Australian Government

Australian Security Intelligence Organisation

ASIO Report to Parliament 2011–12

OUR VISION

The intelligence edge for a secure Australia

OUR MISSION

To identify and investigate threats to security and provide advice to protect Australia, its people and its interests

OUR VALUES

ASIO is committed to:

Excellence

- producing high quality, relevant, timely advice
- displaying strong leadership and professionalism
- improving through innovation and learning

Integrity

- being ethical and working without bias
- maintaining the confidentiality and security of our work
- respecting others and valuing diversity

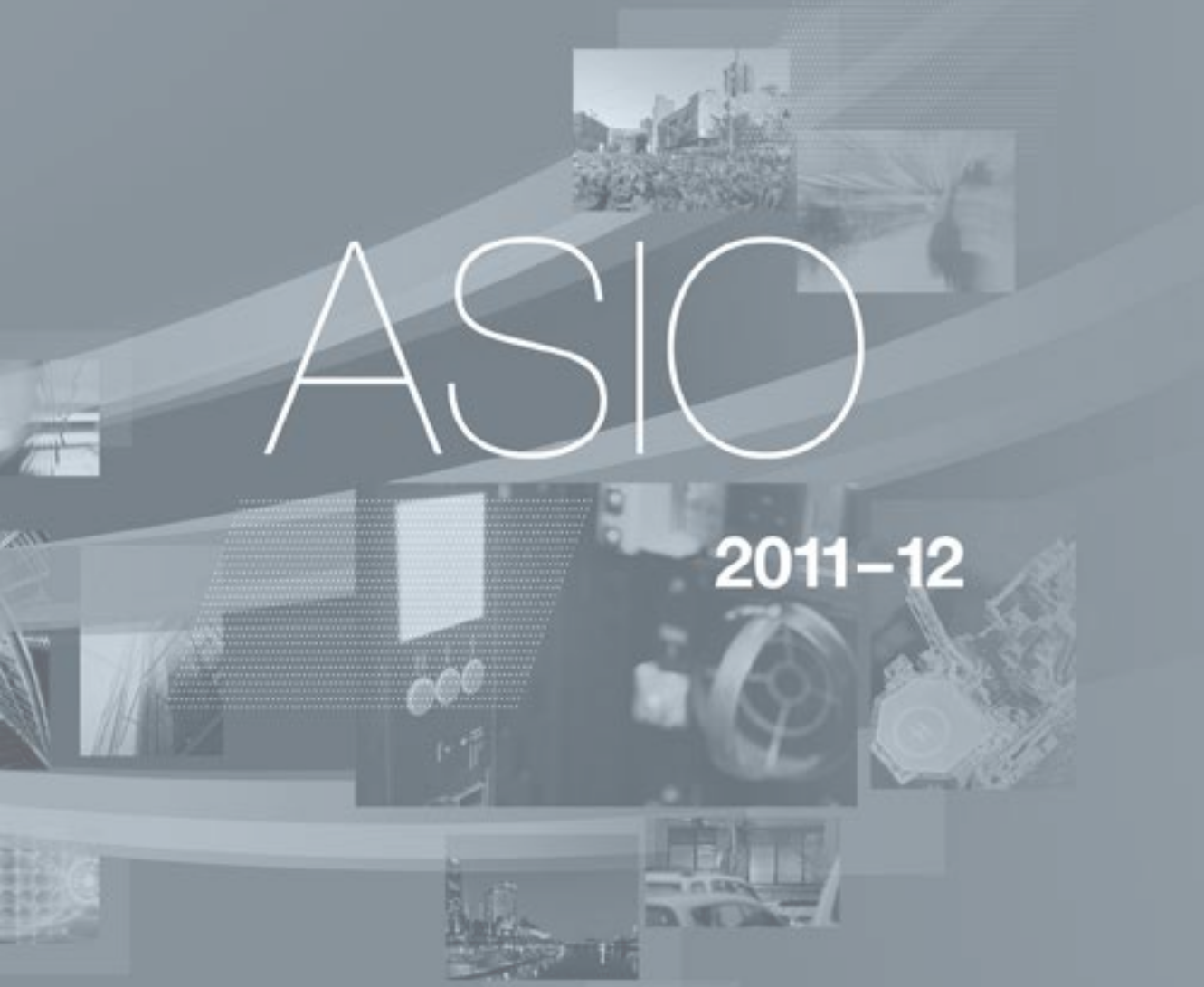
Accountability

- being responsible for what we do and for our outcomes
- being accountable to the Australian community through the Government and the Parliament

Cooperation

- building a common sense of purpose and mutual support
- using appropriate communication in all our relationships
- fostering and maintaining productive partnerships

ASIO Report to Parliament 2011–12



ISSN 0815-4562

© Commonwealth of Australia (Australian Security Intelligence Organisation) 2012.

