Spring (Libya, Egypt and Tunisia) are emerging as new arenas for terrorist training, facilitation and attack planning; we expect to see Australians interested in travelling overseas for these reasons.

We expect that G20 in 2014 will be the subject of protest activity by a range of IMGs. Most of these are expected to be peaceful, but possibly confrontational and adversarial. It is likely however, that the extreme left wing groups, some of which include violence-prone anarchists and Marxists, will seek to participate and use the cover of mainstream protests to undertake violent action and coopt others to do the same.

Espionage remains a first-order threat to the security of Australia. A priority for ASIO is the continued detection and disruption of acts of espionage and foreign interference against Australian interests.

Numbers of irregular maritime arrivals continue to increase as people smugglers use established pipelines to Australia. Departures direct from Sri Lanka and Southern India are expected to continue.



Expenditure

Budget

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

In 2011–12, ASIO's operating result was a loss of $5.3 million against a Government approved operating loss of $6.2 million. This is a technical loss and is attributable to the accounting treatment required for employee provisions due to interest rate movements.

Revenue from Government in 2011–12 was $328.1 million, a decrease of $16.8 million from the 2010–11 financial year. This decrease was due to savings provided to Government in prior year budgets.

ASIO's budgetary situation will continue to place pressure on our ability to meet the expectations of Government and the Australian public, and will continue to be impacted by ongoing Government efficiency dividends and absorbed additional functions.

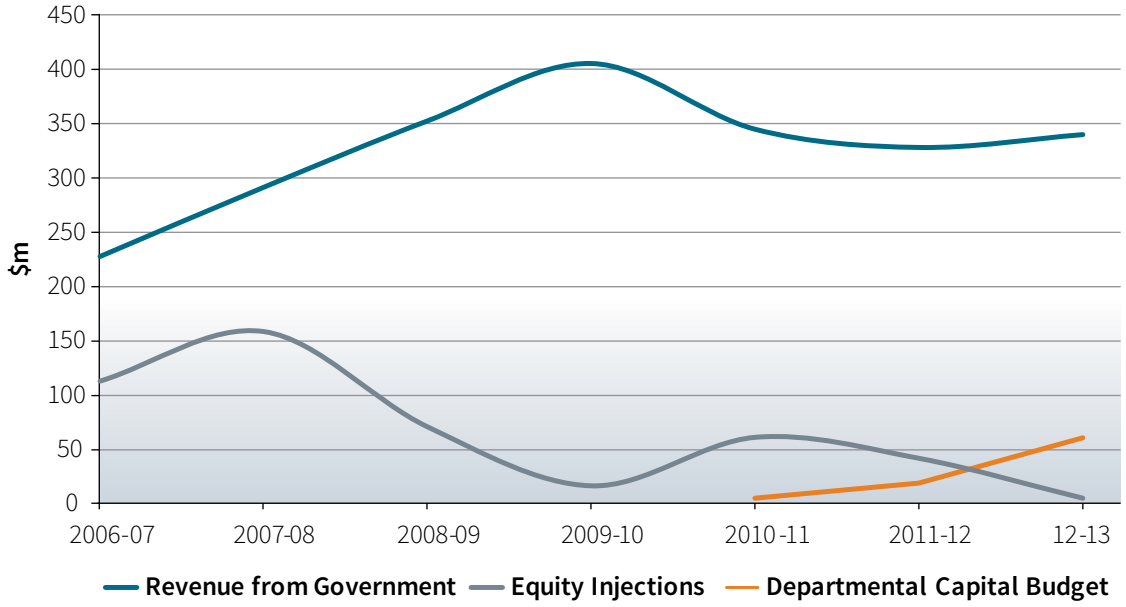
ASIO is continuing to examine options to manage the situation without a significant diminution of core operational work, including:

- Reductions to our overseas presence;
- Reducing our foreign engagement for training and capability development purposes; and
- Reducing the amount of domestic and overseas travel undertaken by ASIO officers.

ASIO has been required to make some difficult decisions regarding prioritisation and resourcing of activity over the 2011–12 financial year, and this is expected to continue in subsequent years. The fundamental considerations underpinning such decisions are the need to continue to invest in capability as defined by the professional skills of our staff and the technologies required to support our business.

The intelligence capabilities that exist within ASIO are national resources, and it remains vital they are preserved to address national security threats and the security challenges of the future. This remains particularly important as many of the skills required for ASIO to succeed in its mission require many years to develop.

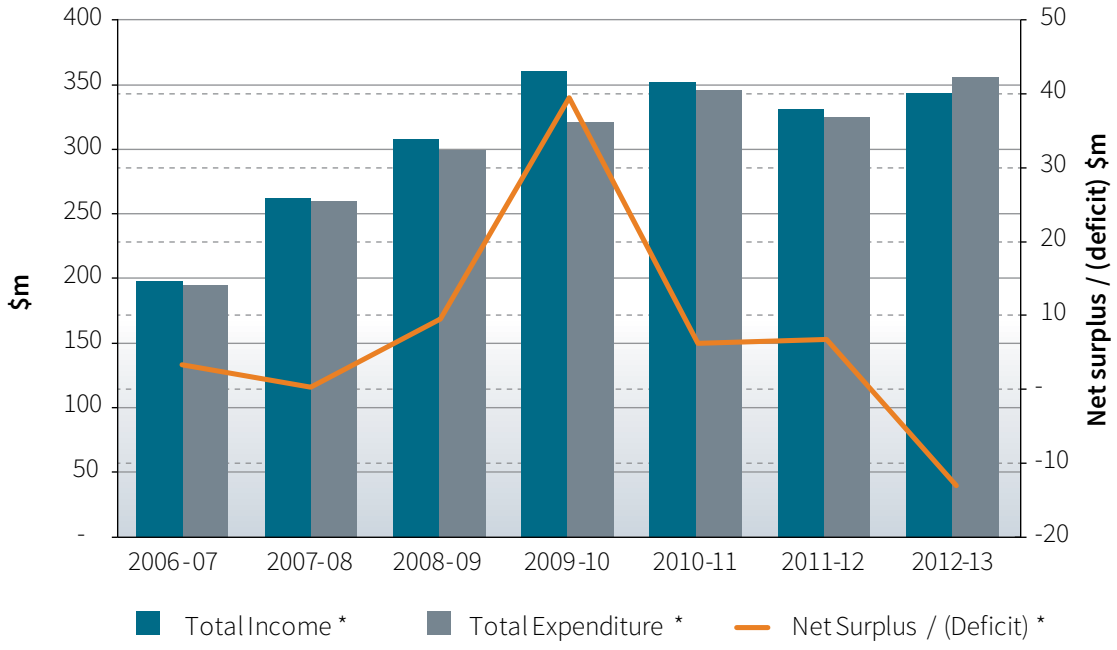
Figure 1: Revenue from Government: 2006–07 to 2012–13



Financial Performance

ASIO recorded an operating deficit of $45.5 million in 2011–12 due to the Net Cash Funding arrangements. Excluding depreciation, ASIO achieved an operating loss of $5.3 million.

Figure 2: Financial Performance: 2006–07 to 2012-13



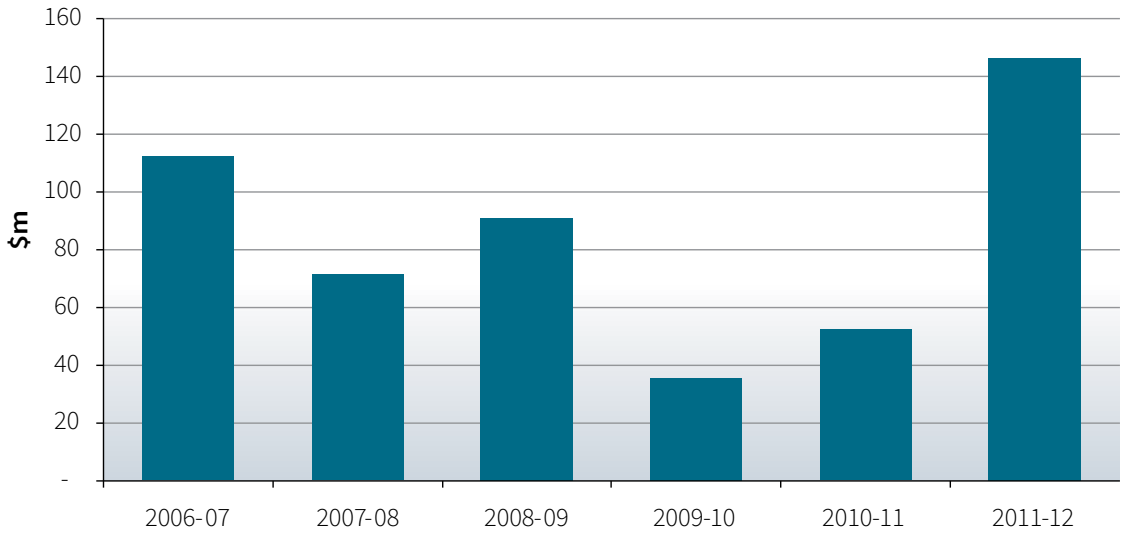
Strategic Allocation of Resources

ASIO's internal budget and resource allocations are set by the ASIO Finance Committee consistent with direction given by ASIO's Executive Board. Ongoing advice from the Finance Committee is provided to the Executive Board to ensure alignment of ASIO's budget and resource allocation with organisational priorities.

