Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure

No.12 2012–2013

www.asio.gov.au

Contents

Figures 3
Tables 3

Scope of review 5
Reader's guide 6

Executive summary 7
The security environment 2012–13 and outlook 7
Expenditure 7
Structure of the Organisation 7
Corporate direction and strategic planning 7
Human resource management 7
Accommodation 8
Legislation and Litigation 8
Security of ASIO 8
Relationships 8
Accountability 8

ASIO's role and functions 9

The security environment 2012–13 and outlook 10
Espionage and foreign interference 10
Politically motivated violence 10
Communal violence and violent protest 11
Border security 11
Outlook for the security environment 11

Expenditure 13
Budget 13
Financial performance 13
Strategic allocation of resources 14
Financial management and internal controls 15

Structure of the Organisation 16
Organisational structure 16

Corporate direction and strategic planning 19
ASIO strategic planning 19
Corporate governance 19
Communications and leadership meetings 21
Audit and evaluation 21
Fraud control 21

Human resource management 22
Recruitment 22
Training and development 22
Performance management 24
Attachments 25
Staffing ratios 25
Staff complaints 28
Separation rates 28

Accommodation 29
Ben Chifley Building, Canberra 29
State and territory offices 29
Legislation and litigation 30
Legislative amendments 30
Litigation matters 31
Use of ASIO special powers 32
Security of ASIO 33
Security governance and policy 33
Security clearances in ASIO 33
Security breaches 33
Relationships, reporting and accountability 34
Oversight and accountability mechanisms applying to ASIO 34
Parliamentary oversight 35
External oversight mechanisms 36
Public statements 37
ASIO's domestic relationships 38
ASIO's international relationships 38
Glossary 39

Figures

Figure 1 Revenue from government for years from 2007–08 to 2012–13 14
Figure 2 Financial performance for years from 2007–08 to 2012–13 14
Figure 3 Purchase of capital items for year from 2007–08 to 2012–13 15
Figure 4 Staffing growth for years from 2007–08 to 2012–13 22
Figure 5 Management and Leadership in Security Intelligence strategy 23
Figure 6 Ratio of SES to middle and lower level staff 25
Figure 7 Age of staff for years from 2007–08 to 2012–13 26
Figure 8 Length of service of ASIO staff for 2012–13 27
Figure 9 Gender balance by classification for 2012–13 27
Figure 10 Separations by percentage of total staff and reason for 2012–13 28

Tables

Table 1 Workplace diversity of ASIO staff 26

Scope of review

The Australian Security Intelligence Organisation (ASIO) submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review into Administration and Expenditure No. 12 provides a detailed account of ASIO's activities during the financial year. For 2012–13 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.

Reader's guide

ASIO's role and functions

- Outlines ASIO's role and functions, as well as a brief description of its legislative and oversight frameworks.

Security environment and outlook

- Provides information on the security environment throughout the reporting period and its implications for ASIO's resourcing. Also includes an outlook of the security landscape for 2014 and beyond.

Expenditure

- Outlines ASIO's organisational income and expenditure, including measures ASIO has taken to offset absorbed additional costs.

Organisational structure

- Provides ASIO's organisational structure at the end of the reporting period and describes the changes that took place and why.

Corporate direction and strategic planning

- Describes ASIO's strategic planning and how this will help ASIO respond to current and emerging challenges, as well as how ASIO's corporate governance structure supports the decision-making of the ASIO Executive Board and the Director-General.

Human resource management

- Outlines how ASIO manages and improves its human resources to help the Organisation achieve its mission.

Accommodation

- Describes the administration of ASIO's accommodation, including the progress made during the reporting period.

Legislation and litigation

- Provides information on relevant legislative amendments and inquiries, and ASIO's contribution to various criminal and administrative litigation matters.

Security of ASIO

- Outlines ASIO's approach to the security of its people, premises and information through strong security policies, practices and technologies.

Relationships, reporting and accountability

- Describes ASIO's accountability to the government and various independent oversight mechanisms, as well as how ASIO's maintenance of its domestic and international relationships supports the Organisation to investigate and provide advice on matters of security.

Executive summary

The security environment 2012–13 and outlook

Espionage and foreign interference

In 2012–13 espionage and foreign interference targeting Australian interests remained a serious and sustained threat. ASIO continued to work with its partners in government and industry to deliver ASIO's mission to discover, defend against and degrade these activities, and to provide a holistic protective security response.

The scale and sophistication of state-sponsored cyber attacks against Australian Government and private sector systems has increased considerably in recent times.

In addition, individuals who exploit their legitimate access to national systems and environments to publicly disclose classified and sensitive information are a constant source of potential harm to Australia's national interest.

The source and type of espionage and foreign interference is becoming more varied and the effects more diverse.

Politically motivated violence

Politically motivated violence, particularly terrorism, is constantly evolving and remains a significant threat to Australia and Australians, accounting for about 70 per cent of ASIO's operational effort.

The threat of lone actor attacks utilising basic capabilities and simple technologies does not supplant the ongoing threat from more organised and directed extremists, who continue to aspire to conduct large scale, mass-casualty attacks against the West.

The Syrian conflict poses its own challenges for ASIO in combating the threat of terrorism to Australia. Many more Australians have travelled to the region to engage in fighting than for any comparable conflict.

We expect these challenges to play out over several years and have a medium- to long-term influence on the extremist environment in Australia, beyond any immediate resolution to the Syrian conflict—which is unlikely.

Expenditure

In 2012–13 ASIO recorded an operating deficit of $45.1 million due to the net cash funding arrangements. Excluding depreciation, ASIO achieved an operating surplus of $1.5 million.

ASIO has adapted to the constrained fiscal environment through rigorous prioritisation.

Structure of the Organisation

Over the reporting period ASIO continued to consolidate and refine its organisational structure in response to a continually tightening fiscal environment. ASIO adopted a new organisational structure designed to align like functions and reinforce the way each Division contributes to ASIO's mission and maximise the impact of outreach.

Corporate direction and strategic planning

The reporting period saw the conclusion of ASIO's *Strategic Plan 2011–13.* In review of the plan, it was recognised that many of ASIO's broad strategic objectives remained. This is reflected in ASIO's new *Strategic Plan 2013–16* which has adopted and, where appropriate, updated the strategic objectives of the organisation. The current plan allows ASIO to focus on critical priorities while responding with agility and resilience to emerging challenges in both the security and fiscal environments.

Human resource management

ASIO continues to operate in a challenging fiscal environment and has adapted its recruitment approach to maintain organisational capability while deferring the optimal growth target for ASIO of 1860 as identified by Mr Allan Taylor AM in his 2005 Review of ASIO Resourcing.

During the reporting period ASIO reduced its Senior Executive Service staffing levels by 15 through a voluntary redundancy program. Outside the reporting period ASIO also issued voluntary redundancies to 34 staff at the AEO1, AEO2 and AEO3 levels.

Two Intelligence Development Programs were completed over the reporting period, with 35 intelligence professionals graduating and commencing their first posting.

In early 2013 ASIO developed and implemented a new Management and Leadership in Security Intelligence strategy aimed at officers at the AO5 to Senior Executive Service Band 2 level with a renewed focus on building and reinforcing fundamental management skills.

Accommodation

The Ben Chifley Building was opened on 23 July 2013. At the time the decision was made, completion was expected to occur in August 2013 and the opening was timed to enable greater access, including by media, to the Ben Chifley Building prior to staff and technical equipment occupying the building.

Delays in the commissioning and testing of essential building systems in the Ben Chifley Building have led to further slippages in the dates of handover.

Legislation

In the absence of modernisation of the telecommunications interception and access regime, ASIO faces the prospect of progressively losing access to critical intelligence, putting at risk ASIO's ability to identify threats to security. To this end, ASIO provided submissions and attended hearings to assist the PJCIS consideration of these issues. ASIO has also provided a submission to the Legal and Constitutional Affairs References Committee inquiry into the comprehensive review of the *Telecommunications (Interception and Access) Act 1979* which was initiated outside the reporting period.

Litigation

ASIO continues to direct substantial resources to managing its involvement in litigation. This is expected to continue due to the continued upward trend in merits and judicial review of adverse security assessments, notably in relation to migration and Australian passport related security assessments, and the recent surge in criminal prosecutions that require ASIO's intelligence as evidence.

Security of ASIO

A strong security culture underpins ASIO's ability to carry out its mission to protect Australia, its people and its interests. This requires robust security policies, practices and technologies. These standards serve to protect the Organisation's people, premises and information from compromise and ensure ASIO can carry out its mission.

Relationships

At the end of the reporting period the Attorney-General had authorised ASIO to liaise with 347 authorities in 131 countries, an increase on last year of seven authorities and six countries.

Accountability

The stringent oversight and accountability mechanisms for ASIO's work continued at a high tempo over the reporting period.

The Inspector-General of Intelligence and Security maintained regular inspections of key elements of ASIO's work, while also undertaking a number of formal Inquiries.

During the reporting period the Hon. Margaret Stone commenced as the Independent Reviewer of Adverse Security Assessments. As at 30 January 2014 the Independent Reviewer had released her findings in relation to 15 individuals. In 12 cases the Independent Reviewer found the adverse security assessment was an appropriate outcome. In three cases the Independent Reviewer found the adverse security assessments were not appropriate. ASIO undertook new assessments in relation to these individuals, resulting in the Director-General issuing two non-prejudicial security assessments and one qualified assessment in relation to the individuals.

ASIO's role and functions

ASIO is Australia's security service. Its role and responsibilities are precisely defined by the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). ASIO's primary function is to collect, analyse, assess and disseminate security intelligence, and provide security advice. Security intelligence is concerned with a specific set of activities that might harm Australia, Australians or Australian interests (including overseas). Those activities are:

- espionage;
- sabotage;
- politically motivated violence (including terrorism);
- 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 (in Australia and overseas). 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[1];
- 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 of people to Commonwealth agencies to inform decision making in relation to prescribed administrative action, including visas and Australian passports.

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 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 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.

Under the ASIO Act, ASIO is responsible to the government through the Attorney-General. ASIO is also required to comply with the Attorney-General Guidelines, which outline how ASIO must conduct its operations. The guidelines stipulate that ASIO's information collection activities should be conducted in a lawful, timely and efficient manner, using the least intrusion necessary into an individual's privacy and proportionate to the gravity of the threat being investigated.

The Inspector-General of Intelligence and Security, an independent statutory authority, also plays an important role in overseeing ASIO's activities.

1 The Attorney-General's Guidelines can be found online at www.asio.gov.au\img\files\AttorneyGeneralsGuidelines.pdf

The security environment 2012–13 and outlook

Espionage and foreign interference

Espionage and foreign interference targeting Australian interests remains a serious and sustained threat. ASIO continued to work with its partners in government and industry to deliver ASIO's mission to discover, defend against and degrade these activities, and to provide a holistic protective security response.

The scale and sophistication of state-sponsored cyber attacks against Australian Government and private sector systems have increased considerably in recent times. ASIO continues to work with its national security partners to raise awareness in the private and public sectors of the very real threat posed by cyber espionage, and to harden defensive responses—both at the technical and human level.