All material presented in this publication is provided under a Creative Commons (CC) BY Attribution 3.0 Australia Licence (http://creativecommons.org/licenses/by/3.0/au/deed.en).

The details of the relevant licence conditions are available on the Creative Commons website (http://creativecommons.org/licenses/) as is the full legal code for the CC BY Attribution 3.0 Australia Licence (http://creativecommons.org/licenses/by/3.0/legalcode).

Using the Commonwealth Coat of Arms

The terms of use for the Commonwealth Coat of Arms are available from the It's an Honour website (http://www.itsanhonour.gov.au/coat-arms/index.cfm).

ASIO Report to Parliament 2011–12

Correction – Errors occurred in:

Appendix A – Agency Resource Statement 2011–12 and
Appendix B – Expenses and Resources Table 2011–12,

of the tabled ASIO Annual Report (2011–12).
The correct tables are provided below.

Appendix A

Agency resource statement 2011–12

	Actual available appropriations for 2011–12 $'000	Payments made 2011–12 $'000	Balance remaining $'000
Departmental appropriation			
Prior year departmental appropriation	250,039	250,039	-
Departmental appropriation	328,124	110,902	217,222
S.31 Relevant agency receipts	19,856	17,852	2,004
S.30 Receipts	12,346	12,346	-
	610,365	**391,139**	**219,226**
Departmental non-operating			
Prior year equity injections	48,699	48,699	-
Equity injections	41,806	41,806	-
Departmental capital budget	19,228	12,228	7,000
	109,733	**102,733**	**7,000**
Total resourcing and payments	**720,099**	**493,872**	**226,226**

Appendix B

Expenses and resources table 2011–12

	Budget 2011–12 $'000	Actual expenses 2011–12 $'000	Variation 2011–12 $'000
Departmental expenses			
Ordinary annual services (Appropriation Bill No.1)	332,724	355,950	(23,226)
Expenses not requiring appropriation in the budget year	70,248	40,288	29,960
Total expenses for outcome 1	**402,972**	**396,238**	**(6,734)**

	2010–11	2011–12	Variation
Average staffing levels (number)	1,662	1,683	21

Australian Government
Australian Security
Intelligence Organisation

Director-General of Security

10 October 2012

A6695871

The Hon Nicola Roxon MP
Attorney-General
Parliament House
CANBERRA ACT 2600

Dear Attorney,

In accordance with section 94 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), I am pleased to present to you ASIO's Annual Report for the year ending 30 June 2012.

As required by the ASIO Act, a copy of the Annual Report – with deletions authorised by you to protect national security – is to be laid before each House of the Parliament.

In addition, as required by the *Commonwealth Fraud Control Guidelines*, I certify that I am satisfied ASIO has in place appropriate fraud control mechanisms that meet the Organisation's need and comply with the Guidelines.

Yours,

David Irvine

David Irvine

GPO Box 2176
Canberra City ACT 2601
Telephone: 02 6249 6299
Facsimile: 02 6257 4501

FOI WARNING:
Exempt document under
Freedom of Information Act 1982.
Refer related FOI requests to
Attorney-General's Department, Canberra.

Table of Contents

Director-General's foreword

ASIO's core mission is to identify and investigate threats to security and provide advice to protect Australia, its people and its interests in Australia and overseas. To do so, ASIO must maintain its nationally important security intelligence capability in the face of a challenging security and budgetary environment.

Security environment in 2011–12

In 2011–12, Australia's security environment continued to evolve, but the principal threats remained largely unchanged from recent years.

Terrorism continued to present the most immediate threat to the security of Australians and Australian interests. September 2011 marked the tenth anniversary of the 9/11 attacks in the United States and in October 2012 we will commemorate the tenth anniversary of the tragic terrorist attacks in Bali. A decade on, while Australia is undeniably one of the safer countries in the world, the unfortunate reality is that the threat of terrorism remains real and persistent and therefore represents the greatest focus of ASIO's attention.