New Policy Proposals are endorsed by ASIO's Finance Committee, including appropriate financial strategies for the allocation of funds.

The Finance Committee also considers ASIO's financial policies and procedures against all audit, policy and regulatory requirements.

Figure 3: Purchase of capital items 2006–07 to 2011–12



Expenditure associated with the purchase of capital items in the reporting period increased significantly due to the costs associated with the new ASIO Central Office.

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 Executive Board. 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

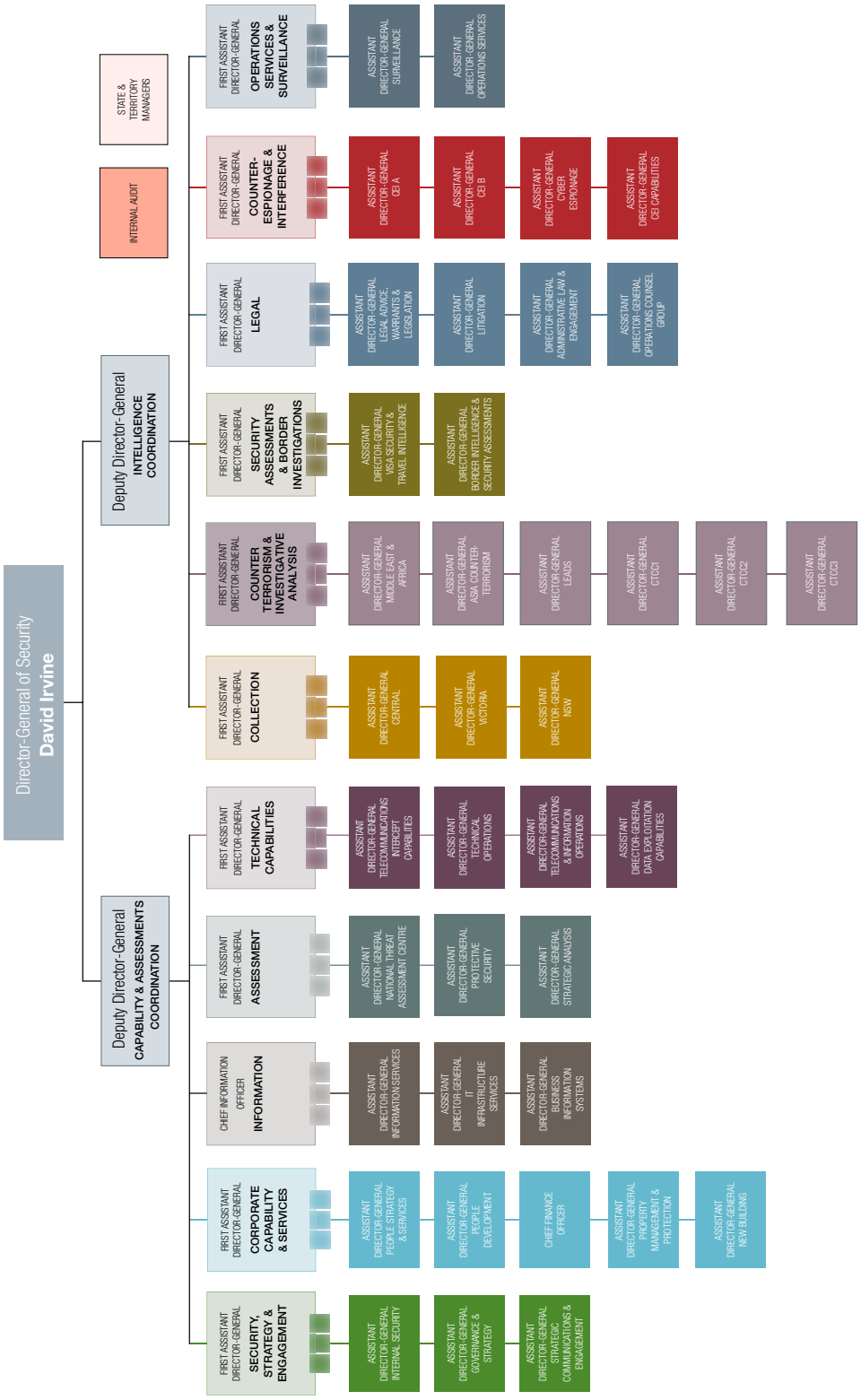
Organisational Structure

In 2011–12 ASIO continued to refine its structure in light of current and anticipated budgetary constraint. This follows a substantial period of growth for the organisation and is an evolving process, driven by financial requirements in the face of a complex security environment.

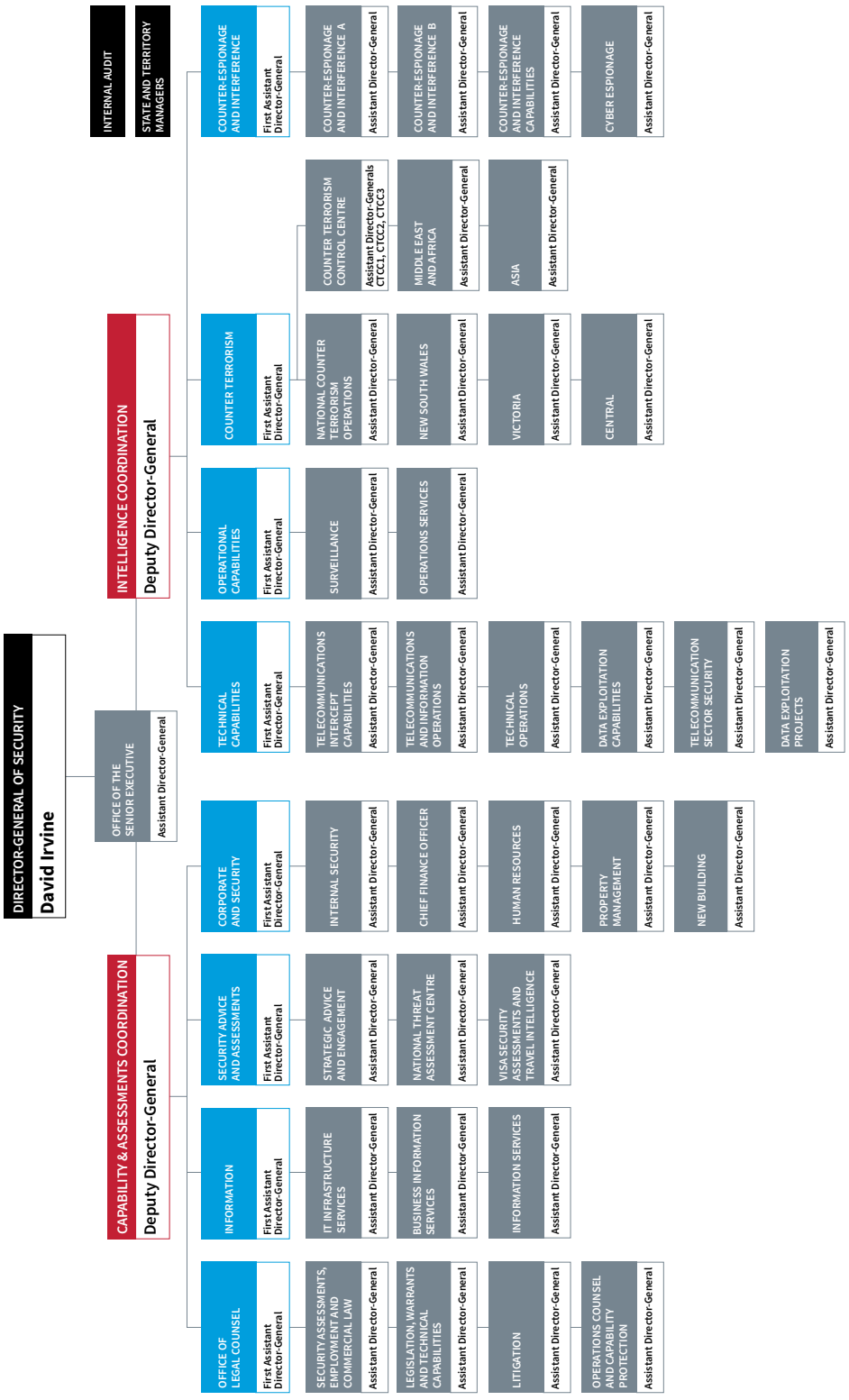
In October 2011, Ms Kerri Hartland joined ASIO on secondment as Deputy Director-General, Capability and Assessments Coordination for a two-year posting.