Individuals who exploit their legitimate access to national systems and environments to publicly disclose classified and sensitive information are a constant source of potential harm to Australia's national interest. These individuals betray the countries they were employed to protect. The public release of national security classified material could cause significant damage to Australia's security and the safety of its people. Whatever the motives of individual actors, unauthorised disclosures of sensitive information—publicly or clandestinely—to foreign intelligence services can damage national security by revealing sources, capabilities, material and methodologies. This can put the safety of sources and intelligence officers at risk, and make more difficult the identification and prevention of activities of security concern.

The threat to Australia posed by espionage and foreign interference activities will remain of substantial concern into the future, particularly given the increasingly technologically interconnected environment in which we live.

Politically motivated violence

Politically motivated violence, particularly terrorism, is constantly evolving and remains a significant threat to Australia and Australians, accounting for about 70 per cent of ASIO operational effort.

Hang Dinh/Shutterstock.com

Some overseas attacks in 2013—such as those in Boston and London—utilised basic capabilities and simple technologies, demonstrating that an attack need not be complex to achieve the aims of the perpetrators. However, the increasing prevalence of lone actor attacks does not supplant the ongoing threat from more organised and directed extremists, who continue to aspire to conduct large-scale, mass-casualty attacks against the West.

The Syrian conflict poses its own challenges for ASIO in combating the threat of terrorism to Australia. ASIO is currently investigating between 120 and 150 people in Australia and offshore who are directly involved with extremist groups and activities in Syria. Hundreds of Australians have travelled to the region to participate in various aspects of the conflict—from providing humanitarian aid to having direct involvement, including fighting, with terrorist groups.

There are four primary security concerns arising from the current Australian involvement with Syria-based extremist groups:

1. Australia-based extremists who have been prevented from travelling to Syria may seek to undertake acts of politically motivated violence in Australia.
2. Australians in Syria are likely to adopt, or reinforce their commitment to, violent jihadist views and this may translate to planning for a terrorist attack in Australia on return.
3. Australians in Syria will acquire new terrorist capabilities and develop extremist networks and many will have returned having experienced involvement in violence.

4. Returned extremists might increase the potential for increased sectarian violence between Sunni and Shia communities in Australia.

ASIO will continue to prioritise those individuals it considers to be the most significant threats to national security and distribute its resources accordingly.

We expect these challenges to play out over several years and have a medium- to long-term influence on the extremist environment in Australia, beyond any immediate resolution to the Syrian conflict—which is unlikely.

Communal violence and violent protest

Section 17A of the ASIO Act enshrines an individual's right to lawful protest, advocacy or dissent. ASIO investigates protest activity only when it includes, or has the potential to include, planned violent activity or where it has the potential to impinge on the security of certain designated persons or places. However, ASIO may prepare threat assessments in relation to demonstration or protest activity on the basis of existing information. ASIO's threat assessment advice is integral to national arrangements for the protection of high office holders, internationally protected persons, sites of national significance and critical infrastructure.

A by-product of the Syrian conflict has been sporadic instances of small-scale communal violence in Australia during the last year by both pro- and anti-Syrian Government supporters. ASIO expects communal tensions as a result of the Syrian conflict to continue, and small-scale acts of communal violence may result.

The 15 September 2012 protest against the film *Innocence of Muslims* turned violent when several members of the wider protest group clashed with police. Condemnation of violence from local Islamic community leaders and the general public, as well as the subsequent police response, combined to prevent further violent protest activity or retaliatory action.

Protest activity by issue motivated groups—whose focus can range from environmental causes, anti-capitalism and animal rights through to indigenous affairs, industrial relations and local community issues—are generally not of security concern. Although there has been relatively little violent protest activity in Australia in recent years, the threat remains greatest from extreme left-wing groups, particularly anarchists. Instances of anarchist violence have increased internationally since the global financial crisis.

Australian anarchists maintain links with overseas groups, including overseas anarchist collectives, and are influenced by these groups. Some Australian anarchist groups consider violence against authorities and destructive actions against infrastructure, including government and business targets, to be legitimate protest activity.

Border security

ASIO continues to contribute to the whole-of-government effort to counter serious threats to Australia's border and territorial integrity. This contribution includes identifying and investigating Australians and Australia-based people involved in maritime people smuggling, and providing advice to government, such as security assessments of people seeking a visa to enter Australia.

ASIO continued to conduct security assessments on individuals who apply for Australian visas, whether they did so inside or outside Australia.

Outlook for the security environment

The security challenges Australia is facing are the most diverse in a generation—the most potentially damaging stemming from terrorism, espionage and foreign interference.

Espionage and foreign interference

The source and type of espionage and foreign interference is becoming more varied and the impact more diverse.

The threat posed by trusted insiders is expected to continue well into the future, as is the harm of past unauthorised disclosures. The portrayal of individuals disclosing classified material without authorisation as 'whistleblowers' by much of the media does not recognise the underlying motivations of the individuals.

Espionage and foreign interference challenges are set to persist into the future. Traditional forms of espionage are being increasingly supplemented by cyber espionage. Given our increasingly globalised and technologically interconnected society, cyber threats are likely to continue to increase in volume and sophistication.

Politically motivated violence

The threat to Australia from terrorism will continue to emanate from various, occasionally overlapping, sources. New lone actors will continue to emerge, often having accessed extremist material online including instructions on how to conduct an attack. The security challenges stemming from the Syrian conflict will also continue into the future. These challenges are set to increase into the future as a result of the increased volume of individuals involved in the Syrian conflict and their eventual return to Australia.

ASIO investigations suggest that Australians who previously travelled overseas and who were exposed to violence and extremist ideologies represented an increased threat when they returned here. ASIO is aware of 30 individuals who traveled to extremist training camps in Afghanistan and Pakistan in the 1990s and 2000s. Of these, 19 were involved in activities of security concern after their return to Australia, with eight being convicted of terrorism offenses in Australia. While the conflicts are not directly comparable, these statistics explain ASIO's concern with the scale of Australian involvement in the Syrian conflict.

Events

ASIO's resourcing will also be required to prepare for and respond to a variety of expected and unexpected events. Depending on the nature of the event, it may require ASIO to divert resources away from addressing the thematic challenges outlined above. ASIO provides advice to government in anticipation of visits to Australia by foreign dignitaries, which can often occur with short notice, as well as events that are organised months, or even years, beforehand.

ASIO anticipates the Group of Twenty (G20) meetings in 2014, particularly the Heads of Government meeting in December, will attract protest activity due to the nature of the meetings, the high profile of the attendees and the considerable international media coverage. While most protest activity is expected to be peaceful, ASIO remains cognisant of the potential for extreme groups, such as anarchists, to use the cover of mainstream protests to undertake and incite violence.

Given their status and audience, a number of major sporting events occurring in the next 12 months, including the Sochi Winter Olympics, the FIFA World Cup in Brazil and the Commonwealth Games in Scotland, are potential targets for violence and extremist activities. Due to the Australian association with these events ASIO will provide advice to government to help ensure the security of participants, officials and spectators.

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 2012–13 ASIO's operating result was a $1.5 million surplus. Revenue from government for 2012–13 was $329.7 million, up slightly from $328.1 million in 2011–12.

ASIO was approved to operate at a loss of $13 million for 2012–13 for costs associated with the move to the Ben Chifley Building. Due to the delay in the move, ASIO is seeking to defer this loss to the 2014–15 financial year.

ASIO has continued to absorb a range of additional costs, including border security investigations, increased number of visa security assessments, greater costs of telecommunications interception and increased litigation activity—most recently related to an increase in security assessment litigation where, to date, all of ASIO's decisions have been upheld. In the reporting period ASIO has made changes to adapt to the fiscal environment without adverse effects on ASIO's core operations, including by reducing:

- ASIO's overseas presence;
- ASIO's foreign engagement for training purposes;
- The amount of domestic and overseas travel undertaken by ASIO officers; and
- The number of Senior Executive Service (SES) officers through a voluntary redundancy program. During the reporting period, ASIO reduced its SES staffing level by 15, equating to 25 per cent of total SES staff.
    - Outside the reporting period, ASIO also issued voluntary redundancies to 34 staff at the AEO1, AEO2 and AEO3 levels.

ASIO's restructure in January 2013 and the introduction of the range of efficiency measures detailed above have ensured an appropriate level of operational activity and longer term capability will be maintained with a smaller staffing level than originally anticipated and in a tighter fiscal environment.

While ASIO has been able to adapt to the constrained fiscal environment to date without substantial diminution of its core operations, it will be increasingly difficult to do so in the future without having adverse operational effects.

Financial performance

ASIO recorded an operating deficit of $45.1 million in 2012–13 due to the net cash funding arrangements. Excluding depreciation, ASIO achieved an operating surplus of $1.5 million.

Figure 1 Revenue from government for years from 2007–08 to 2012–13

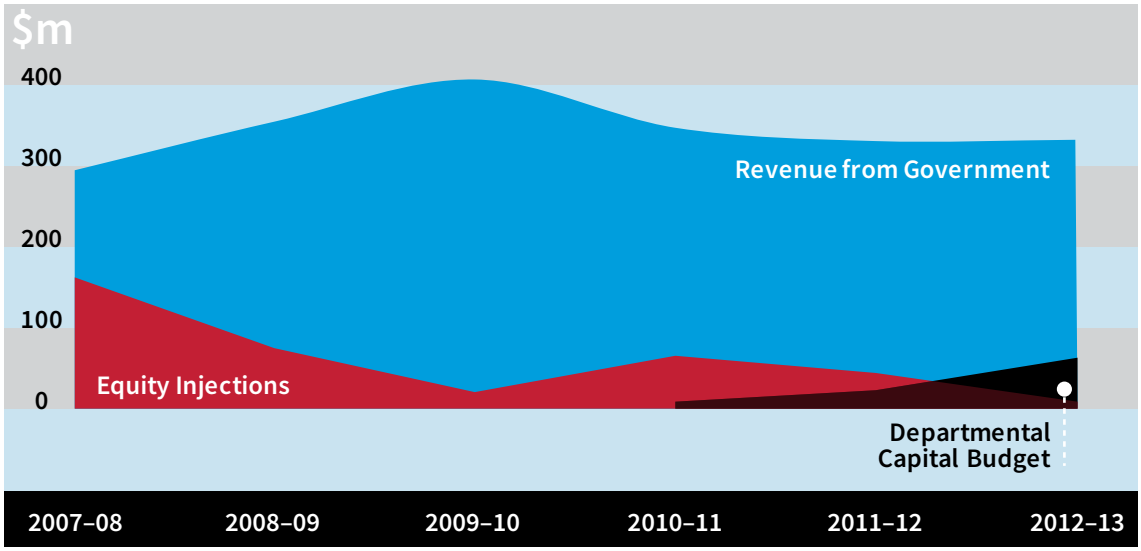
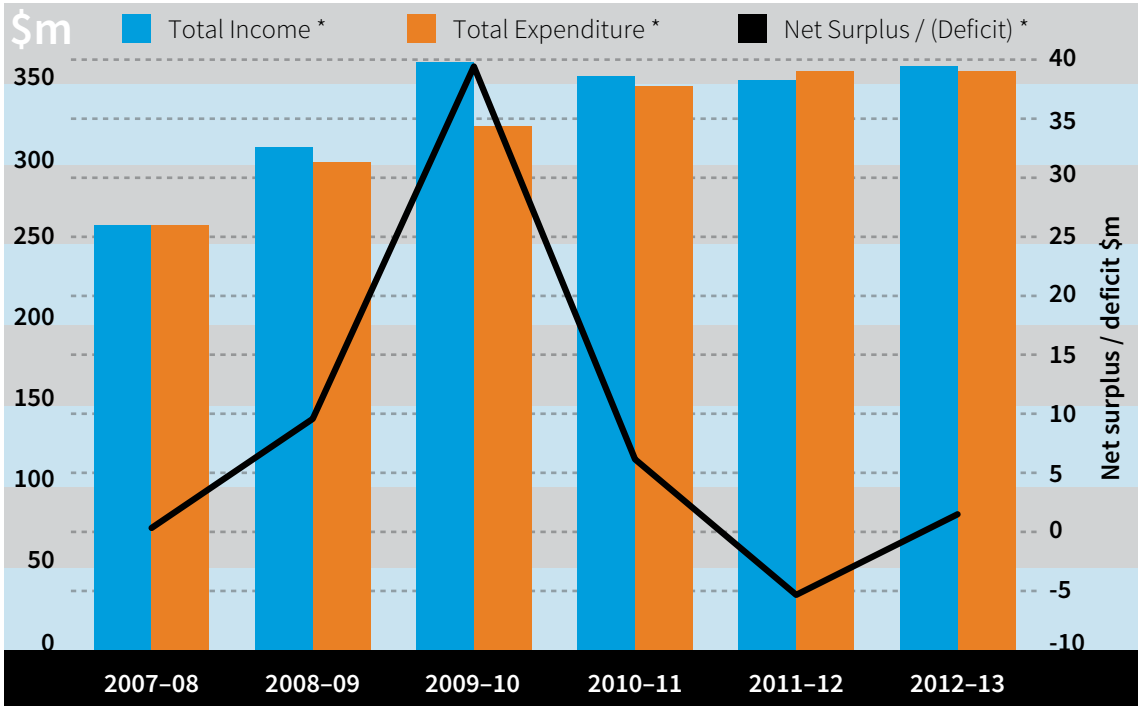