In keeping with the trend of recent years, the threat of home-grown terrorism remains a principal concern. Groups or individuals in Australia engaged in terrorist planning with little or no direction from established international extremist groups. At the same time, we witnessed in Norway in July 2011, the appalling loss which can be inflicted by a 'lone actor' terrorist—this incident also serves as a reminder that extremism exists in a broad spectrum of ideologies.

In 2011–12, together with law enforcement and other national and international partners, ASIO was involved in disrupting terrorist planning in Australia, in preventing Australians seeking to travel overseas to engage in terrorist training and in countering violent extremism amongst the Australian community.

Espionage, including via cyber means, also continues as an enduring and first-order threat to Australia's security—targeting not only government departments and agencies, but key commercial enterprises and industries. The hostile and pervasive nature of this threat required increased cooperation and coordination with domestic and international partners, as well as active engagement with elements of nationally critical industry.

External reviews

In 2011–12, the Australian Government received the report of the Independent Review of the Intelligence Community, commissioned by the Prime Minister to evaluate the effectiveness of the Australian intelligence community. I was heartened but not at all surprised by the review's findings, released in January 2012, that Australia and its citizens were safer than they would otherwise have been as a result of the community's intelligence efforts and that our intelligence capabilities had contributed significantly to the global security effort. I also particularly welcomed the statement that Australia's intelligence agencies were working well together. One of ASIO's strategic goals is to enhance our strategic impact by working closely with and employing our capabilities to support the broader national security effort.

Also during the reporting period, the Joint Select Committee on Australia's Immigration Detention Network, the Australian National Audit Office (ANAO) and the Inspector-General of Intelligence and Security conducted reviews which focused on, or encompassed, aspects of ASIO's security assessment function. ASIO's support for these reviews demonstrated the Organisation's commitment to strong accountability mechanisms. I welcomed the conclusion of the ANAO report that ASIO's arrangements for providing security assessments of individuals to client agencies are robust and broadly effective.

Reform and modernisation program

Significant progress was made in 2011–12 on ASIO's comprehensive business reform and modernisation program, with a number of projects delivering important efficiencies for the Organisation. Notable highlights include the implementation of a new streamlined, but no less accountable, warrants process; the development of a reliable case management function enhancing efficiency and accountability in ASIO investigations; and the establishment of new corporate governance arrangements.

Another important component of ASIO's reform program has been its work with the government to develop and modernise the legislative framework within which we operate to ensure it is contemporary and can support the national security capability in a constantly changing operational and technical environment.

In May 2012 the Attorney-General asked the Parliamentary Joint Committee on Intelligence and Security to inquire into proposed reforms to national security legislation, including to the *Australian Security Intelligence Organisation Act 1979*, the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997* and the *Intelligence Services Act 2001*. I believe these reforms are necessary to ensure our investigative capability continues to be effective and is commensurate with the threats we face and with the technology used by those who threaten national security. These are also necessary to ensure effective collaboration with partners, so Australia's critical telecommunications infrastructure is properly protected and so we can continue to provide appropriate protection for our sources and officers engaged in vital intelligence collection. I look forward to the outcomes of this inquiry in 2012–13.

ASIO's budgetary outlook

Preparing for the future in a more tightly constrained budgetary environment has underpinned ASIO's corporate management and strategic planning during 2011–12. The past decade has seen significant challenges and changes for ASIO in a period of growth. The Organisation is now in a period of consolidation—both in terms of staffing and the maintenance of our technical capabilities. During the year we made a number of decisions to deliver savings, while focusing our effort on priorities of highest risk. These included reductions to our senior executive structure, overseas representation and travel budgets where possible. Budgetary pressures forced ASIO, in February 2012, to defer the program of growth to a staffing level of 1860 recommended by the Taylor Review in 2005, with current numbers approximately 130 below that target.

While staffing growth has been deferred indefinitely, ASIO must continue to recruit high-calibre officers—particularly intelligence professionals and technical officers—to ensure we maintain ASIO's nationally important security intelligence capability into the future. Given that the strengths of our people are the key to our effectiveness, we will also need to maintain our investment in training, professional skills and leadership development.

ASIO's intelligence collection, analysis, operational, technical and people capabilities are national resources. These capabilities take many years to develop and it is vital they remain effective and up to date to address the national security threats and the security challenges of today and the future.

Maintenance of these core national capabilities has been a priority in 2011–12 and will continue to be central to our investment planning as we move forward in what will be a more constrained budgetary environment. Well developed national capabilities take considerable effort to build and are difficult to re-establish in an emergency. ASIO will continue to drive its reform and modernisation program to ensure that it can maintain the necessary level of investment in capability development.