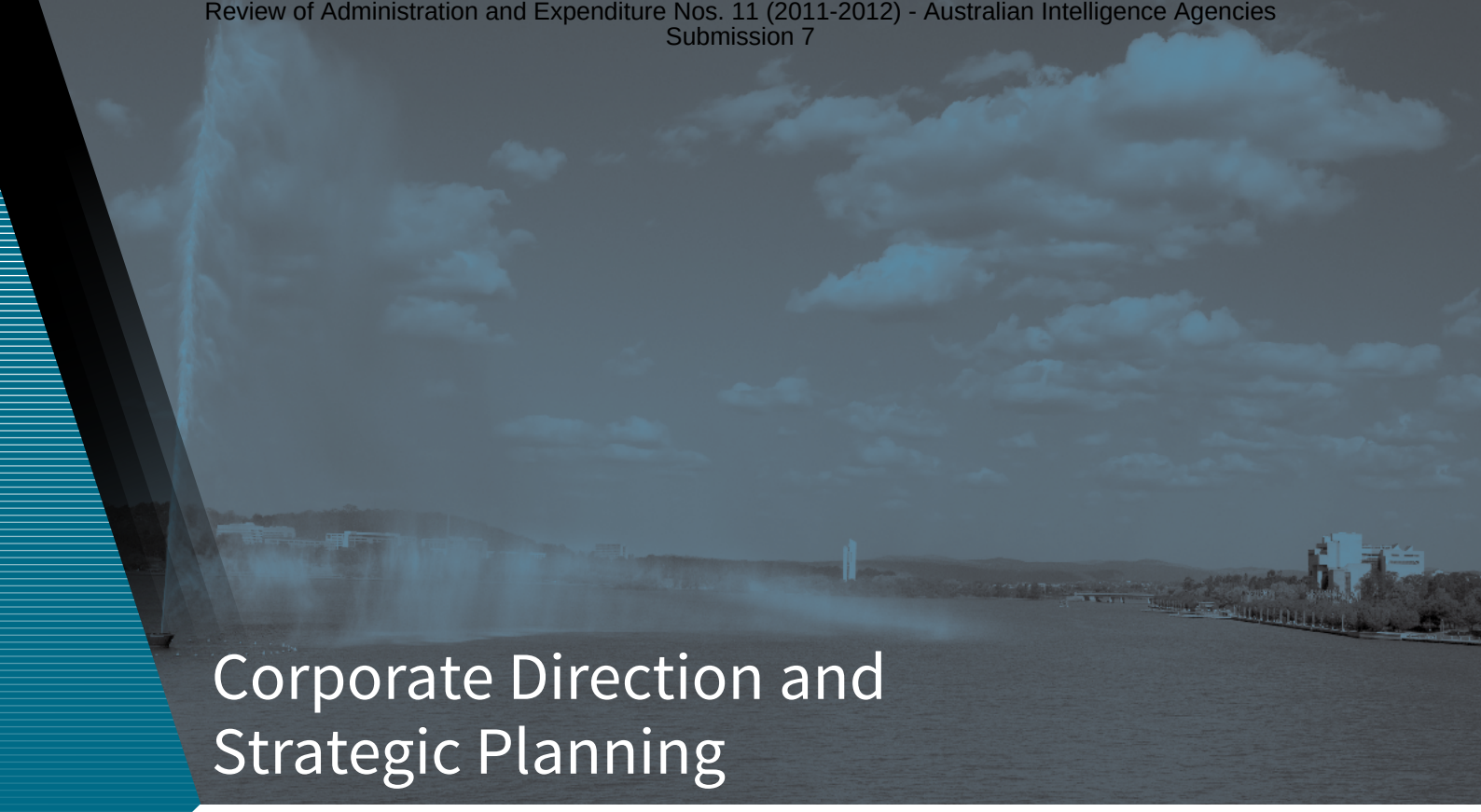
Since the conclusion of the reporting period, ASIO has implemented a revised structure. The new structure has shifted ASIO from eleven divisions to eight.

ASIO Senior Management as at June 2012



Current Organisation chart as at January 2013





Corporate Direction and Strategic Planning

ASIO Strategic Planning

In 2011–12 ASIO business planning and investment activities continued to deliver against four key programs, supporting ASIO's mission to protect Australia, its people and its interests from threats to security through intelligence collection, assessments and advice to government. These four key programs are:

- security intelligence analysis and advice;
- protective security advice;
- security intelligence investigations and capabilities; and
- foreign intelligence collection.

ASIO's reform and modernisation program has enabled agility in the face of a complex security environment. It has also set the foundation for ASIO's move from a period of growth to a period of consolidation by allowing for the maintenance of Australia's nationally important security intelligence capability, while finding efficiencies in undertaking its work.

Preparations for a more tightly constrained budgetary environment have resulted in ASIO deferring the remainder of its program of growth recommended by the Taylor Review in 2005. Consistent with the current budgetary situation, ASIO has reduced its recruitment target from 1 860 to 1 730 full-time equivalent (130 less than the review recommended).

This deferral of growth has been managed through a considered internal review of ASIO's staffing and resource allocation, resulting in recommendations to be implemented by January 2013.

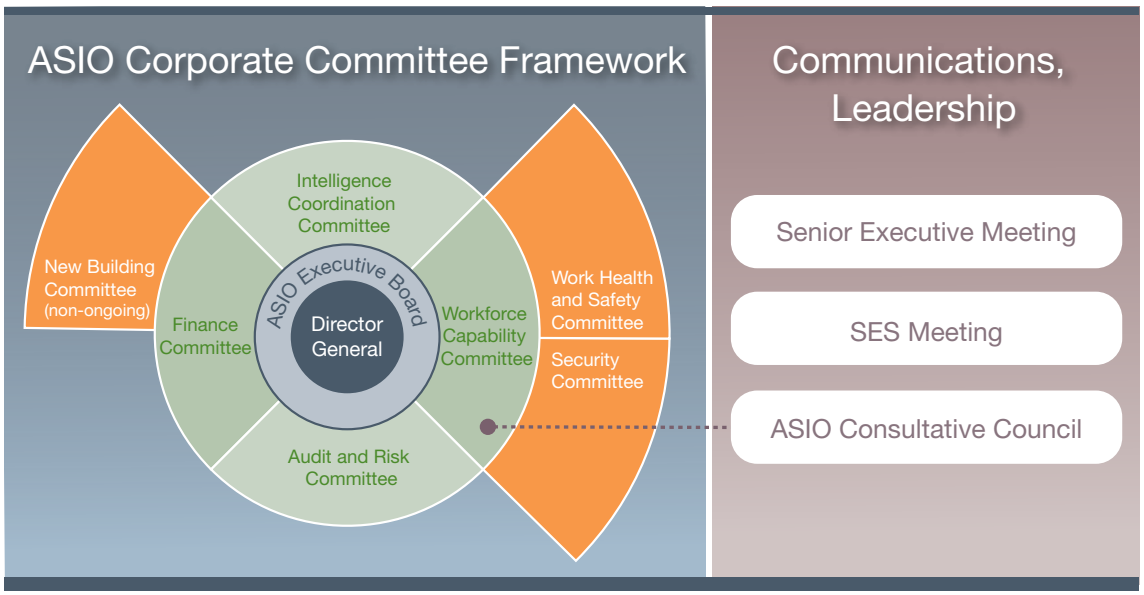
These include:

- A reduction from eleven to eight divisions; and
- Realigning staff allocation to ensure ASIO's ongoing capability to meet its obligations to Government.

Corporate Governance

In January 2012 ASIO implemented a new, simplified and more accountable committee structure to support strategic resource and business planning, risk management and performance reporting.

The revised ASIO corporate committee framework comprises of an Executive Board, supported by four corporate committees—each with a particular responsibility to inform the Executive Board and by this mechanism the Director-General.



ASIO Executive Board

The Executive Board is chaired by the Director-General and its members are the Deputy Directors-General and an external member, currently a Deputy Secretary from another government department.

Intelligence Coordination Committee (ICC)

The ICC provides strategic direction for the formal and effective coordination of ASIO's investigative and assessment priorities. It reviews performance against investigative and assessment objectives.

Workforce Capability Committee (WCC)

The WCC considers issues surrounding ASIO's workforce resourcing, including people, property and equipment. The Security Committee and Work Health and Safety Committee operate as sub-committees of the WCC.

Finance Committee (FC)

ASIO's FC advises the ASIO Executive Board on resource allocation and financial management and strategy.

Audit and Risk Committee (ARC)

The ARC provides independent assurance and assistance on ASIO's risk, fraud control and compliance framework, and its financial statement responsibilities. The ARC also facilitates the internal audit (in accordance with the Internal Audit Mandate) and external audit of ASIO and applying the outcomes.

In 2011–12 the Director-General appointed an independent chair of ASIO's Audit and Risk Committee.

Communications and Leadership Meetings

Senior Executive Meeting (SEM)

SEM is a regular forum allowing for the open exchange of emerging corporate and operational issues. It is attended by Senior Executive Service Band 2 and above.

Senior Executive Service Meeting (SESM)

The SESM is held each month and is attended by Senior Executive Service Band 1 and above. This management group meets to hold leadership discussions on key strategic issues impacting ASIO.

ASIO Consultative Council (ACC)

The ACC meets once a month to make recommendations to the Director-General on personnel policies and practices.

Audit and Evaluation

In 2011–12 ASIO continued to develop audit practices, specifically at the corporate committee level, in line with changes made to the *Financial Management and Accountability Act 1997* (FMA Act). These included:

- transitioning ASIO's audit and evaluation committee to an audit and risk committee (ARC). This reflects the management of risk within ASIO, in compliance of section 45 of the FMA Act and Regulation 22c of the Financial Management and Accountability Regulations;
- ensuring the ARC work plan meets all requirements set out in the FMA Act; and
- appointing an independent chair of the ARC.