Figure 2 Financial performance for years from 2007–08 to 2012–13



Strategic allocation of resources

ASIO's Executive Board sets the Organisation's strategic direction which is reflected in the allocation of resources across ASIO's activities. The Finance Committee reports regularly to the ASIO Executive Board to ensure the Organisation's budget and resource allocation are aligned with organisational priorities.

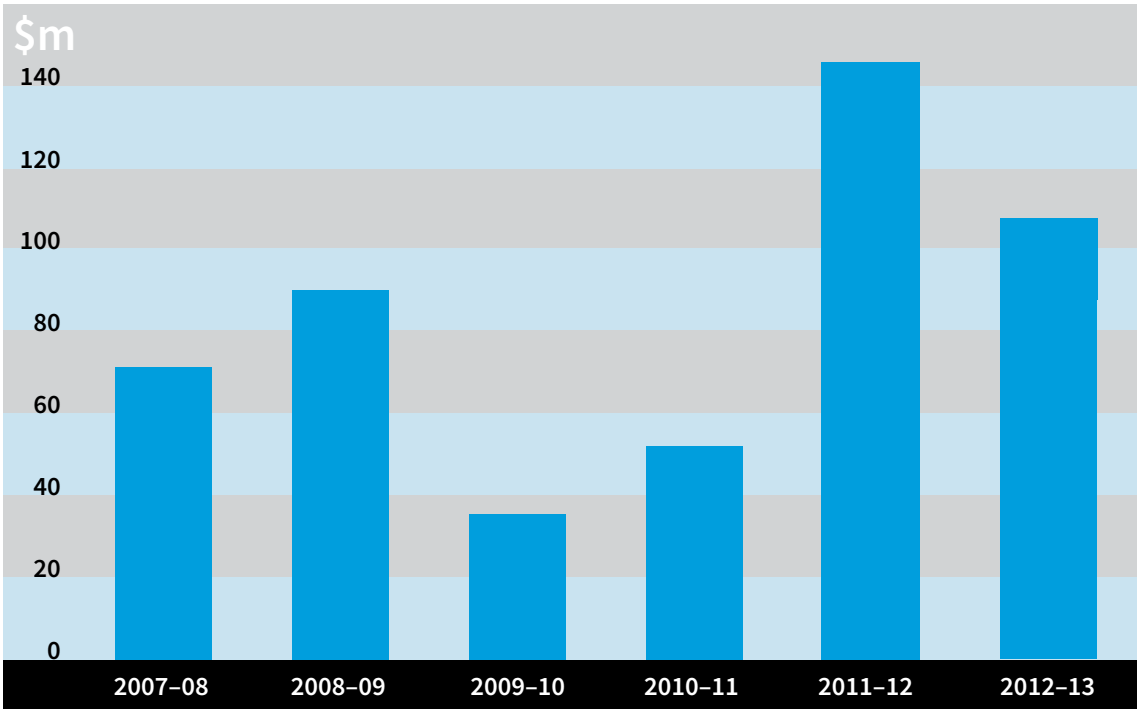
New Policy Proposals are submitted through the relevant ASIO committee to the Finance Committee to agree on funding strategies before being put to the ASIO Executive Board for endorsement.

In 2012–13 ASIO continued its focus on maintaining and enhancing capabilities across the collection, operational and technical fields. Rapid technological advances continue to present challenges to ASIO maintaining its capabilities and in the absence of legislative reform and continued investment,

ASIO faces the prospect of the ongoing decline in our ability to intercept communications. From ASIO's perspective, the proposed legislative reforms considered by the PJCIS are vital in arresting the decline in this capability which is of central importance to our ability to identify threats to security.

The high level of expenditure on capital items in 2012–13 was due to the costs associated with the Ben Chifley Building.

Figure 3 Purchase of capital items for year from 2007–08 to 2012–13



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* 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. In 2012–13 ASIO did not receive 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. ASIO's Audit and Risk Committee also receives quarterly briefings from the Chief Finance Officer, in support of the committee's role to provide independent assurance and advice on design, operation and performance of ASIO's internal governance, risk and control framework.

In addition to audits conducted by the ANAO and internal system controls, ASIO's internal audit section also undertakes financial audits.

Structure of the Organisation

Organisational structure

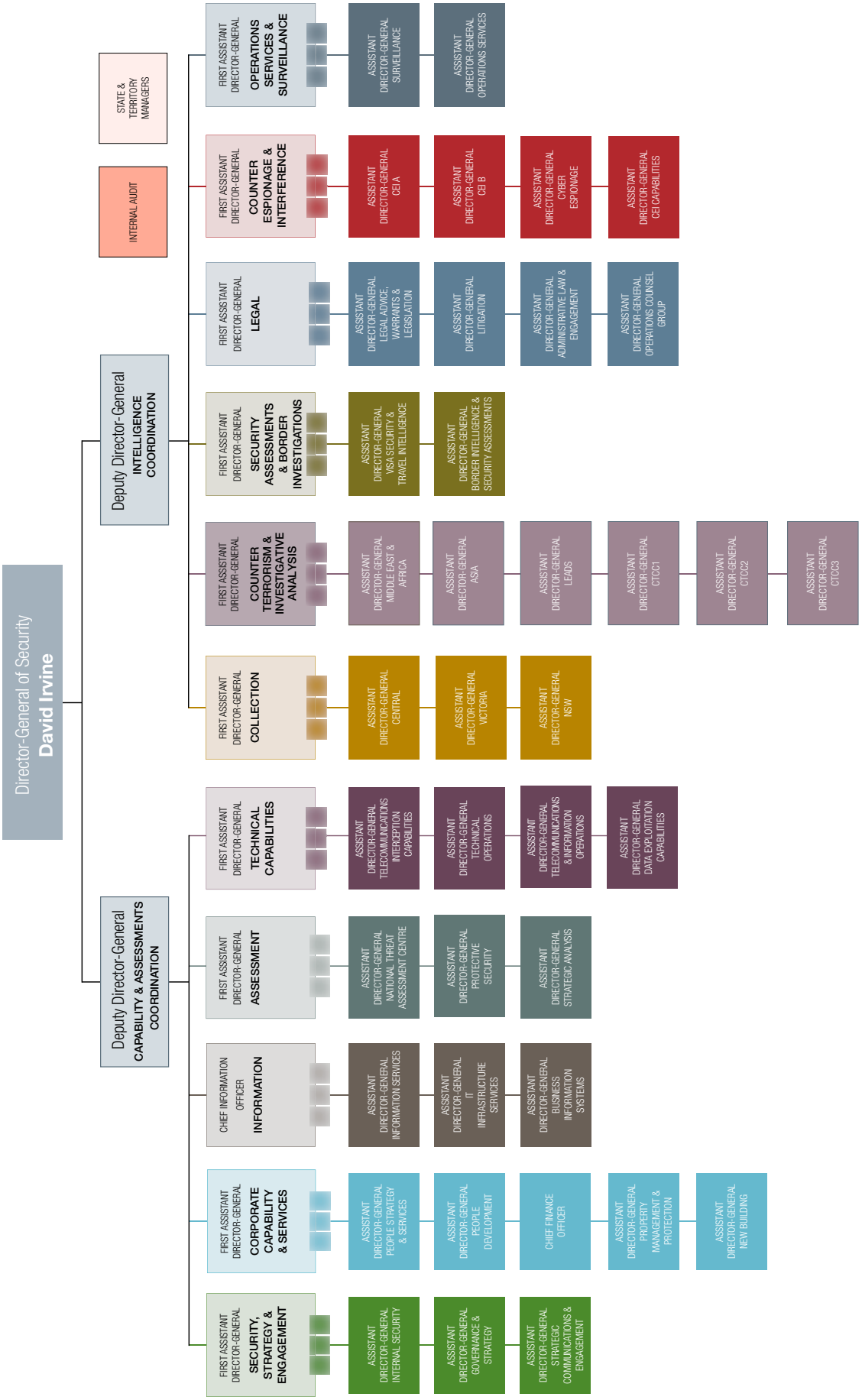
In 2012–13 ASIO continued to consolidate and refine its organisational structure in response to a continually tightening fiscal environment. In the last reporting period the Director-General ordered a review of ASIO's organisational structure to ensure ASIO continued to operate in the most effective and efficient way possible. On 17 January 2013 ASIO adopted a new organisational structure which reduced the number of divisions from 11 to eight. ASIO reduced its number of SES officers by 15 (representing 25 per cent) through a voluntary redundancy program.

The revised organisational structure is designed to:

- Align like functions;
- Reinforce the ASIO mission and the way each Division contributes to the mission; and
- Maximise the impact of outreach through consolidated Divisional engagement.

ASIO's organisational structure as at 30 June 2013

ASIO's organisational structure as at 30 June 2012



Corporate direction and strategic planning

ASIO strategic planning

The reporting period saw the conclusion of ASIO's *Strategic Plan 2011–13.* In review of the plan, it was recognised that many of ASIO's broad strategic objectives remained. This is reflected in ASIO's new *Strategic Plan 2013–16* which has adopted and, where appropriate, updated the strategic objectives of the organisation. The current plan allows ASIO to focus on critical priorities while responding with agility and resilience to emerging challenges in both the security and fiscal environments. The four goals of the new strategic plan are:

- deliver high-quality security intelligence collection, analysis, assessment and advice in support of ASIO's mission;
- continue to enhance ASIO's strategic impact and reputation;
- evaluate, evolve and strengthen ASIO's capabilities and business practices; and
- attract, develop and retain a professional and highly competent workforce.