At the same time, the tightening budgetary environment requires constant rigorous prioritisation of operational activity and the allocation of resources to ensure effort is concentrated against the highest security risks. Active management of risk will become even more important during the next reporting period. ASIO has refined its Strategic Risk Management Framework to support and guide senior management to identify, treat and monitor the strategic risks ASIO manages on behalf of the nation.

Engagement with the public

I am acutely conscious of the tension that exists between the need for a security intelligence organisation to operate in secret to protect its sources, methods and capabilities and the need for the community which ASIO serves to feel confident its security agencies are acting within the bounds of the law and in accordance with moral and ethical standards. ASIO has long operated within a stringent accountability framework. The details of this framework and the considerable levels of independent external oversight to which ASIO is subjected are often not well known or understood.

A particular focus throughout 2011–12 has been to find ways to provide greater visibility and enhance public awareness of the work of the Organisation, how it goes about its business and the strict legal and accountability framework under which we function. I have accepted more invitations to address public seminars and engagements and we have further enhanced our outreach with the community to build trust and greater mutual understanding. Through the appearances at public Senate Estimates and parliamentary hearings, development of the ASIO website and through publications such as this Annual Report to Parliament, ASIO seeks to make available as much information as possible about the work of the Organisation with national secruity constraints. While there will always be significant areas of ASIO's work which must necessarily remain secret, particularly our operations and methods, I am committed to continuing this focus on increased public engagement.

I trust this report will provide insights into ASIO's work during 2011–12 as well as the challenges we are anticipating and preparing for in the future.

The year at a glance

Our outcome To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government.

Our vision The intelligence edge for a secure Australia.

Our mission To identify and investigate threats to security and provide advice to protect Australia, its people and its interests.

In 2011–2012:

Our people (see Part 5)

- We welcomed 147 new staff, bringing the full time equivalent to 1721.
- 32 officers graduated from our Intelligence Development Program, becoming ASIO Intelligence Professionals.
- Our separation rate decreased from 5.9% to 4.7%.

Our funding (see Part 6 and appendices A and B)

- ASIO received $328 million from government and was allocated a further $42 million equity injection for costs associated with the move to the new central office.

Our work (see Part 2)

The Organisation:

- initiated and continued numerous counter-terrorism and espionage investigations in line with our mission; and
- published 3000 written products across a range of security intelligence topics.

We completed:

- 34 Business Liaison Unit (BLU) reports distributed via the BLU website;
- 153,644 counter-terrorism security assessments;
- 27,801 personnel security assessments;
- 24,097 visa security assessments; and
- the Top Secret certification of 42 sites.

Building national security capability (see Part 5)

Highlights of our ongoing modernisation and reform activities.

- implemented a case management function, improving efficiency and accountability of ASIO's inquiries and investigations;
- developed an Intelligence Coordination Prioritisation Framework to assist decision-making around investigations; and
- introduced a Job Family Model and Workforce Sourcing Plan to focus and build the resources we need to meet Australia's national security challenges.

Improving our environmental impact

The Organisation:

- saved 180,000 kilowatt hours from its total electrical energy consumption;
- installed energy efficient lighting effectively reducing energy consumption; and
- halved the volume of water used to process shredded paper waste.

Looking forward… ASIO will take possession of the new central office in April 2013.

Looking back… the first volume of the official history of ASIO is scheduled for completion in 2013.

Guide to the report

The Director-General of Security reports annually on the activities of ASIO to the Attorney-General, as required under section 94 of the *Australian Security Intelligence Organisation Act 1979*. The minister is required to table an unclassified version of this Report in each House of Parliament within 20 sitting days of receipt.

This Report forms part of ASIO's accountability framework and is an opportunity to provide information on ASIO's work.

Part One provides a summary of ASIO's operating environment and national security focus.

Part Two outlines performance of ASIO, in providing information, guidance and advice to stakeholders.

Part Three reports in detail on ASIO's performance. This part is classified Top Secret and is excluded in its entirety for reasons of national security.

Part Four looks at the internal and external reviews, audits and accountability for ASIO.

Part Five reports on the corporate services and management functions of the Organisation.

Part Six sets out financial statements for the 2011–12 financial year.

Part Seven details information regarding finances, resources and reports required under legislation.