ASIO also provides a training regimen for internal and external members of the ARC to ensure members remain aware of relevant policy and legislation.

Over the reporting period ASIO assisted the ANAO by completing sampling and fieldwork. This assisted with the conduct of an audit of financial statements across ASIO's operational expenditure. No issues requiring rectification were identified in this work.

ASIO also provided a response to the annual fraud survey conducted by the Australian Institute of Criminology in September 2011.

Assumed identities and commercial cover, as used to protect an ASIO officer's identity and prevent the potential compromise of ASIO operational activities, are subject to a six-monthly audit in line with Part IAC of the *Commonwealth Crimes Act 1914*. A small number of authorities are also maintained under *the NSW Law Enforcement and National Security (Assumed Identities) Act 2010* and are also subject to six-monthly audits. Compliance was found with each of the Acts across all of these audits.

Fraud Control

Throughout 2011–12 ASIO's fraud control processes were redesigned to consolidate responsibility and accountability for fraud control to ASIO's Internal Audit Unit. ASIO also maintains both a Fraud Control Plan and Fraud Policy. These documents are integral to the prevention and detection of fraud in ASIO.

Over the reporting period there were three allegations of fraud, with two instances confirmed. These matters were resolved through administrative action including adjustment of leave entitlements and increased management oversight.

Human Resource Management

Recruitment

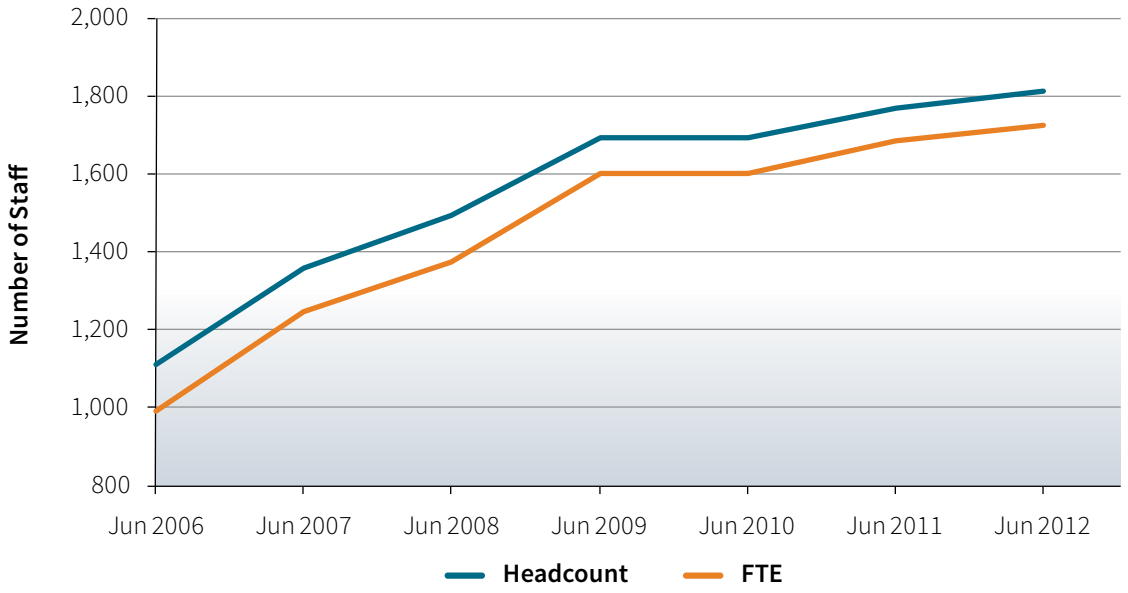
The 2005 Review of ASIO Resourcing, conducted by Mr Allan Taylor AM, identified 1 860 full-time staff as the optimal growth target for ASIO. In 2011–12 revisions to ASIO's budget resulted in an indefinite deferral of the remainder of organisational growth.

In February 2012 ASIO's approved staffing target was reduced to 1 760. However in order to manage within its current budget, ASIO is maintaining a level of 1 730 full-time equivalent staff.

While overall staff growth has been deferred indefinitely, ASIO will continue to recruit new intelligence professionals and technical officers within budget allocations and increase the skill-set of existing officers to meet the increasingly diverse challenges of our security environment.

The specialist requirements of ASIO's current recruitment efforts have required innovative ways of attracting suitable applicants. These include more specific sourcing strategies that limit advertising, for example, to online media or specialised publications. Selection and assessment activities are better aligned to the specific skills and capabilities required for individual roles.

Figure 7: Staffing growth, 2006–12



Training and Development

Intelligence Training

In 2011–12 ASIO's Intelligence Development Program (IDP) continued to provide new recruits with the foundations required to work as ASIO case officers and analysts. ASIO's IDP is an intensive program consisting of foundational training, core skills, competency assessments and work placements.

Two cycles of the IDP took place over the reporting period, with 32 officers graduating to become intelligence professionals.

In November 2011 ASIO dedicated resources to deliver against ongoing training requirements of ASIO's intelligence professionals. This function is now located in a dedicated post-IDP training unit and has developed a range of specialist courses to address the identified requirements of ASIO's case officers and analysts.

Corporate Training

Corporate training in ASIO is delivered at specified intervals of an officers' employment. Training activities address requirements as a new starter, when undertaking specific roles in the organisation and to meet development requirements.

Training activities include:

- An induction program for all new starters;
- Administrative training, including procurement, project management, finance and writing;
- Information technology, including training on systems specific to job-types;
- Ethics and accountability training—a core requirement to ensure all ASIO officers identify and act in-line with the key principles of ethical standards and accountability within the Australian Public Service (APS) and ASIO; and
- Discipline-specific courses, including social, political and religious history and influences.

Management and Leadership Skills

Building the management and leadership skills of ASIO's workforce, from Executive Level 1 to Senior Executive Service Band 1, continued to be a key priority in 2011–12. This occurred through a number of initiatives including a leadership program (Leading Edge), a Senior Executive Service Career Development Strategy and seminars contextualising ASIO's work in the broader intelligence and government community.

Additional development opportunities at the SES Band 2 level were provided through a rigorous 360 degree feedback program and coaching services by an external provider.

Over the reporting period ASIO undertook work to review the Leading Edge program offered to all members of ASIO's leadership team. The work conducted in 2011–12 will result in an updated program being delivered through the 2012–13 period.

Language Training

Over the reporting period ASIO increased its foreign language capabilities, while also extending its foreign language support activities with domestic and foreign partners. This has required an expansion of ASIO's Language Skills Development Program, which includes a language skills allowance supported by recognised proficiency testing.

E-learning

E-learning, a computer-based training method, was used in 2011–12 to deliver key training to ASIO staff on matters including information technology, workplace behaviour and workplace health and safety. Eight new modules were developed over the reporting period, many in response to feedback on performance management, new legislation and changes to ASIO policy.

Studies Assistance

A studies assistance program is available to ASIO officers and makes available opportunities to study across a range of disciplines relevant to ASIO's work. In 2011–12 ASIO revised its Study Support Program in preparation for a more constrained fiscal environment. However, ASIO's program remains one of the most generous offered amongst APS agencies.

In 2011–12 ASIO provided assistance to 147 officers enrolled in external study programs. ASIO fully or partly funded the language development training of 19 officers.

Australian Intelligence Community Training

ASIO is a proactive contributor to shared training opportunities across the AIC. These help foster a collaborative approach to intelligence challenges and a mutual understanding of the role of each AIC agency.

ASIO adopts a number of mechanisms to achieve this outcome, including participation and presentations to the AIC-wide Induction and Senior Officer Development programs. Additionally, ASIO routinely makes available places for other agencies to participate in ASIO training courses.

ASIO provides opportunities for staff to develop a shared understanding and culture of both the organisation and the National Intelligence Community through participation at the National Security College and their executive development activities.

Performance Management

In response to staff feedback, and as part of a broader reinvigoration of ASIO's performance management framework, work was conducted in the last reporting period to implement a more rigorous and meaningful framework for performance, development and career direction discussions.

The 2011–12 reporting period marks the first full year of Enhancing Performance—ASIO's system to manage, build and deliver capability within its workforce. Early feedback from ASIO staff indicates the new framework delivers better dialogue and more relevant training and employment considerations between ASIO staff.

Effort over the next reporting period will focus on a greater uptake of the new framework, to ensure the benefits are experienced by as many ASIO staff as possible.