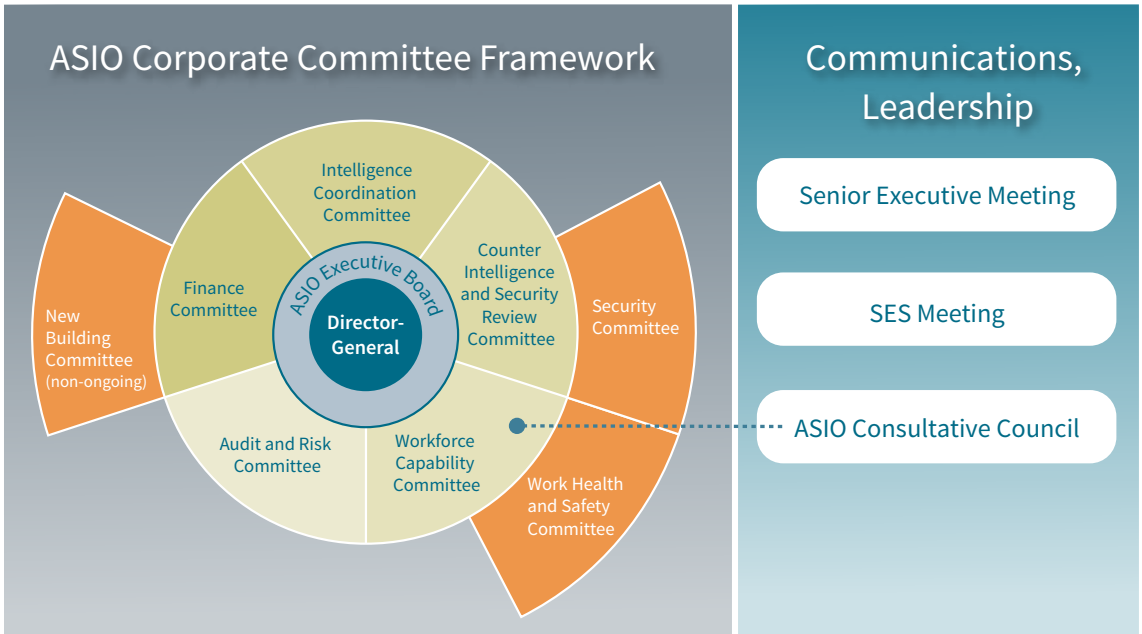
The plan will be the basis for subordinate business plans, including performance and development agreements, so that everyone in ASIO understands how they contribute to ASIO's mission and the government's national security strategy.

Corporate governance

During the reporting period ASIO continued to modify its corporate governance structures to ensure they continue to act as the best forums for providing strategic advice to the Director-General on the Organisation's corporate and operational activities. The creation of a new Counter Intelligence and Security Review Committee demonstrates the continued emphasis ASIO places on effective security policy and practices.

ASIO Executive Board

The ASIO Executive Board is the primary advisory committee supporting Director-General in the governance of the Organisation. Its monthly meetings set ASIO's strategic direction and manage organisational resources. The Executive Board is attended by the Director-General, the Deputy Directors-General and an external member.



Supporting committees

The ASIO Executive Board is supported by a range of committees, each focusing on a separate aspect of ASIO's work. These committees provide advice to inform decision-making by the Executive Board and the Director-General on matters including the Organisation's financial health, strategic capability planning, work health and safety issues, enterprise risks and mitigation strategies, and intelligence priorities.

Intelligence Coordination Committee

The Intelligence Coordination Committee provides strategic direction for ASIO's operational activities, allocates resources according to investigative and assessment priorities and regularly reviews performance against benchmarks.

Workforce Capability Committee

The Workforce Capability Committee advises the ASIO Executive Board on matters relevant to maintaining the capacity and capability of ASIO's workforce necessary for the Organisation to meet its current and future needs.

Work Health and Safety Committee

The Work Health and Safety Committee builds cooperation between management and staff in formulating, implementing and reviewing health and safety policies, procedures and initiatives. It works to promote an anticipatory and proactive approach to work health and safety, and foster a positive work health and safety culture.

Counter Intelligence and Security Review Committee

The Counter Intelligence and Security Review Committee provides guidance and direction in respect of security policy for ASIO and sets counter-intelligence and security priorities. It also approves security policy and procedure documentation, and reviews the compliance of ASIO in meeting legislative and policy responsibilities specific to Australian Government mandatory standards.

ASIO Security Committee

The ASIO Security Committee reviews and addresses ASIO's security culture, framework and processes and ensures security risk management best practice is applied to ASIO people, property and information technology systems. It is also responsible for the development and integration of the government and ASIO's security policies and ensures Organisational accordance with legislative and policy responsibilities regarding protective security.

Finance Committee

ASIO's Finance Committee provides advice and makes recommendations to the ASIO Executive Board on resource allocation, and financial management and strategy.

New Building Committee

The New Building Committee provides strategic guidance on the progress of the new building project, ensuring the building will meet ASIO's needs. The committee is also responsible for preparing and implementing a smooth and secure transition to the Ben Chifley Building.

Audit and Risk Committee

The Audit and Risk Committee provides independent advice to the Director-General on ASIO's risk, fraud control and compliance framework and its financial statement responsibilities. To ensure the committee is able to conduct its activities effectively, it is provided with wide authority to access information relevant to its role and responsibilities. The committee has an independent chair appointed by the Director-General and an external committee member.

Communications and leadership meetings

Senior Executive Meeting

The Senior Executive Meeting is a weekly meeting attended by officers at the SES Band 2 level and above to discuss emerging issues. It is chaired by the Director-General.

Senior Executive Service Meeting

The monthly Senior Executive Service Meeting provides a forum for officers at the SES Band 1 level and above to discuss key strategic issues affecting ASIO and ensure messages are communicated.

ASIO Consultative Council

The ASIO Consultative Council was established to enable management and staff of the Organisation to meet regularly in a structured way to discuss and resolve issues of interest and concern.

Audit and evaluation

In 2012–13 ASIO consolidated changes made to its risk governance structure to further foster and entrench a positive risk culture. The independent chair of the Audit and Risk Committee has been in place for over 12 months and has guided the committee in embedding change and identifying opportunities for continuous improvement.

ASIO's internal audit area completed a range of tasks to improve organisational performance, including:

- undertaking compliance audits to ensure conformity to privacy requirements and agreements with external partners;
- completing professional training to maintain and develop their professional qualifications and promote best audit practice; and
- completing fieldwork into operational expenditure across ASIO to assist the Australian National Audit Office in conducting its financial statements audit.

These activities value-added to business areas, identified potential business improvements and validated compliance with relevant legislation and established practices and processes.

Assumed identities and commercial cover are used to protect ASIO officers' identities and prevent the potential compromise of ASIO operational activities. Under Part IAC of the *Commonwealth Crimes Act 1914*, ASIO is required to maintain appropriate records about its use of assumed identities and commercial cover, and audit these records every six months.

The small number of authorities maintained under the *New South Wales Law Enforcement and National Security (Assumed Identities) Act 2010* are also audited six monthly while active.

Audits undertaken in respect of assumed identities did not identify any fraud or unlawful activity.

Fraud control

During the reporting period ASIO refreshed its fraud risk assessment. This assessment identified a series of fraud risks that were found to be appropriately mitigated by controls in the ASIO security and financial frameworks. ASIO also drafted and, in June 2013, implemented the *ASIO Fraud Control Plan 2013–15*, which outlines the Organisation's strategies to control and manage fraud.

In the reporting period ASIO received four allegations of fraud, all of which were investigated with no fraud activities identified.

Human resource management

Recruitment

ASIO continues to operate in a challenging fiscal environment and has adapted its recruitment approach to maintain organisational capability while deferring the optimal growth target for ASIO of 1860 as identified by Mr Allan Taylor AM in his 2005 Review of ASIO Resourcing.

In 2012–13 ASIO focused on recruiting intelligence professionals, technical officers and security assessors. ASIO also strengthened its strategies to attract and develop entry-level staff and existing staff across the breadth of ASIO's activities.

Training and development

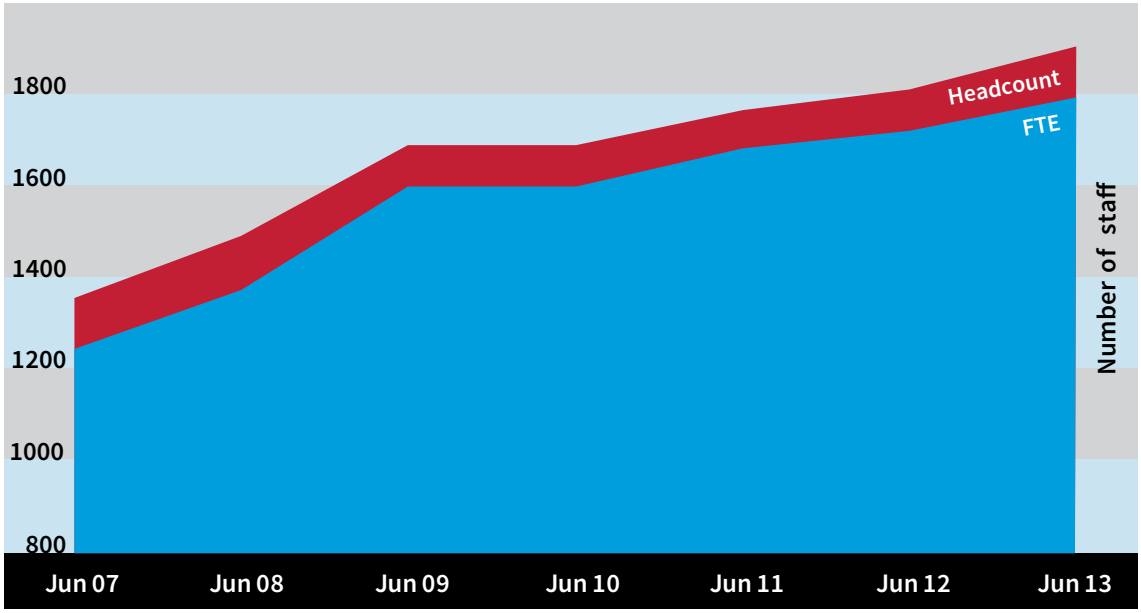
Intelligence training

In 2012–13 ASIO's Intelligence Development Program (IDP) continued to provide new recruits with the fundamental skills and knowledge in analytical and operational disciplines. The IDP is an intensive training program consisting of foundational training, core skills, competency assessments and work placements.

Two IDPs were completed over the reporting period, with 35 intelligence professionals graduating and commencing their first posting.

An important feature of ASIO's intelligence training is the provision of specific training modules to officers who identify a need in order to perform aspects of their role. ASIO provided an additional 51 instances of analytical and operational training to these officers of between five days and three weeks duration.