ASIO's role and functions

Australia's Security Intelligence Organisation (ASIO) protects Australia's national security in accordance with the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). To do this, ASIO collects, correlates and evaluates intelligence relevant to security and provides advice to government concerning security threats. ASIO operates under the direction of the Director-General of Security, who is responsible to the Attorney-General.

In the ASIO Act 'security' is defined as:

- the protection of Australia and its citizens from;
  - espionage;
  - sabotage;
  - politically motivated violence;
  - promotion of communal violence;
  - attacks on Australia's defence system;
  - acts of foreign interference;

  whether these are directed from, or committed within, Australia or not;
- the protection of Australia's territorial and border integrity from serious threats; and
- the carrying out of Australia's responsibilities to any foreign country in relation to the above.

ASIO is entrusted with gaining intelligence to identify and investigate security threats, and with providing advice to government, in order to protect Australia and Australians from such threats. ASIO also provides advice on protective security to government, and obtains foreign intelligence within Australia under warrant on matters relating to Australia's national security, foreign relations or national economic well-being at the request of the Minister for Defence or the Minister for Foreign Affairs.

ASIO functions within very specific policies, procedures and legislative parameters which enable it to be accountable to government, parliament and the Australian community. The foundation of the Organisation's governance and oversight is the ASIO Act, which has been carefully drafted to maintain the balance between the civil rights of an individual and the right of the public to live in a safe and secure society. The ASIO Act limits ASIO's activities to a number of specific functions, set out in section 17. ASIO submits an annual Review of Administration and Expenditure to the Parliamentary Joint Committee on Intelligence and Security. Additionally, the Inspector-General of Intelligence and Security inspects, inquires into and reports on ASIO's activities to ensure that ASIO is acting legally and with propriety.

ASIO continues to develop collaborative relationships with Australian intelligence and defence agencies, the wider Australian national security community, other government departments and agencies and industry, along with foreign partners, to achieve its mission.

Organisational structure

The past decade has seen significant challenges and change for ASIO—the emergence of new high-intensity threats and rapid growth to develop the national security intelligence capability from a low and inadequate base of 10 years ago.

ASIO is now in a period of consolidation. Over the reporting period ASIO underwent some initial changes in both structure and leadership roles, with further refinement expected in 2012–13.

In 2011–12 work to align the corporate and operational areas of ASIO resulted in a change of designation for both Deputy Directors-General.