Attachments

ASIO remains highly committed to the development and maintenance of relationships with other agencies. One of the programs in support of this goal is the placement of staff to and from ASIO with the following government agencies:

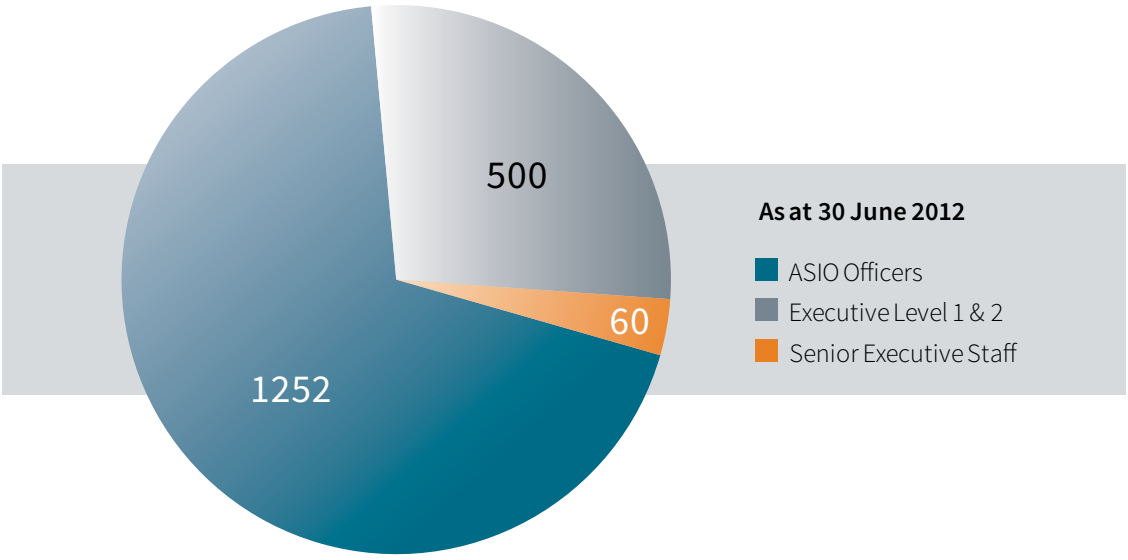
- Attorney-General's Department;
- Australian Customs and Border Protection Service;
- Australian Federal Police;
- Australian Secret Intelligence Service;
- Defence Intelligence Organisation;
- Defence Security Authority;
- Defence Signals Directorate;
- Defence Imagery and Geospatial Organisation;
- Department of Foreign Affairs and Trade;
- Office of National Assessments;
- Department of Immigration and Citizenship;
- Office of Transport Security within the Department of Infrastructure and Transport;
- Department of the Prime Minister and Cabinet;
- Department of Parliamentary Services;
- Department of Human Services
- AUSTRAC
- Department of Regional Australia, Local Government, Arts and Sport;
- The Treasury;
- Victoria Police;
- New South Wales Police; and
- Western Australia Police.

Staffing Ratios

Ratio of Senior Executive to Middle and Lower Level Staff

At 30 June 2012, there were 60 Senior Executive Service (SES) officers, 500 Executive Level 1 and 2 officers, and 1 252 other officers. These ratios are represented below in Figure 8.

Figure 8: Staff by Classification Group



Workplace Diversity

ASIO recognises that workplace diversity builds on the positive outcomes attainable by a workforce with varied skills, cultural perspectives and backgrounds. During 2011–12, ASIO undertook work in recognition of the value of an inclusive working environment, seeking to employ a range of people who reflect the broad Australian community.

The diversity of ASIO's staff is reflected in the table below.

Table 1: 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)	60	15	0	0	1	58
Senior Officers[3]	500	181	17	0	8	458
AO5[4]	617	318	47	3	5	549
AO1 – 4[5]	536	276	24	3	4	496

Information Technology Officers Grades 1 and 2	90	13	6	0	2	85
Engineers Grades 1 and 2	9	0	0	0	0	9
Total	**1,812**	**803**	**94**	**6**	**20**	**1,655**

[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

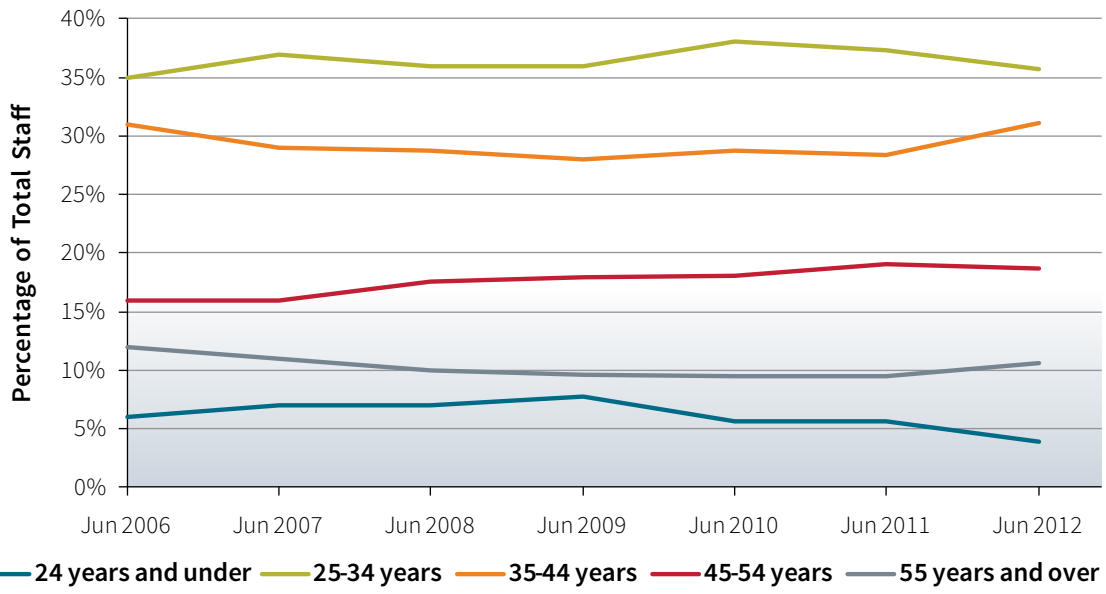


Figure 10: Length of Service of ASIO staff

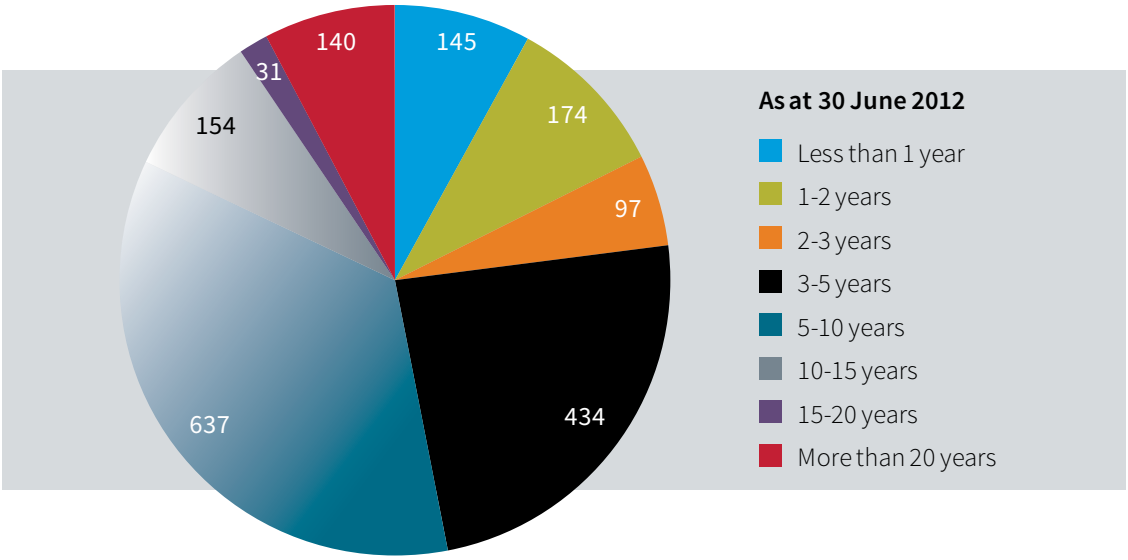
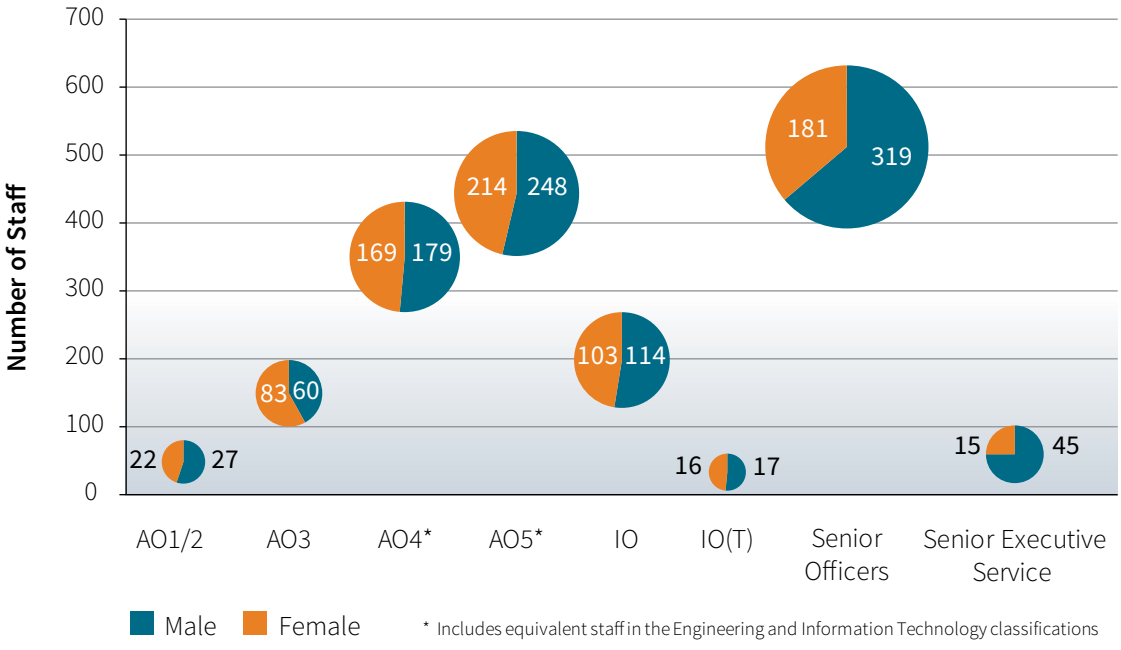


Figure 11: Gender balance by classification



Staff Complaints

The reporting period marked the first full year of ASIO's anti-bullying campaign, Silence Hurts. In May 2012 ASIO conducted an organisation-wide staff survey which included questions specific to working relationships, bullying and harassment. The survey noted a significant decrease in the number of staff reporting that they had been subject to harassment or bullying in the last 12 months.