Figure 4 Staffing growth for years from 2007–08 to 2012–13



Corporate training

ASIO delivers corporate training programs at various stages of an officer's employment. These programs can be specific to an officer's role or Organisation-wide mandatory training to ensure minimum standards of behaviour. Corporate training activities include:

- an induction program for all new starters to explain ASIO's role and functions, the nature of the security environment and the standard of behaviour expected of ASIO officers;
- administrative training including contract management, procurement, finance and communication;
- information technology training, including training on ASIO's various systems and databases;
- mandatory training, including security awareness, ethics and accountability, environmental management, work health and safety, and workplace behaviour, to ensure all ASIO officers behave in accordance with the key principles and standards within the Australian Public Service and ASIO; and
- discipline-specific courses including social, cultural, political and religious history and influences.

Management and leadership skills

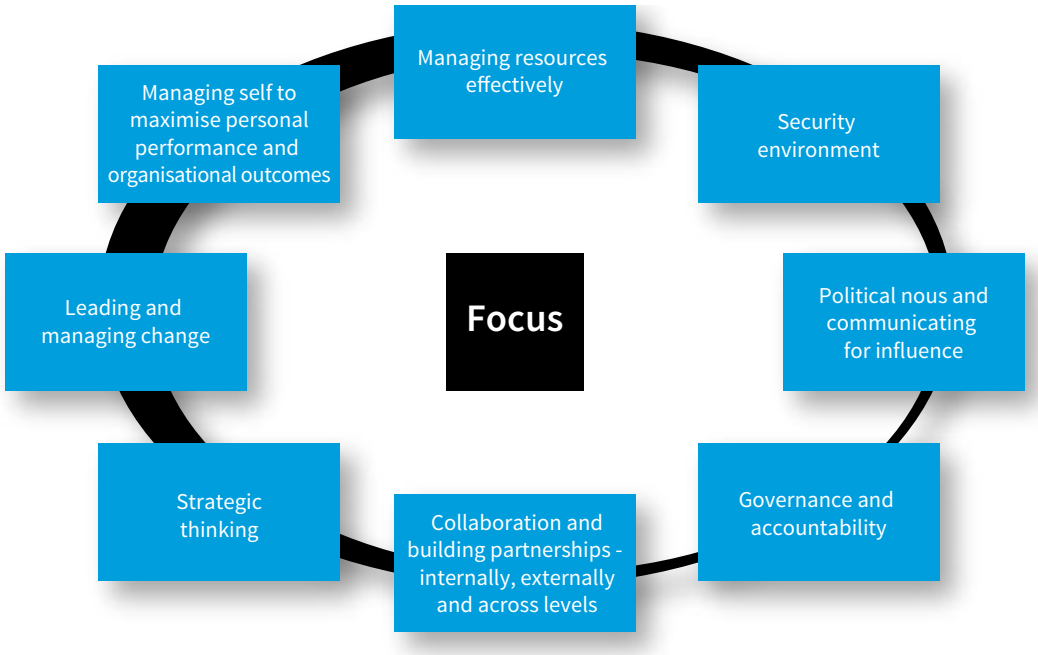
ASIO's Leading Edge leadership program, which concluded during the reporting period, enhanced the leadership and management skills of ASIO's executive work force, with over 95 per cent of participants reporting it would improve the way they worked.

In early 2013 ASIO developed and implemented a new Management and Leadership in Security Intelligence strategy aimed at officers at the AO5 to SES Band 2 level with a renewed focus on building and reinforcing fundamental management skills. This 'back to basics' strategy will better prepare ASIO for future challenges by ensuring managers and leaders are proactive and adaptable in:

- addressing the rapidly evolving security environment;
- meeting the expectations of government and the public;
- developing and meeting strategic goals;
- dealing with operational, investigative and workplace issues; and
- sharing knowledge and information appropriately.

The strategy places value and emphasis on developing management and leadership skills, operational and investigative excellence, intellectual rigour and positioning ASIO for the future, as shown in the diagram below.

Figure 5 Management and Leadership in Security Intelligence strategy



The management and leadership framework supports a learning culture where learning occurs every day and not solely at formal training events. This approach allows concentration on business results and uses learning as a means to achieve the required results, rather than an approach where knowledge and learning are seen as the end result.

Language training

Maintaining and improving ASIO's language capabilities is crucial to its ability to conduct effective counter-terrorism, counter-espionage and foreign intelligence operations.

In addition to its linguist capability, ASIO also utilises the language skills of its officers working in other disciplines. To this end, ASIO's Language Skills Development Program provides support to officers interested in enhancing their language skills in operationally relevant languages. In the reporting period the program provided support to 26 officers across a range of languages.

E-learning

ASIO's suite of e-learning modules provides an efficient and effective way to deliver training to ASIO officers across a range of disciplines, including work health and safety, workplace behaviour, ethics and other mandatory training requirements. ASIO's e-learning modules continue to be updated as required to ensure currency and maintain best practice.

Three e-learning modules on reporting standards, and several modules for new and existing information technology systems, were implemented to assist in achieving organisational outcomes.

Studies assistance

ASIO offers a study assistance program to support officers in their endeavours to undertake further professional development in disciplines relevant to their roles in ASIO and broader government. During the reporting period 145 officers participated in ASIO's Study Support Program in fields of study including business management, policy, project management and information technology.

National Intelligence Community training

ASIO considers shared training opportunities within the National Intelligence Community to be a valuable way to improve understanding of and cooperation between National Intelligence Community (NIC) agencies. During the reporting period, ASIO continued to actively contribute to NIC training as a presenter and a participant.

ASIO makes available places for other agencies to participate in ASIO training courses and holds the ASIO Partnership Forum to provide a greater understanding of ASIO's work to individuals within the NIC (and more broadly) who work on a regular or semi-regular basis with ASIO.

ASIO also enables officers to participate in courses offered by the National Security College to develop a deeper understanding of national security challenges and provide an opportunity for further executive and professional development.

Performance management

ASIO's performance management framework—Enhancing Performance—aims to create a performance culture where the Organisation builds and develops capability to achieve our strategic and operational objectives to protect Australia, its people and its interests.

ASIO's Executive Directions set the direction for the year ahead in building ASIO's performance culture. The two broad types of behaviour ASIO aimed to recognise in 2012–13 were:

- Operational achievements, including effectively handling operational issues, producing high impact assessments or advice and contributing significantly to national security policy development.
- Good corporate citizenship, including exhibiting leadership, initiative, collaboration and contribution to the ethos of the Organisation.

Attachments

During the reporting period ASIO remained committed to its outreach with regard to secondments, with placements to and/or from the following government agencies:

- the Attorney-General's Department;
- the Australian Federal Police;
- the Australian Secret Intelligence Service;
- the Australian Geospatial-Intelligence Organisation (also known as the Defence Imagery and Geospatial Organisation);
- the Australian Signals Directorate (also known as the Defence Signals Directorate);
- the Defence Intelligence Organisation;
- the Department of Foreign Affairs and Trade;
- the Department of Immigration and Citizenship;
- the Office of Transport Security, within the Department of Infrastructure and Transport;
- the Office of National Assessments;
- the Department of the Prime Minister and Cabinet;
- the Department of Human Services;
- the Department of the Treasury;
- the New South Wales Police Force;
- the Queensland Police Service;
- Victoria Police; and
- Western Australia Police.

In determining potential secondments, ASIO identifies opportunities to mutually enhance strategic and operational outcomes.

Staffing ratios

Ratio of Senior Executive to middle and lower level staff

At 30 June 2013 there were 45 SES officers, 517 ASIO Executive Officers and 1342 other ASIO officers.

Figure 6 Ratio of SES to middle and lower level staff

Workplace diversity

ASIO recognises that positive outcomes are achieved by a workplace with a diverse range of skills, cultural perspectives and backgrounds. This is especially true in the security intelligence arena where understanding the intricacies of various cultures, societies and religions is crucial to understanding and addressing the broader security environment.

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

Table 1 Workplace diversity of ASIO staff

Group	Total Staff [1]	Women	Non-English Speaking Background	Aboriginal and Torres Strait Islander	People with a Disability	Available EEO Data [2]
Senior Executive Service (excl DG)	45	11	0	0	1	43
Senior Officers [3]	517	185	19	2	9	476
AO5 [4]	641	331	48	3	7	580
AO1 – 4 [5]	591	292	29	3	3	557
Information Technology Officers Grades 1 and 2	102	15	6	0	3	97
Engineers Grades 1 and 2	8	0	0	0	0	8
Total	**1904**	**834**	**102**	**8**	**23**	**1761**

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

[2] Provision of Equal Employment Opportunity (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 translates to APS Level 6.