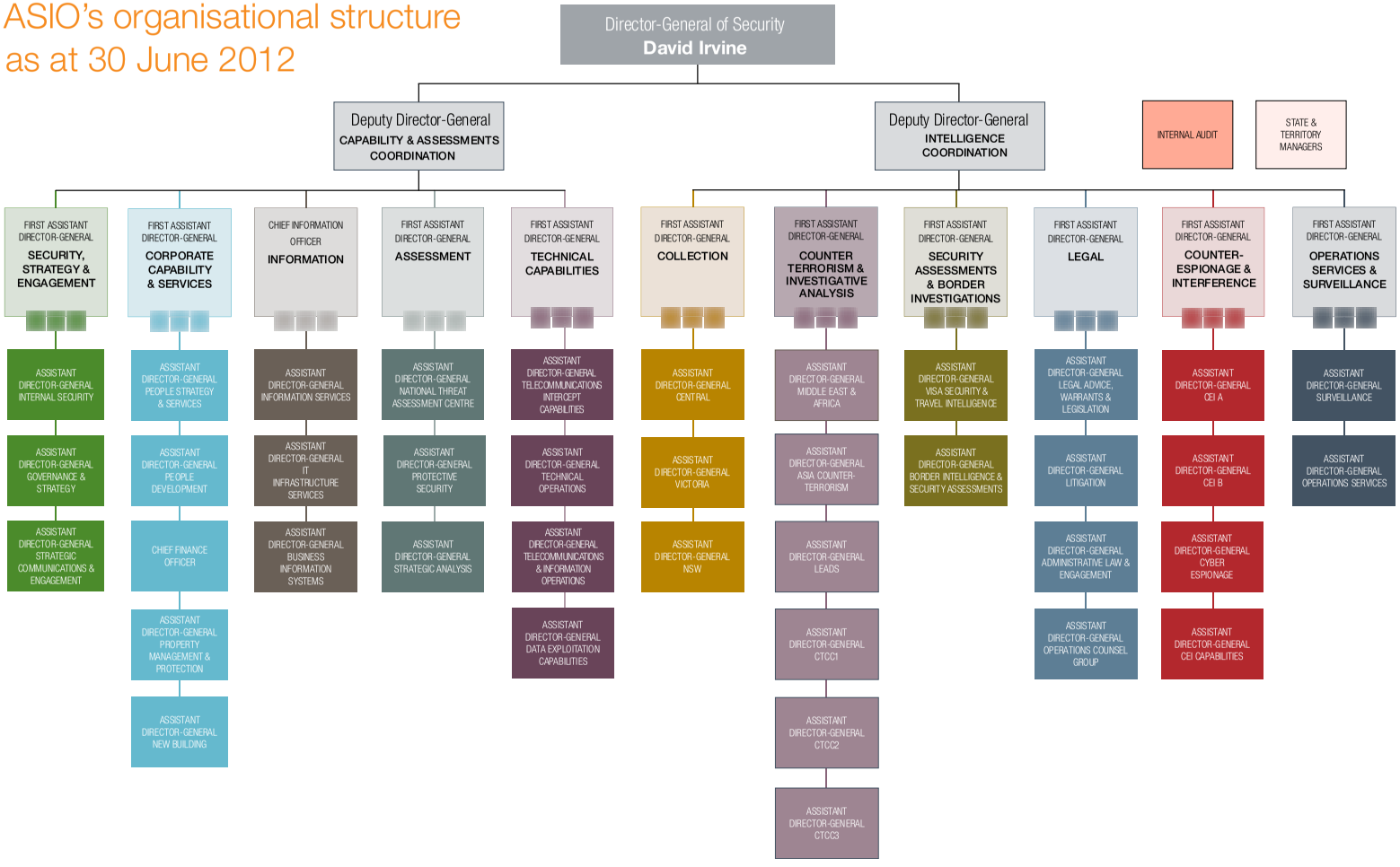
- Deputy Director-General, Corporate and Strategy, changed to Deputy Director-General, Capability and Assessments Coordination; and
- Deputy-Director General, Operations and Assessments, changed to Deputy Director-General, Intelligence Coordination.

Changes to structure and responsibilities have resulted in a re-alignment of divisions and branches to promote more effective security intelligence capability and increase integration and collaboration.

In October 2011, Ms Kerri Hartland joined ASIO on secondment as Deputy Director-General Corporate and Strategy. As one of two publicly identified ASIO officers, the other being the Director-General, Ms Hartland participated in a number of public appearances on behalf of the Organisation, including Senate and Budget Estimates, and public addresses.

Ms Kerri Hartland
Deputy Director-General, Capability and Assessments Coordination

ASIO's organisational structure as at 30 June 2012



Part 1

The security environment 2011–12 and outlook

"Australia's security environment is inextricably linked to, and influenced by, the overseas environment."

The Director-General of Security, Security in Government Conference
26 July 2011

Terrorism

Australia is a terrorist target. The challenge of terrorism is real and persistent, with the greatest threat continuing to be terrorism motivated by a violent jihadist ideology. Australian interests and Australian people overseas have been deliberately and actively targeted by terrorists. Over the past decade, we have seen individuals involved in four significant terrorist plots in Australia convicted and jailed. Others have been disrupted at earlier points (including prevention of travelling overseas to conduct terrorist activities) and some Australians have been involved in terrorism activities overseas. Overseas influences, including through the internet, will continue to inspire some Australians to terrorism and drive their commitment.

Over the past twelve months, al-Qa'ida and its affiliates have suffered a number of setbacks including the loss of senior figures, Anwar al-Aulaqi, in Yemen, and Abu Yahya al-Libi, in Pakistan. The continuing counter-terrorism efforts of Australia's partners in South-East Asia are also having an effect on regional extremist networks, although terrorist threats persist.

However, these and other setbacks have not lessened the intent of violent jihadist groups to promote, foster and engage in terrorism. Jihadist succession planning has demonstrated their resilience to the inevitable losses of individual leaders. The global tempo of terrorist activities, including attacks, attempted attacks, plotting, fundraising and recruitment, remains undiminished.

In addition, new terrorist groups continue to emerge in the Middle-East and Africa, such as Boko Haram in Nigeria. Attacks targeting the West remain a priority, but the threat they pose is now defined as much by regional, domestic or local issues as by al-Qa'ida's global agenda. ASIO must maintain a comprehensive understanding of these regions in order to consider and advise on the threat to Australia, Australians and Australian interests overseas.