A broad range of assistance is made available to staff members or managers requiring guidance or support to those who have witnessed or experienced bullying or harassment. In 2011–12, nine requests for support or information were raised for advice on the options available.

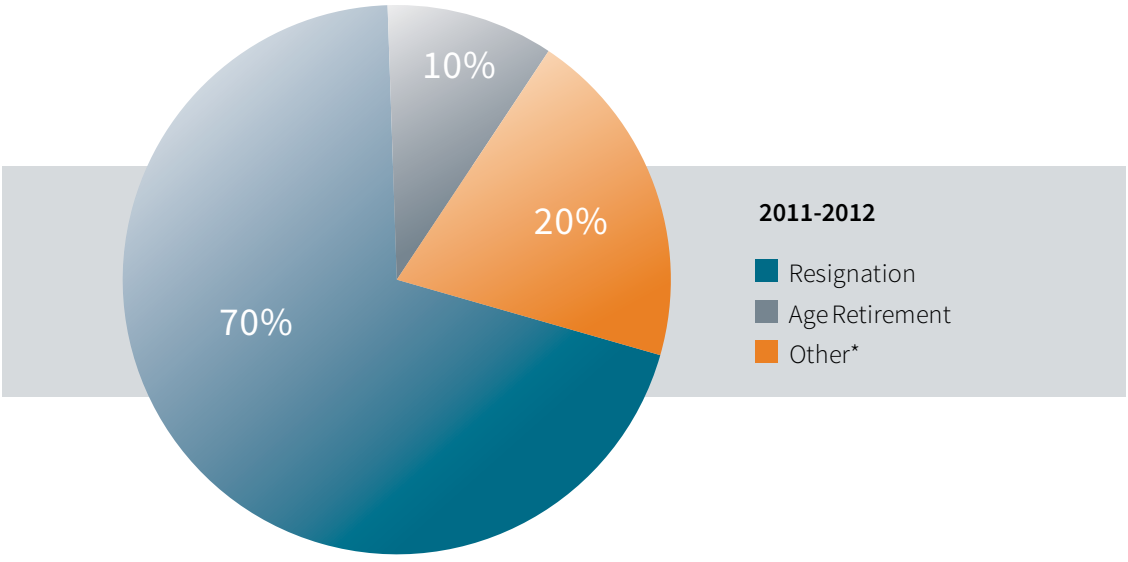
Advice and support on workplace issues is also available to staff via an external ombudsman. The Ombudsman's goal is to resolve issues impartially, informally and quickly where possible through advice, consultation and mediation.

In 2011–12 the Ombudsman responded to a range of matters including workplace issues, transfer and employment opportunities and conditions of employment.

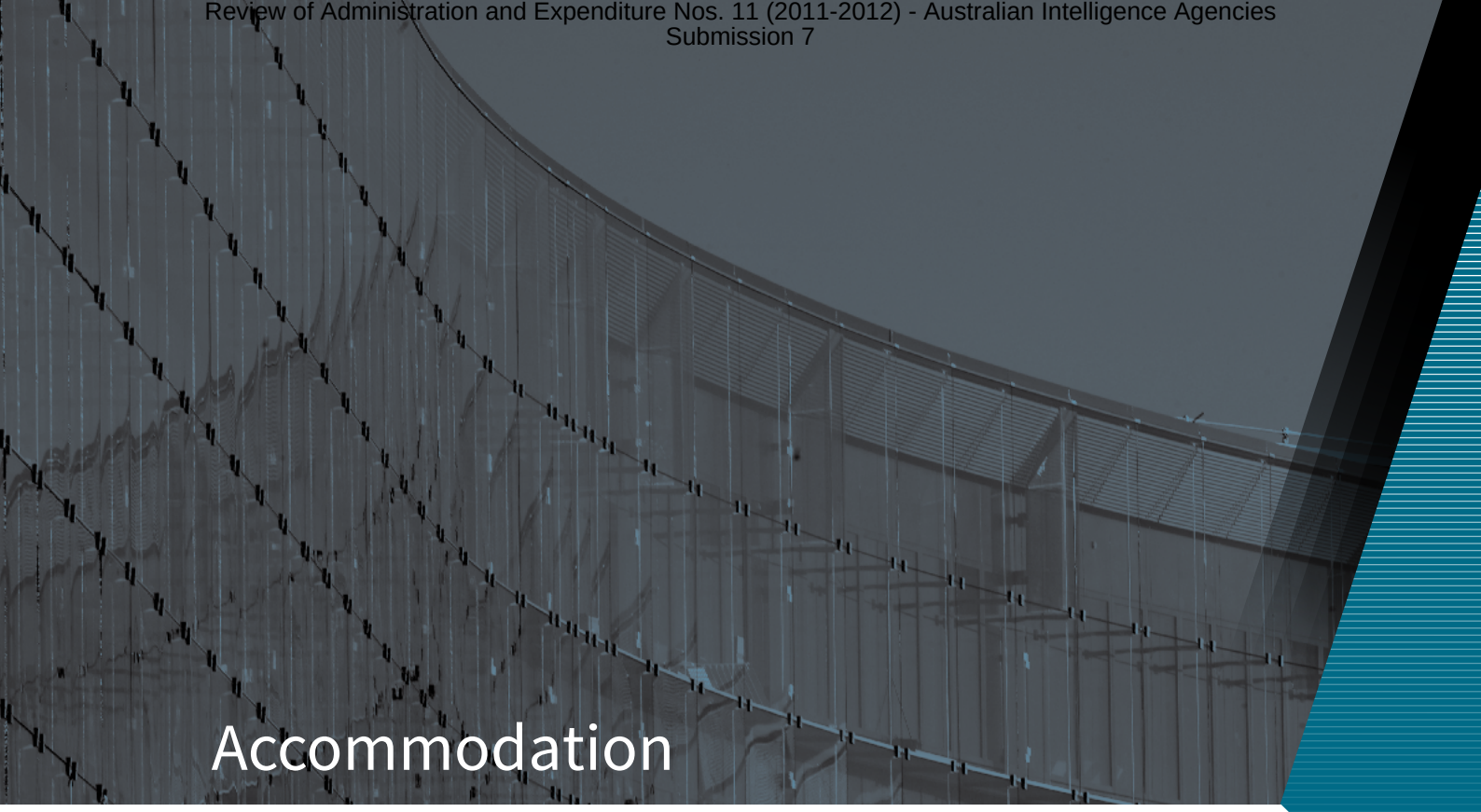
Separation Rates

During 2011–12, ASIO experienced a decrease in the separation rate from 5.8 per cent (corrected down from 5.9 per cent) in 2010–11 to 4.7 per cent in 2011–12, with this level comparing favorably to the APS average separation rate of 6.6 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

Construction of ASIO's new Central Office continued over the reporting period. Delays in the construction of ASIO's new Central Office have led to the handover date slipping.

The project has experienced overruns to date of $41.6 million, which equates to seven per cent of the approved budget of $589.2 million set in 2008. ASIO's contribution to cost overruns is $24.3 million which is being met within existing budgets.

ASIO is now scheduled to take possession of the new building mid-2013. Relocation is expected to begin early in the second half of 2013. It is important to consider these budgetary pressures and scheduling delays in the context of the complexity and tenure of the project, given the approved budget and construction schedule was approved in 2008.

State and Territory Offices

The previous reporting period marked the completion of a national program to deliver upgraded ASIO accommodation around Australia. In 2011–12 work with ASIO's state and territory offices has focused on implementing cost effective energy saving measures to make financial savings and improve ASIO's green credentials.

ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security

Legislation and Litigation

Legislative Amendments

Throughout 2011–12, ASIO and other Australian government agencies pursued a range of legislative amendments to better meet the challenges posed by current and emerging technologies and modernise existing legislation. While some of these amendments occurred outside of the reporting period, much of ASIO's contribution towards these reforms occurred in 2011–12. This work includes:

- reform of the *Telecommunications (Interception and Access) Act 1979* including proposals that modernise lawful access to communications and associated communications data;
- amendments to the *Telecommunications Act 1997* and other relevant legislation to strengthen measures to mitigate the national security risks posed to Australia's telecommunications infrastructure; and
- amendments to the ASIO Act and *Intelligence Services Act 2001* which seek to improve the operational capabilities of intelligence agencies, as well as making some technical and administrative amendments.