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

Figure 7 Age of staff for years from 2007–08 to 2012–13

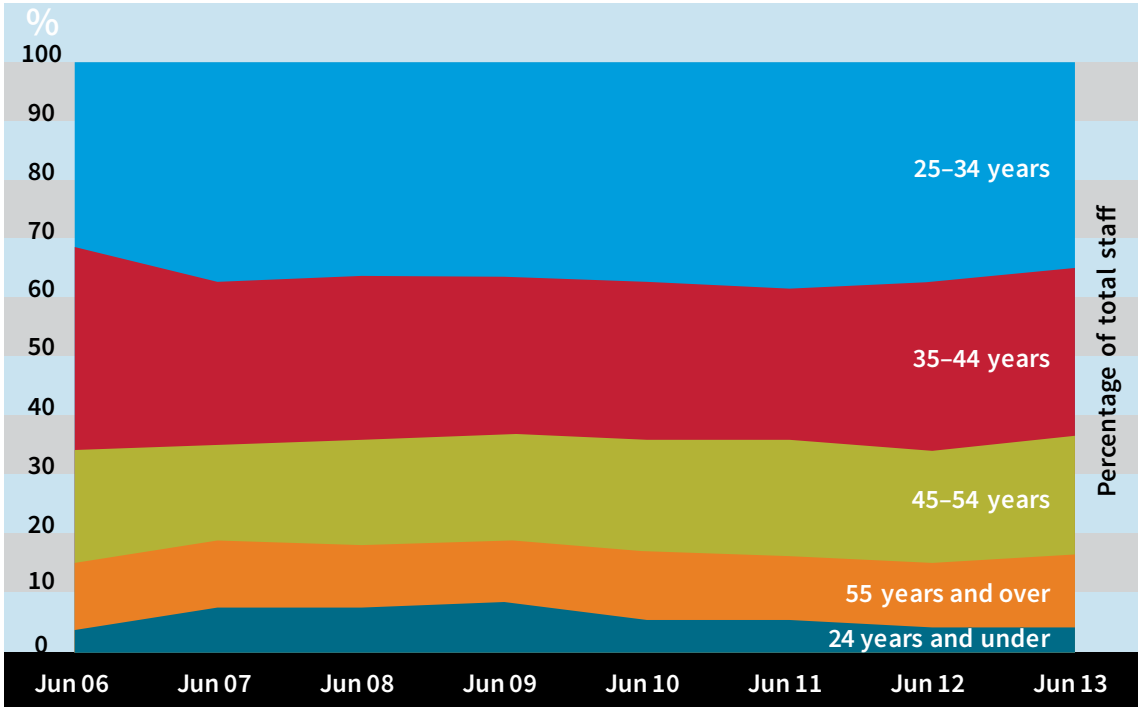


Figure 8 Length of service of ASIO staff for 2012–13

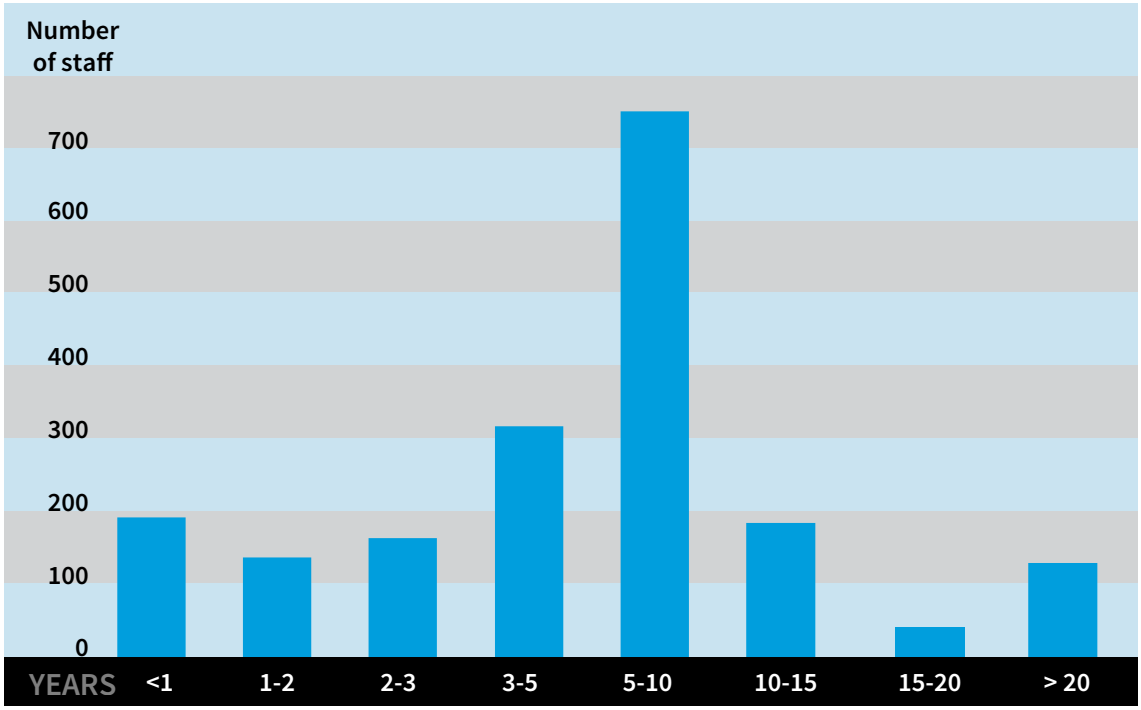
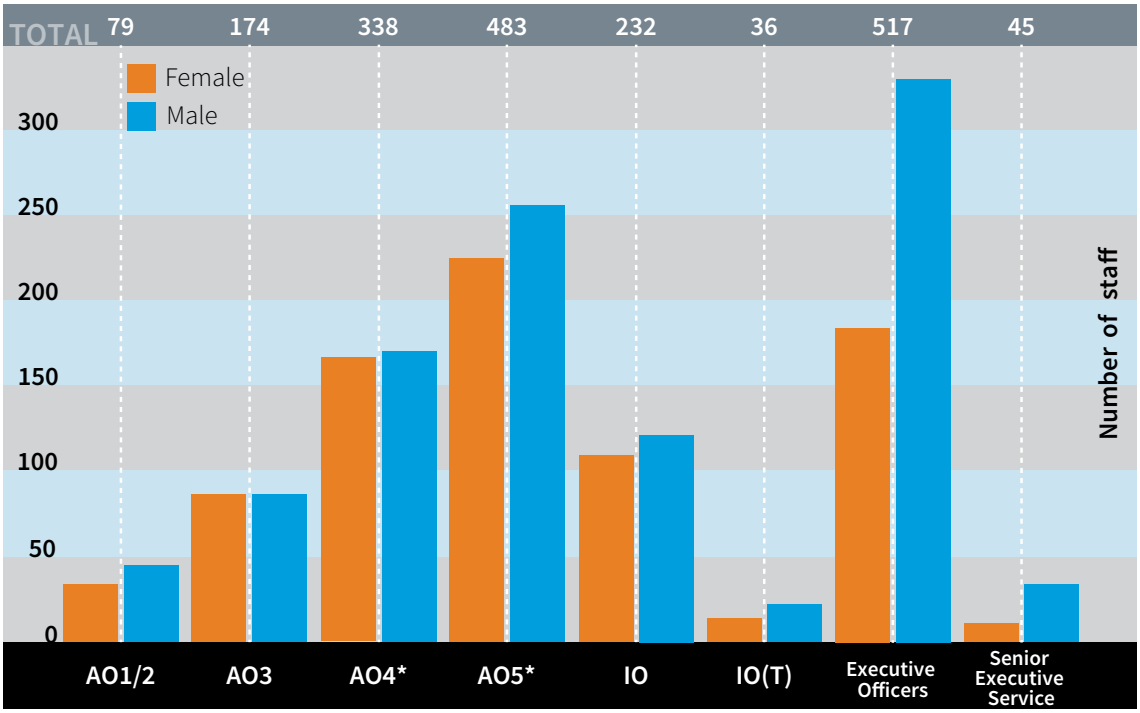


Figure 9 Gender balance by classification for 2012–13



Staff complaints

During the reporting period ASIO undertook work in updating its strategy addressing professional conduct and behaviour of ASIO officers. This strategy is being developed in recognition of recent legislative amendments and the impending finalisation of Safe Work Australia's draft Code of Practice: Preventing and Responding to Workplace Bullying.

While reducing the likelihood of bullying occurring in the workplace is an important objective of the Professional Conduct and Behaviour Strategy, ASIO has chosen to take a more holistic approach and consider all forms of inappropriate workplace behaviour.

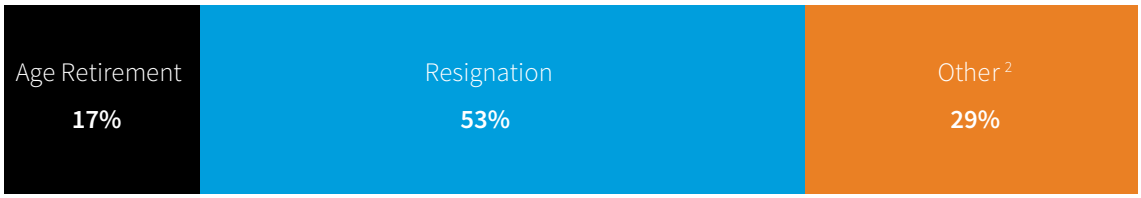
In 2012–13 the Director-General formally referred seven complaints to the ASIO Ombudsman of which six were completed during the reporting period and one was ongoing. The Ombudsman also responded informally to an additional 20 queries from ASIO officers. Of these, six complaints and 11 queries were in relation to bullying or harassment.

During the reporting period one complaint in relation to ASIO was made to the Office of the Inspector-General of Intelligence and Security (IGIS) by a current or former ASIO officer. The complaint was lodged by a former ASIO officer regarding the loss of their security clearance. The IGIS conducted a full inquiry into the matter, and ASIO fully and actively cooperated with the Office of the IGIS to achieve a resolution to this complaint in a timely manner. The IGIS found ASIO's decision was not inappropriate, but made three recommendations in relation to security vetting, risk management and record keeping practices. ASIO has implemented or is actively implementing all recommendations.

Separation rates

During 2012–13 ASIO experienced an increase in the separation rate from 4.7 per cent in 2011–12 to 5.7 per cent in 2012–13. This figure includes the 15 SES officers who accepted voluntary redundancies during the reporting period.

Figure 10 Separations by percentage of total staff and reason for 2012–13



2 Please note that 'voluntary retirement' was reported under 'age retirement' last year. This reason code was changed to 'voluntary redundancy' and this category is now reported under 'other'. 'Other' includes contract expired, contract terminated, dismissed, voluntary redundancy and voluntary retirement.

Accommodation

Ben Chifley Building, Canberra

Construction and commissioning of ASIO's new central office, the Ben Chifley Building, continued over the reporting period.

Delays in the commissioning and testing of essential building systems in the building have led to further slippages in the dates of handover.

At the time of writing, ASIO was scheduled to take possession of the building in May 2014.

To the end of June 2013 the project has experienced overruns of $44 million, which equates to 7.5 per cent of the approved budget of $589 million set in 2008. ASIO's contribution to cost overruns is $24 million which has been met within existing budgets.

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 settled in 2008.

The Ben Chifley Building was opened on 23 July 2013. At the time the decision was made, completion was expected to occur in August 2013 and the opening was timed to enable greater access, including by media, to the ASIO building prior to staff and technical equipment occupying the building.

Australian Cyber Security Centre

In April 2013 the Cyber Security Operations Board made a recommendation to accommodate the Australian Cyber Security Centre (ACSC) within the Ben Chifley Building. This recommendation was agreed to by government in June 2013. The design and construction of the ACSC was executed as a $14.6 million variation to the Ben Chifley Building project. The ACSC is expected to have an operational capability by late 2014.

State and territory offices

In 2012–13 work on ASIO's state and territory office accommodation has focused on implementing energy saving measures to make financial savings and improve energy efficiency. ASIO is committed to reaching the targets set by the government's Energy Efficiency in Government Operations policy. Light and power consumption across ASIO's national property portfolio reduced by 18 per cent from the previous reporting period.

Legislation and litigation

ASIO's high level of involvement in legal and judicial matters continued throughout 2012–13. ASIO's Office of Legal Counsel continued to provide valuable and necessary support to ASIO's core operational and corporate functions by advising on ASIO's mandate and functions, legislative interpretation and reform, use of special powers and operations, furnishing of security assessments and other key legal risk areas.

Legislative amendments

ASIO's Office of Legal Counsel works to ensure legislation affecting ASIO adequately equips and assists the Organisation to fulfil its functions, including by advocating for legislative amendment within a whole-of-government agenda.

PJCIS review of national security legislation

In April 2012 the Attorney-General referred a national security legislation consultation package to the PJCIS for consideration and consultation. The package sought to ensure the statutory powers accorded to Australia's intelligence and law enforcement agencies remained effective in the current and future national security environments. The submission had three components:

- **Telecommunications interception reform**, including proposals to modernise lawful access to communications and associated communications data under the *Telecommunications (Interception and Access) Act 1979* (TIA Act);
- **Telecommunications sector security reform**, including measures to mitigate the national security risks posed to Australia's telecommunications infrastructure; and
- **Australian Intelligence Community legislative reform**, proposing amendments to the ASIO Act and the *Intelligence Services Act 2001* to improve the operational efficiency of intelligence agencies, as well as making some technical and administrative amendments.

ASIO provided a classified submission and a joint unclassified submission with the Australian Federal Police and Australian Crime Commission to assist the PJCIS to consider the issues. ASIO attended two private hearings, on 29 October 2012 and 2 November 2012, to supplement these submissions.

Outside the reporting period, the Senate referred a comprehensive inquiry of the TIA Act to the Legal and Constitutional Affairs References Committee. ASIO has provided a submission to the Committee, noting that rapid technological advances present considerable challenges to ASIO maintaining its capabilities and, in particular, changes to the telecommunications environment have meant our ability to intercept communications under the current regime is under challenge. In the absence of modernisation of the telecommunications interception and access regime ASIO faces the prospect of continuing to progressively lose critical intelligence enabling it to identify threats to security and provide advice so that preventative action can be taken.