The basic drivers and inspirations that underpin this violent ideology continue to resonate with individuals, in Australia. Individuals who seek to engage in violence in Australia or attempt to travel overseas to train and fight are priorities for ASIO and law enforcement investigations. Favoured destinations overseas are Lebanon, Yemen, Somalia, Afghanistan and Pakistan. Australians who are currently training or fighting overseas may also return to Australia to engage in terrorism, use their knowledge of Australia to help others plan an attack, or engage in terrorism overseas.

The internet is an important vector for radicalising individuals to extremism and connecting them with extremists. It enables access to and the sharing of voluminous amounts of violent extremist ideology and propaganda, instruction on how and what to attack, authorisation of violence and the results of terrorist violence. English-language material targets a Western audience and is increasingly available, as are translations of material that deceased terrorist leaders and ideologues have left behind. This material will contribute to the radicalisation of individuals and groups in Australia now and into the future. This literature of violence indicates that Australia remains a target for violent extremist jihad.

There remains an aspiration for large-scale, centrally coordinated 9/11-style attacks, but the promotion of stand-alone, unilateral attacks by individuals or small independent groups has increased. Propagandists are specifically targeting an English-speaking audience, encouraging them to act using whatever means are at their disposal without seeking any further sanction. Individuals are capable of undertaking significant acts of violence, whether as 'lone actors' acting on their own belief system (for example, the attacks in Norway by Anders Breivik in July 2011) or as 'standalones' motivated by an existing extremist narrative (such as in the case of Mohammed Merah in France, in March 2012).

Communal violence and violent protest

Many of the specific tensions and national issues from around the world have the potential to be reflected in Australia. For example the situation in Syria, with the potential for violence spilling into other parts of the Middle-East, increases the possibility of associated communal violence in Australia and remain a concern for ASIO. There are a small number of people actively promoting hatred and inter-communal violence in Australia.

Over the past year, there have been a number of protests which have involved the use of violence. Some of these protests resulted in media coverage and public interest, including a demonstration and subsequent intrusion into the Syrian Embassy in Canberra.

While far right nationalist and racist groups continue to operate within Australia, the majority do not advocate the use of violence to achieve their objectives. Rather, the groups tend to participate in activities aimed at furthering their message, including lawful political advocacy, concerts, festivals and protests.

Over the reporting period, the rise in right wing extremism in parts of Europe was not reflected, nor did it gain large-scale support, in Australia. Regardless, ASIO remains alert to any foundation or support for extremist ideologies that could result in extremist right wing groups, or lone actors, engaging in acts of violence.

Protest activity on issues of national and international significance is unlikely to diminish and there are likely to be elements within society who attempt to manipulate or escalate peaceful protest situations into violence. In some cases, this has included the use of provocative and covert tactics. Fortunately, the number of people involved and the scale of violent protest activity in Australia have been relatively low. It is ASIO's responsibility to provide advice to government and law enforcement partners on the potential for such violence. This advice generally takes the form of ASIO Threat Assessments.

Espionage

Espionage is an enduring and first-order threat to Australia's security. Emerging technology and an internet-connected world offer new avenues of espionage. The espionage threat is evidenced by foreign intelligence services seeking agents in relevant positions, including in the Australian Public Service and working for Australian businesses, but also seeking access to any computer system or network holding data that could be targeted for espionage activity.

Cyber espionage remains an ongoing significant concern to ASIO and is likely to remain so in the future. The rapidly changing technological environment poses real challenges in ensuring the Organisation, along with our partner agencies, is able to identify and respond to attempts at attacking or infiltrating systems holding sensitive information. In 2011–12, cyber espionage targeting Australian interests continued from both state and non-state actors. ASIO works closely with domestic partners, including as a participant in the Cyber Security Operations Centre, to mitigate or prevent any risk to Australia's security emanating from cyber espionage.

During the reporting period, ASIO continued to contribute to increased awareness among government agencies and Australian business of the scale and magnitude of the threat and the implications of espionage activity. While ASIO continues to investigate and, where appropriate, disrupt espionage threats to Australia's security, an important part of the Organisation's efforts has been raising awareness and advice on security practice. This work is conducted in close collaboration with the Attorney-General's Department and the Defence Signals Directorate.