These legislative amendments, currently being considered by the PJCIS, are technologically neutral to enable ASIO, and other Australian agencies, to operate effectively into the future while maintaining the appropriately stringent accountability regime that already exists across intelligence and law enforcement agencies.

ASIO provided a number of submissions to the PJCIS to support the Committee's review, including:

- a number of classified submissions covering the range of legislative reforms under consideration;
- an unclassified submission on data retention (Submission 209 on the PJCIS website[1]);
- an unclassified supplementary submission on data retention prepared in conjunction with the AFP and the ACC; and
- a number of classified submissions covering the range of legislative reforms under consideration.

The Director-General of Security, along with other senior ASIO representatives, also appeared before the PJCIS in a number of *in camera* hearings to provide further information to support ASIO's views and position on the reforms being considered.

[1] www.aph.gov.au/pjcis/.....

ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security | 34
Review of Administration and Expenditure

ASIO does not see the range of reforms under consideration as solving all of the technological and legislative challenges currently facing the organisation. Neither does it see the reforms as expanding on its existing powers. However, these reforms would go much of the way to reclaiming lost capability and establishing a framework of legislation that would remain current and enable ASIO to undertake our functions regardless of the specific technology being utilised by individuals of security concern.

Cybercrime Legislation Amendment Act 2012

The stored communications preservation regime, which received Royal Assent outside the reporting period, on 12 September 2012, allows intelligence and law enforcement agencies to request targeted retention of stored communications. This Act applies only to specified stored communications, such as emails or voice mail messages, and includes the content rather than just the communications data that falls within the data retention regime under consideration.

Under this Act, notices can be issued to create an obligation for industry to preserve stored communications for up to 90 days from the date of issue of the relevant notice. ASIO will then require a warrant to access the preserved stored communications.

In accordance with the phased commencement of the Act, ASIO could only issue historic domestic preservation notices from 10 October 2012 and only issue ongoing domestic preservation notices from 12 December 2012, meaning no notices were issued by ASIO in 2011–12.

Independent National Security Legislation Monitor

Throughout 2011–12, ASIO continued to engage with the Independent National Security Legislation Monitor (INSLM) to support and assist ongoing work in the review of ASIO's questioning, and questioning and detention warrants. ASIO has provided information to the INSLM through formal hearings with senior officers as well as written, classified submissions covering ASIO's use of these special powers.

ASIO last executed a questioning warrant in 2009–10, the sixteenth time these powers have been utilised. Fortunately, circumstances have not since arisen requiring ASIO to seek a questioning and detention warrant.

Litigation Matters

In 2011–12, the trend of increased ASIO involvement in legal and judicial matters continued, with ASIO contributing actively to prosecutions in national security cases and remaining involved in a number of civil matters arising from the discharge of statutory functions and indirectly in other proceedings where ASIO information was relevant.

Throughout the reporting period, ASIO was involved in 58 litigation matters, including criminal (particularly terrorism) prosecutions, judicial and administrative reviews of security assessments, and a range of civil actions.

There remain a number of other challenges of ASIO adverse security assessments in the Administrative Appeals Tribunal (AAT) and the Federal Court. Each of these cases involves substantial legal, operational and administrative involvement from ASIO and this continued to put strain on ASIO's resources throughout 2011–12.

The scope and diverse nature of ASIO involvement in legal proceedings continues to place strain on the organisation's legal, operational and administrative resources in preparing appropriate support and input, while maintaining appropriate protection of security classified information.

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.

Security of ASIO

The secure and effective conduct of ASIO operations and investigations begins with strong personnel, physical, information and IT security supported by appropriate governance, policy and technological mechanisms.

These elements, engaged in concert, serve to protect the information, people and business systems necessary to deliver ASIO's outcome—to protect Australia, its people and its interest from threats to security through intelligence collection, assessment and advice to government.

The reporting period marked the first full year of ASIO operating within the Government's new Protective Security Policy Framework (PSPF). It also marked a significant revision of the Sensitive Material Security Management Protocol, which provides detailed policy guidance for those agencies operating in the highly classified Top Secret environment.

Security governance and policy

Security is one of the high level risks identified in ASIO's Strategic Risk Management Framework. Within ASIO's governance structure, security is overseen by the ASIO Security Committee, where senior executive-level representatives consider and recommend actions for the secure conduct of ASIO business to the ASIO WCC, ASIO Executive Board, and, ultimately, the Director-General.

ASIO's security policy, practices and governance are guided by the PSPF. This framework informs the considerations and recommendations made by ASIO's Security Committee.

Security clearances in ASIO

Initial and ongoing vetting of ASIO staff is conducted in-line with whole of government requirements, security risk management strategies, policies and procedures. During the course of employment, ASIO officers must maintain clearance suitability and report proactively any changes in circumstances which might impact their clearance.

To ensure ASIO officers remain aware of their obligations, all ASIO staff participate in security awareness education at the outset of employment and at regular intervals thereafter.

In support of the high expectations of ASIO staff and the need to ensure ASIO's security integrity, ASIO provides health and wellbeing support through an employee assistance program and psychological health services.

Vetting Review (revalidation and re-evaluation)

ASIO conducts a comprehensive program of revalidation and re-evaluation of staff members' security clearances to ensure staff remain suitable to access highly classified information. This involves the review of a person's circumstances, including financial, personal and psychological factors.

Security breaches

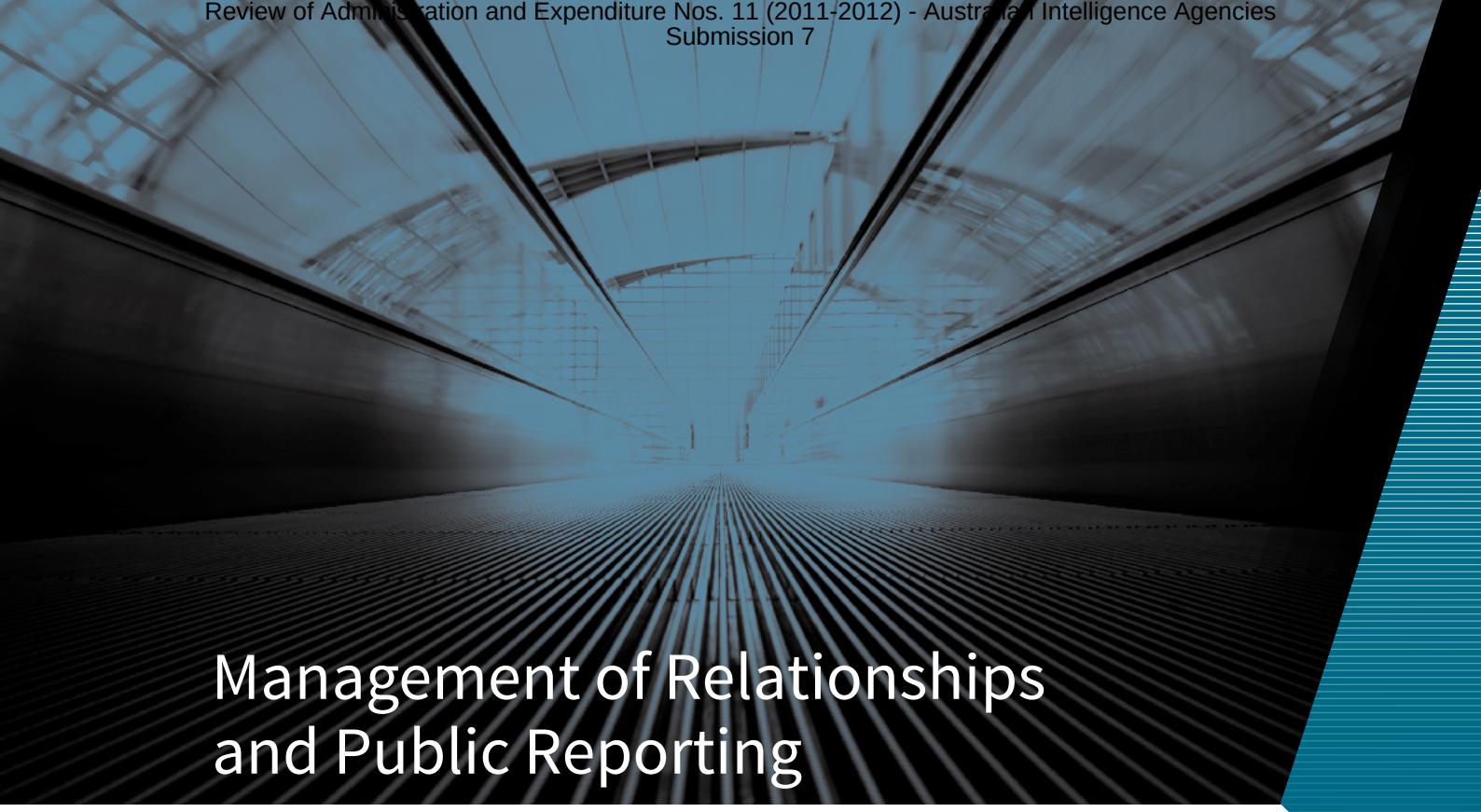
ASIO strives to exemplify security best practice and engages a robust array of internal security policies. One of these measures is the reporting of security breaches. In this context a security breach is an accidental or unintentional failure to observe the protective security mandatory requirements.