ASIO believes reform of the legislation governing interception and access to telecommunications data is required to create a regime that is sufficiently robust and technologically neutral so as not to require revision with each new technological or business development. This needs to continue to recognise the fundamental right to privacy of communications while balancing the critical need to support our efforts to protect our community.

Public Interest Disclosure Act

The *Public Interest Disclosure Act 2013* (PID Act) received royal assent on 15 July 2013 and came into effect on 15 January 2014, both outside the reporting period. The PID Act provides agencies and whistleblowers with procedures to follow in making a 'public interest disclosure', and protections for those who make such disclosures in accordance with the scheme.

In ASIO's view, the resulting PID Act achieves a balance between ensuring the accountability of all agencies while still ensuring the ability of Australian Intelligence Community agencies to carry out their national security functions.

Litigation matters

Throughout the reporting period ASIO was involved in approximately 50 litigation matters including terrorism and other criminal prosecutions and civil matters, in particular judicial and administrative review of ASIO security assessments. ASIO continues to direct considerable resources to managing its involvement in litigation. This is expected to continue due to the continued upward trend in merits and judicial review of adverse security assessments, notably in relation to migration and Australian passport related security assessments; and, the recent surge in criminal prosecutions that require ASIO's intelligence as evidence.

ASIO's litigation focus remained the protection of sensitive national security information-and assisting the Administrative Appeals Tribunal in the performance of merits review of ASIO's security assessments.

M47/2012 v. Director-General of Security and Others [2012] HCA 46

M47, an illegal maritime arrival on the *Oceanic Viking* vessel, asked the High Court to quash his adverse security assessment on the basis that ASIO had denied him procedural fairness in not interviewing him.

He also sought an order that a visa be granted and a declaration that his immigration detention was unlawful. M47 instituted proceedings in the High Court against five defendants, including the Director-General of Security.

On 5 October 2012 the High Court delivered its judgement, finding ASIO had provided procedural fairness in the circumstances of the case. On 29 November 2012 the Court remitted M47's visa application to the Refugee Review Tribunal for further consideration.

S138/2012 v. Director-General of Security and Others

In 2009 ASIO issued an adverse security assessment in respect of S138, an illegal maritime arrival in immigration detention. S138 asked the High Court to quash the assessment, compel a visa grant and declare his detention unlawful. In 2012 the Court handed down its related M47 decision, which was limited to applicants who had made valid protection visa applications under Migration Regulation 866.225(a). S138 did not fall into this category because he was not eligible to make a valid visa application and had requested the Minister for Immigration and Citizenship exercise his discretion to enable him to do so. This request was declined.

On 7 June 2013, following an advisory opinion by the Independent Reviewer of Adverse Security Assessments, the Director-General issued a non-prejudicial security assessment for S138. The Department of Immigration and Citizenship subsequently granted a bridging visa pending consideration of S138's refugee claim. On 13 June 2013, on the basis of the parties' consent, the Court dismissed the application.

The Queen v. Khazaal [2012] HCA 26

Mr Khazaal was found guilty in 2008 of making a document in connection with a terrorist act and sentenced to 12 years imprisonment. The jury was unable to reach a verdict on the additional charge of attempting to incite others to commit a terrorist act. In 2011 the New South Wales Court of Criminal Appeal (NSW CCA) overturned the conviction and ordered a retrial, to be heard with the incitement retrial. The Crown was granted special leave to appeal to the High Court, on the basis of provisions in the Criminal Code Act 1995 relating to evidence.

On 10 August 2012 the High Court unanimously allowed the Crown's appeal, overturning the NSW CCA decision and reinstating the conviction. The Court remitted the matter to the NSW CCA, which on 13 June 2013 dismissed Mr Khazaal's appeal against the severity of his sentence. Mr Khazaal may be eligible for release on parole in 2017.

RJCG v. Director-General of Security [2013] FCA 269

ASIO assessed RJCG, an Australian citizen employed by the Commonwealth, to have engaged in acts of foreign interference by providing information to foreign intelligence officers. ASIO issued an adverse security assessment recommending revocation of his security clearance. On 22 August 2012 the Administrative Appeals Tribunal affirmed ASIO's decision. RJCG appealed this decision to the Federal Court.

TCXG and Director-General of Security and Anor [2013] AATA 284

On 21 June 2012 ASIO issued an adverse security assessment in respect of TCXG. The Minister for Foreign Affairs consequently refused TCXG's application for an Australian passport. ASIO assessed that TCXG adhered to an extremist interpretation of Islam which condoned the use of politically motivated violence. ASIO assessed his extremist actions involved encouraging, fostering and supporting extremist activities, including the use of politically motivated violence. On 10 May 2013 the AAT affirmed ASIO's security assessment and the passport refusal.

NBMW v. Minister for Immigration and Citizenship [2013] FCA 651

NBMW, an illegal maritime arrival, challenged ASIO's adverse security assessment. On 12 September 2012 the Administrative Appeals Tribunal affirmed the security assessment. NBMW appealed this decision to the Federal Court but then discontinued that appeal and sought instead to join the Director-General of Security to his separate Federal Court action against the Minister for Immigration and Citizenship. He claimed the security assessment was not lawful or validly made because ASIO had denied him procedural fairness. On 5 July 2013 the Federal Court dismissed the application to join the Director-General to the separate proceedings.

Use of ASIO special powers

In the performance of its functions it is sometimes necessary for ASIO to use highly intrusive methods of investigation, such as telecommunications interception and access, listening devices, entry and search of premises, computer access, tracking devices, and the examination of postal and delivery service articles.

The Attorney-General may authorise warrants for ASIO to lawfully undertake such activities under the ASIO Act or the TIA Act. The ASIO Act also enables ASIO, with the Attorney-General's consent, to seek warrants from an independent issuing authority (a federal magistrate or judge) for questioning, or questioning and detention, of individuals.

All ASIO warrants must satisfy strict thresholds in the relevant legislation and comply with the Attorney-General's Guidelines. The guidelines dictate that ASIO must collect information using the most effective means that are proportionate to the gravity of the threat and its likelihood and to use as little intrusion into personal privacy as possible.

Security of ASIO

A strong security culture underpins ASIO's ability to carry out its mission to protect Australia, its people and its interests. This requires strong security policies, practices and technologies. These standards serve to protect the Organisation's people, premises and information from compromise and ensure ASIO can carry out its mission. Without strong security practice, sensitive information could be accessed by those who wish to do Australia harm, and allied partners and members of the public would be less willing to communicate information to ASIO.

ASIO's security policies and practices are compliant with the Australian Government's Protective Security Policy Framework (PSPF) and ASIO regards its security standard as best practice. ASIO continually develops and reviews its security policies and procedures. ASIO's active security culture, contributed to by all officers, further works to protect officers, premises and information from compromise.

Security governance and policy

During the reporting period, ASIO established the Counter Intelligence and Security Review Committee (CISRC) to provide guidance and direction in respect of security policy for the Organisation. The CISRC is also responsible for setting insider threat and other internal counter intelligence and security priorities, including by evaluating the security environment and understanding the evolving strategic nature of the threat. The CISRC is chaired by the Director-General and attended by both Deputy Directors-General and other ASIO senior executive officers.

The ASIO Security Committee (ASC) operates as a sub-committee of the CISRC and comprises SES-level representatives. The ASC provides advice and recommendations to the CISRC for consideration and action as appropriate.

Security clearances in ASIO

Security vetting is an integral part of ASIO's security requirements. As a clearance holder, ASIO officers must maintain clearance suitability and proactively report on any matters which may affect their clearance. Pressures on ASIO's initial vetting and revalidation continued over the reporting period. It is a time consuming process and ASIO is constantly seeking ways to become more efficient in security vetting, without compromising the high standards the government rightly places on ASIO security practices. Initial and ongoing security vetting of ASIO staff provides a critical counter-intelligence function and is conducted in line with whole-of-government requirements, security risk management strategies, policies and procedures.

Security breaches

ASIO strives to uphold the highest standard of security practice, including the reporting of security breaches—accidental or unintentional failures to observe protective security mandatory requirements. ASIO is required to report annually on its security status, including security breaches, to the Secretaries' Committee on National Security and the National Security Committee of Cabinet.

Relevant senior managers in ASIO are notified of breaches which occur within their branch or division to enable proactive management of each occurrence. Multiple breaches by the same individual within a 12 month period attract additional consequences, from formal counselling to misconduct sanctions. An ASIO officer's security breach history over the previous 12 month period may also be taken into consideration when considering the officer's suitability for internal promotion or posting.

ASIO continually modifies and enhances its e-security capabilities to ensure its information technology systems are adequately protected from both accidental and malicious activity. ASIO employs a range of policies and practices in regards to information communication technology systems to ensure vulnerabilities are avoided where possible and remedied when needed.

Relationships, reporting and accountability

There are numerous, layered oversight and accountability mechanisms that act to provide assurance to the Australian public of the legality and propriety of ASIO's activities (see Box).

Oversight and accountability mechanisms applying to ASIO

Ministerial and Parliamentary accountability

- ASIO regularly advises and reports to the Attorney-General on the Organisation's security intelligence activities, including through ASIO's classified Annual Report which is also considered by the National Security Committee of Cabinet.
- The PJCIS regularly reviews ASIO's administration and expenditure.
- The Director-General of Security appears before Senate Estimates.

Inspector-General of Intelligence and Security

- The IGIS provides assurance to the government and Australian public that ASIO operates with propriety, according to the law and ministerial guidelines, and with due regard for human rights.
- As an independent statutory office holder, the IGIS is not subject to general direction from the Prime Minister or other Ministers on how responsibilities under the IGIS Act should be carried out.
- The Office of the IGIS may access all of ASIO's records, interview any of ASIO's staff, and enter ASIO's premises.
- The IGIS conducts ongoing inspections of ASIO's activities (particularly its operational activities) and initiates inquiries when necessary (or referred by ministers).
- The IGIS reports on the outcomes of these inspections and inquiries to the Attorney-General, other ministers as appropriate, and the Parliament.

Independent review and approval of warrants

- The Attorney-General's Department independently reviews each case ASIO submits for a warrant to ensure it meets the legislative test.
- Responsibility rests with the Attorney-General to approve ASIO's use intrusive warrant powers (and, in the case of questioning and detention powers, approval of a judicial officer).
- ASIO reports to the Attorney-General on the value and intelligence obtained from each warrant.

Review of ASIO decisions

- Australian citizens, permanent residents and special category visa holders have a right of review of adverse ASIO security assessments through the Administrative Appeals Tribunal, and all individuals can seek judicial review.
- There are reviewers with specific powers to examine counter-terrorism legislation and adverse security assessments issued in relation to protection visa applicants in immigration detention.

ASIO's internal accountability and training

- ASIO's code of conduct and security clearance requirements require all ASIO employees to exhibit high standards of integrity and probity in their duties.
- Internal policies and procedures provide direction to ASIO officers in carrying out their duties.
- All employees are required to undertake ethics & accountability eLearning every three years. All employees have access to the Attorney-General's Department human rights e-learning resource.

Parliamentary oversight

Attorney-General

ASIO is responsible to the Australian Government through the Attorney-General, as outlined in the ASIO Act. During the reporting period the Hon. Mark Dreyfus QC MP was sworn in as Attorney-General on 4 February 2013, replacing the Hon. Nicola Roxon MP.