ASIO's senior executive is briefed on security breaches and senior managers are notified of breaches occurring within their divisions and branches in a timely fashion to enable proactive management of each occurrence.

E-Security Arrangements and Enhancements

In 2011–12 ASIO contributed to a significant body of work in providing advice to government and the private sector to mitigate threats posed by cyber intrusions. ASIO's considerable understanding of the threat of cyber intrusions, particularly against government bodies, has translated into significant e-security arrangements for ASIO. Additionally, ASIO e-security arrangements are prioritised to ensure ASIO Information Communication Technology (ICT) targets of highest value remain the most protected.

Over the reporting period work continued to provide assurance that ASIO's ICT systems were designed, installed, maintained and operated within acceptable security risk boundaries. ASIO applies stringent control in the introduction or implementation of ICT systems to ensure potential vulnerabilities are remedied.



Management of Relationships and Public Reporting

ASIO's Domestic Relationships

A difficult balance in any security-related government body is managing the need to conduct its work in secret and the need to develop community trust through the maintenance of sound relationships. ASIO continues to see fundamental value in reaching out to, and working with, partners.

A particular focus during 2011–12 has been for ASIO to enhance awareness of the work of the organisation amongst the public, and across government and industry partners. This approach to domestic engagement has included an increase in the number of public addresses by the Director-General, regular senior officer partnership forums with state and federal government and the provision of security reporting to industry via the Business Liaison Unit (BLU).

ASIO conducts an annual stakeholder satisfaction survey, seeking feedback on levels of satisfaction with ASIO engagement, views on collaboration and an evaluation of ASIO's information and advice. The 2011 survey included an email component, aiming to collate broader feedback, while still using face-to-face interviews. Responses were gathered from a range of government and industry stakeholders at various levels of representation.

The feedback indicated a significant improvement in engagement with ASIO, something which ASIO is actively building upon.

ASIO continued to see value in providing information relevant to the security of Australia and its interest via the BLU website. Members of the private sector can access this information via a free subscription to the website. While reports are necessarily unclassified, they serve to increase security awareness and contextualise potential threat information for an audience that might otherwise not consider the practical implications of security matters to their business.

ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security

ASIO's International Relationships

ASIO continues to actively foster and maintain positive working relationships with a range of international partners—both traditional and non-traditional. At the end of this reporting period, the Attorney-General had authorised ASIO to liaise with 340 authorities in 125 countries.

These partnerships have a number of mutual advantages. Shared expertise, capabilities and resources bring natural efficiencies to security intelligence work. More than this, the inherent requirement for a rapid response to unfolding security events requires established relationships and systems.

Over the reporting period ASIO's international relationships with key foreign partners were further strengthened with the collegiate approach to the preparation and conduct of secure large scale events. ASIO provided security intelligence support to a number of international events including:

- the Rugby World Cup in New Zealand in September and October 2011;
- Asia Pacific Economic Cooperative Forum in USA in November 2011;
- the Anzac Day commemorative services in Turkey and France in April 2012; and
- the NATO-International Security Assistance Force Summit in USA in May 2012.

Security threats in Australia emanate from a variety of sources, many with international or transnational influences. ASIO is responsible for the security of Australia, its people and its interests, both domestically and overseas, making ASIO's international relationships critical.

As detailed in the Expenditure component of this report, a constrained budgetary environment has required difficult decisions to be made in regard to ASIO's overseas representation. This includes:

- Reducing our overseas presence; and
- Reducing our foreign engagement for training and capability development purposes.

Public Reporting and Oversight

ASIO's Annual Report to Parliament 2011–12

ASIO produces a highly classified annual report which covers ASIO's operational and corporate activities in significant 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 unclassified 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

A continued focus for ASIO in 2011–12 has been to enhance the public awareness of the work of the organisation and in doing so, dispel many of the myths and misreporting that naturally surround ASIO's business.

ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security | 40
Review of Administration and Expenditure

Over the reporting period the Director-General addressed ten conferences and seminars as well as two undertaken by the Deputy Director-General Capability and Assessments Coordination. Complementing these public events, ASIO maintains an active outreach and community engagement program.

The Director-General, Deputy Director-General and several undeclared senior officers have actively participated in numerous outreach and community oriented events, including discussion with academia, business, industry associations, community and religious groups as well as actively engaging across government both at the federal and state levels. These events are focused on providing relevant information from ASIO as well as promoting holistic exchange and dialogue; these events are neither publicised nor open to the media.

The ASIO website is a key tool for members of the general public to gain an understanding of the work of ASIO and to find information on a variety of frequently asked questions. In 2011–12 the ASIO website was updated to include public statements, media interviews and unclassified submissions to Parliamentary Inquiries.

Parliamentary Oversight

Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is established at the start of each Parliament. The Committee is appointed under section 28 of the *Intelligence Services Act 2001* (the ISA). Section 29 of the ISA states that the functions of the Committee are to:

- review the administration and expenditure of the ASIO, ASIS, DIGO, DIO, DSD and ONA including the annual financial statements of these agencies;
- review any matter in relation to ASIO, ASIS, DIGO, DIO, DSD or ONA referred to the Committee by the responsible Minister or a resolution of either House of the Parliament;
- review, as soon as possible after the third anniversary of the day on which the *Security Legislation Amendment (Terrorism) Act 2002* receives the Royal Assent, the operation, effectiveness and implications of amendments made by that Act and the following Acts - *The Border Security Legislation Amendment Act 2002, The Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* and *The Suppression of the Financing of Terrorism Act 2002;*
- review, by 22 January 2016, the operation, effectiveness and implications of Division 3 of Part III of the *Australian Security Intelligence Organisation Act 1979*; and
- report the Committee's comments and recommendations to each House of the Parliament and to the responsible Minister.

In addition, under Section 102.1A of the Criminal Code, the Committee may review the listing of organisations as terrorist organisations. The Committee is not authorised to initiate its own references, but may resolve to request the responsible Minister refer a particular matter to it for review.

Senate Standing Committee on Legal and Constitutional Affairs

ASIO appears before the Legal and Constitutional Affairs Committee as part of the Attorney-General's portfolio. Over the reporting period ASIO appeared at the Supplementary Budget Estimates in October 2011 and Additional Estimates in February 2012 and Budget Estimates in May 2012.

As the only declared ASIO officers, the Director-General of Security and the Deputy Director-General, Capability Assessments and Coordination, appeared at the three hearings. Following the hearings ASIO responded to questions on a range of topics relevant to both the undertaking of ASIO's functions and the allocation of resources in undertaking its functions.

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.

The IGIS has the legislated remit to conduct inspections and inquiries of AIC agencies, providing a sound accountability mechanism for ASIO.

In 2011 the IGIS commenced an Inquiry into ASIO's security assessments for community detention determinations. The inquiry examined cases where ASIO was required to provide a security assessment for community detention purposes, and considered ASIO procedures, policy and adherence to relevant legislation.

The report from this inquiry, provided to the Attorney-General in June 2012, contained three recommendations. ASIO agreed to two recommendations, pertaining to recording decision-making processes and the maintenance of ASIO's policy and training documentation for interviews, particularly with regard to mental health considerations. The remaining recommendation, of ASIO providing risk mitigation advice to DIAC should DIAC allow a person subject to an ASA into community detention, was considered by ASIO. However, ASIO considers this to be outside its current remit and might have unintended consequences.

In January 2011 the IGIS announced an inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005. An unclassified version of the IGIS report was released on March 2012. The IGIS found that no Australian agency or official was:

- involved in making arrangements for Mr Habib's transfer to Egypt, or was present at any time during his removal from Pakistan; or
- knew Mr Habib's place of detention in Egypt, attended his place of detention or was present during interrogations of Mr Habib in Egypt.

ASIO accepts the IGIS recommendations relevant to ASIO policies and procedures, including engagement with, and provision of information to, foreign authorities.

Glossary

AAT	Administrative Appeals Tribunal
ACC	ASIO Consultative Council
AFP	Australian Federal Police
AIC	Australian Intelligence Community
AQAP	al-Qa'ida in the Arabian Peninsula
ARC	Audit and Risk Committee
ASA	Adverse Security Assessment
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
BLU	Business Liaison Unit
CSOC	Cyber Security Operations Centre
DIAC	Department of Immigration and Citizenship
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DSD	Defence Signals Directorate
FC	Finance Committee
ICT	Information and Communications Technology
IDP	Intelligence Development Program
IGIS	Inspector-General of Intelligence and Security
IMA	Irregular Maritime Arrival
INSLM	Independent National Security Legislation Monitor
ONA	Office of National Assessments
PJCIS	Parliamentary Joint Committee on Intelligence and Security
SEM	Senior Executive Meeting
SES	Senior Executive Service
SESM	Senior Executive Service Meeting
WCC	Workforce Capability Committee
WMD	Weapons of Mass Destruction