ASIO informs the Attorney-General of significant national security developments. This includes advice to the Attorney-General on a range of issues connected to the security environment, specific investigations and operations, and administrative matters relevant to ASIO. Throughout the reporting period, ASIO communicated primarily through over 300 submissions.

ASIO's operational activity is conducted in accordance with the *Attorney-General's guidelines*, last updated by the Attorney-General on 10 December 2007 under sections 8A(1) and 8A(2) of the ASIO Act. The guidelines stipulate that ASIO's information collection activities should be conducted in a lawful, timely and efficient manner, using the least intrusion necessary into an individual's privacy and proportionate to the gravity of the threat being investigated.

All ASIO warrants (other than questioning and detention warrants, which are issued and approved by a person as specified under Part III, Division 3 of the ASIO Act) are issued by the Attorney-General after consideration of a request presented by the Director-General of Security. For every warrant raised, ASIO is required to report to the Attorney-General on the extent to which action undertaken in respect of the warrant assisted the Organisation in carrying out its functions.

Report to Parliament

ASIO is the only Australian Intelligence Community agency that produces an annual unclassified Report to Parliament. This report provides details of ASIO's activities during each reporting period, including the nature of the threat environment, details of ASIO's performance across its functions, details of ASIO's corporate human resources and governance arrangements, and ASIO's financial statements. ASIO's Reports to Parliament are available on ASIO's website (www.asio.gov.au).

ASIO also produces a highly classified annual report outlining ASIO's operational and corporate activities in greater detail. ASIO's annual report is distributed externally to the Attorney-General and a select group of ministers (including the National Security Committee of Cabinet), the Leader of the Opposition and a small group of senior Commonwealth government officials.

Parliamentary Joint Committee on Intelligence and Security

Throughout the reporting period ASIO engaged with the PJCIS on a range of matters relevant to the committee's role, including:

- Providing classified and unclassified submissions to the PJCIS on the Organisation's administration and expenditure;
- Providing a submission and attending a hearing for the PJCIS review of national security legislation; and
- Contributing to four hearings for the proscription of terrorist organisations (Al-Shabaab, Hamas's Izz al-Din al-Qassam Brigades, Lashkar-e-Tayyiba and Palestinian Islamic Jihad).

PJCIS review of national security legislation

In April 2012 the Attorney-General referred a national security legislation consultation package to the PJCIS for consideration and consultation. Further details are available in the 'Legislation and litigation' section of this submission at page 30.

Senate Standing Committee on Legal and Constitutional Affairs

Senate Estimates provides an opportunity for parliamentary scrutiny of the executive branch of government, including on issues of departmental expenditure and government operations. As part of the Attorney-General's portfolio, ASIO appears before the Senate Standing Committee on Legal and Constitutional Affairs. The Director-General and Deputy Director-General appeared at Supplementary Budget Estimates in October 2012 and Budget Estimates in May 2013.

External oversight mechanisms

Inspector-General of Intelligence and Security

The Office of the IGIS was formally established under the *Inspector-General of Intelligence and Security Act 1986.* The IGIS, Dr Vivienne Thom, is an independent statutory office holder responsible for reviewing the activities of the Australian Intelligence Community to ensure the agencies act legally, with propriety, in compliance with ministerial guidelines and directives, and with due regard for human rights.

The IGIS conducts regular and ongoing inspections and monitoring of ASIO activities. The IGIS has wide-ranging powers similar to those of a royal commission, including access to ASIO records or premises at any time.

Inquiry into analytic independence

During the reporting period the IGIS reported the findings of her inquiry into the analytic independence of ASIO, the Defence Intelligence Organisation and the Office of National Assessments. The IGIS noted her findings were generally positive and there was no evidence of inappropriate pressure being placed on any of the agencies. The IGIS made several recommendations in regard to ASIO's recordkeeping, source referencing, key judgements review and dissent management. ASIO accepted all of the IGIS's recommendations.

Inquiry into asylum seekers presenting complex security issues

On 5 June 2013 the then Prime Minister, the Hon. Julia Gillard MP, requested that the IGIS conduct an inquiry into the management by Australian agencies of people seeking asylum who present complex security issues, particularly an Egyptian illegal maritime arrival who was the subject of an Interpol red notice. At the time of writing, the IGIS report had yet to be released. However, ASIO had begun implementing reforms in this area in January 2013—several months in advance of the commissioning of the IGIS inquiry.

Inquiry into the attendance of legal representatives at ASIO interview

On 27 March 2013 the IGIS initiated an inquiry into the attendance of legal representatives at ASIO interviews. In her report, published outside the reporting period, the IGIS made five recommendations regarding ASIO's policies and practices; ASIO accepted four recommendations and partially accepted one recommendation.

Independent Reviewer of Adverse Security Assessments

On 3 December 2012 the Hon. Margaret Stone commenced as the Independent Reviewer of Adverse Security Assessments (the Independent Reviewer).

The role of the Independent Reviewer is to conduct an independent advisory review of ASIO adverse security assessments furnished to the Department of Immigration and Border Protection (DIBP) in relation to individuals who remain in immigration detention, having been found by DIBP to be:

- owed protection obligations under international law; and
- ineligible for a permanent protection visa, or who have had their permanent protection visa cancelled, because they are the subject of an adverse security assessment.

In performing her role, the Independent Reviewer is required to:

- examine all material relied on by ASIO in making the adverse security assessment;
- provide an opinion to the Director-General as to whether the adverse security assessment is an appropriate outcome based on that and other relevant material; and
- make recommendations accordingly, for the Director-General's consideration.

The Independent Reviewer's Terms of Reference require her to conduct a periodic review of adverse security assessments for eligible persons every 12 months.

Immediately following her commencement, the Independent Reviewer informed eligible persons about their right to seek review and invited them to apply. All 55 eligible persons subsequently applied for review, and each is legally represented.

In May 2013 the review of one of the 55 individuals ceased when ASIO issued a new non-prejudicial security assessment. This outcome was part of ASIO's own processes in respect of individuals who are the subject of an adverse security assessment and was not as a result of the independent review process.

In 2012–13 ASIO provided the Independent Reviewer with the information it had relied on in making the adverse security assessments for all eligible persons. Shortly after the Independent Reviewer's appointment, ASIO advised it was reconsidering the assessment of one applicant. It was decided the review would not proceed for that individual until ASIO had concluded its reassessment. ASIO's reassessment was not concluded by the end of the reporting period.

Findings of the Independent Reviewer

During the 2012–13 reporting period the Independent Reviewer released her findings in relation to five applicants for review. In three cases, the Independent Reviewer formed the opinion the adverse security assessments issued by ASIO remain appropriate. In relation to two individuals, the Independent Reviewer formed the opinion the adverse security assessments are not appropriate and recommended ASIO issue either non-prejudicial or qualified security assessments. ASIO undertook new assessments of these two cases, resulting in the Director-General issuing non-prejudicial security assessments in relation to both individuals.

From 1 July 2013 to 30 January 2014 the Independent Reviewer released her findings in relation to an additional 10 individuals. In relation to nine individuals, the Independent Reviewer formed the opinion that ASIO's assessment was appropriate. In one case, the Independent Reviewer formed the opinion the adverse assessment is not appropriate and recommended ASIO issue a non-adverse security assessment. ASIO undertook a new assessment of this case, resulting in the Director-General issuing a qualified security assessment in relation to the individual.

As at 30 January 2014 the Independent Reviewer had referred to ASIO 'new information' in respect of a further four cases. In one of these cases, ASIO completed its consideration of the new information and responded to the Independent Reviewer in December 2013; the Independent Reviewer is now in the process of completing that review. In the remaining three cases, ASIO's consideration of this information was ongoing.

No periodic reviews were undertaken during the reporting period as 12 months had not passed since the release of the Independent Reviewer's initial findings.

Public statements

Throughout the reporting period ASIO continued to engage with the public through a variety of statements and speeches by the Director-General. The Director-General made public comment on a range of matters, including the security environment in Syria, cyber threats, the Ben Chifley Building and ASIO's new strategic plan. The Director-General has addressed a variety of forums, including the Australian Industry Group, the Security in Government Conference 2012 and the Biennial Conference of the District and County Court Judges (of Australia and New Zealand).

ASIO's website contains transcripts of the Director-General's public speeches, copies of ASIO's public submissions to inquiries and answers to frequently asked questions. ASIO frequently updates its website to ensure the most contemporary information is available to the public. ASIO's Report to Parliament is also available on the website and provides a significant body of information to inform the public about ASIO's activities.

ASIO's domestic relationships

ASIO's ability to protect Australia, its people and its interests relies on maintaining effective networks and productive relationships with domestic partners, including government agencies, industry and the general public. These relationships contribute to ASIO's mission and in part seek to ensure threats to security are identified and mitigated appropriately.

During the reporting period ASIO continued to broaden and deepen its engagement with government agencies, including through regular ASIO Partnership Forums. These forums provide information to senior officers of government partners to help them better understand the security challenges faced by Australia, ASIO's approach to dealing with these challenges, and the role and functions of the Organisation and the framework it works within.

ASIO's annual Stakeholder Satisfaction Survey seeks feedback on key partners' engagement with ASIO, their views on collaboration and an evaluation of ASIO's information and advice. A significant majority of agencies interviewed noted an improvement in their engagement with ASIO, something on which ASIO will continue to build.

The Business Liaison Unit (BLU) is a direct and effective public interface between Australian business and Australian intelligence agencies. The BLU provides valuable unclassified advice to private industry through briefings, key industry forums, and written reports published on the BLU website. These reports provide security-relevant contextual information for businesses to consider when making decisions about risk management and continuity planning. Examples of BLU reporting include country security snapshots, critical infrastructure threat assessments and the threat posed by the trusted insider.

ASIO's international relationships

The global, interconnected nature of security threats dictates that ASIO foster and maintain strong international relationships. At the end of the reporting period, the Attorney-General had authorised ASIO to liaise with 347 authorities in 131 countries. This is an increase on last year of seven authorities and six countries and reflects ASIO's commitment to fostering new international relationships where appropriate.

Over the reporting period, ASIO provided security intelligence support to a range of major international events with a nexus to Australian interests, including:

- the 43rd Pacific Islands Forum, of which Australia is a member;
- the 10th anniversary of the Bali bombing;
- ANZAC Day commemorations in Turkey and France; and
- the London Olympic and Paralympic Games.

While the number of officers overseas varies from year to year, over the last three years there has been a total diminution of officers in liaison, exchange or seconded roles overseas by three people.

Glossary

ACSC	Australian Cyber Security Centre
ANAO	Australian National Audit Office
ASC	ASIO Security Committee
BLU	Business Liaison Unit
CISRC	Counter Intelligence and Security Review Committee
DIBP	Department of Immigration and Border Protection
FMA Act	*Financial Management and Accountability Act 1997*
G20	Group of Twenty
IDP	Intelligence Development Program
IGIS	Inspector-General of Intelligence and Security
NIC	National Intelligence Community
NSW CCA	New South Wales Court of Criminal Appeal
PID Act	*Public Interest Disclosure Act 2013*
SES	Senior Executive Service
TIA Act	*Telecommunications (Interception and Access) Act 1979*

Sub