Proliferation

Under various international treaties and United Nations Security Council resolutions, Australia has obligations to prevent the spread of weapons of mass destruction (WMD) capabilities. Throughout the reporting period, ASIO continued efforts in countering the procurement, primarily in Australia, of equipment, materials, services, technology and training that could be used by state and non-state actors for the proliferation of WMDs.

Border integrity

People-smuggling efforts continued to undermine Australia's border integrity and, under the ASIO Act, this requires a response from ASIO. This predominantly takes the form of security assessments of irregular maritime arrivals and investigations into people smuggling activities within Australia.

Part 2

Program performance

"Let Australians get on with their lives, alert but not paranoid with fear, and let the government get on with the business of providing appropriate security measures and security monitoring—without the need to go overboard."

The Director-General of Security, address to the Sydney Institute
24 January 2012

ASIO is responsible for the protection of Australia, its people and its interests from threats to security. This occurs through intelligence collection, assessment and advice to government.

The four programs relevant to ASIO performance are:

- Program 1 – Security intelligence analysis and advice
- Program 2 – Protective security advice
- Program 3 – Security intelligence investigations
- Program 4 – Investigative, analytical and operational capability

Performance of these programs is measured by ASIO on a quarterly basis and by the annual Stakeholder Satisfaction Survey.

- ASIO's performance statement is highly classified and is redacted from the ASIO annual report for reasons of national security.
- ASIO conducts an annual Stakeholder Satisfaction Survey with key government partners to ensure ASIO receives direct feedback on the level of satisfaction with engagement with ASIO, the quality of advice and product (including the timeliness, accuracy, completeness and relevance), and ASIO's overall performance in meeting stakeholder requirements. Details on the ASIO Stakeholder Satisfaction Survey are available at 56 page.

Program 1

Security intelligence analysis and advice informs stakeholders of ASIO's work in countering terrorism, espionage and other threats to national security, and is relevant and actionable.

- Strategic assessment and advice
- Threat assessment and advice
- Critical infrastructure protection and advice
- Cyber-security advice
- Advice on chemical, biological, radiological, nuclear and explosive weaponry
- Advice for special events
- Proscription-related advice
- Intelligence reporting
- Security assessment advice
- Support to prosecutions

Security intelligence analysis and advice

"We are required to make careful judgements and choices on priorities, risk management, and resources."

The Director-General of Security, Security in Government Conference 26 July 2011

Strategic assessment and advice

ASIO's strategic and thematic assessments support Australian Government and partner agencies by providing insight and context to significant developments in our security environment. ASIO advice also provides foresight of emerging and future security challenges. Within ASIO, this work is essential if we are to respond to contemporary threats and anticipate the shifts and changes in the security challenges Australia will face into the future.

ASIO intelligence assessments distil complex issues down to 'what it all means' for our diverse readers. They inform policy settings, capability development, security measures, interventions to prevent and mitigate harm and opportunities to shape the security environment.

Performance 2011–12

ASIO produced a range of strategic assessments providing views on the implications of the Arab Spring, the riots in the United Kingdom, the death of Anwar al-Aulaqi, terrorism trends and other topics. The analysis integrated work from Australian national security community agencies and drew on engagement with international partners. We continued to provide support to the Attorney-General's Department in relation to countering violent extremism.

Threat assessment and advice

A threat assessment addresses the nature of a security threat to people, places, events and interests. It specifically addresses the intent and capability of groups or individuals to cause harm to Australia, Australians or Australian interests, both within Australia and globally. Threat assessments do not advise on specific protective security measures; rather, they inform risk mitigation strategies.

The National Threat Assessment Centre (NTAC) within ASIO is responsible for the provision of threat assessment advice to the Australian state and territory governments, international intelligence partners and relevant industry stakeholders. NTAC draws on a broad range of intelligence and open sources of information in developing its threat assessments.

NTAC threat assessments are one of the sources of advice used by the Department of Foreign Affairs and Trade in preparing its travel advice for Australians. They also inform the protective security measures applied to holders of high office or to physical facilities.

NTAC is staffed by ASIO officers and officers seconded from the national security community. Those working in NTAC retain access to their own agency and are able to draw on the resources of those agencies to inform NTAC's threat assessment work. In addition to ASIO officers, NTAC draws officers from the:

- Australian Federal Police;
- Australian Secret Intelligence Service;
- Defence Signals Directorate;
- Defence Intelligence Organisation;
- Department of Foreign Affairs and Trade;
- New South Wales Police;
- Department of Infrastructure and Transport; and
- Office of National Assessments.

Performance 2011–12

In 2011–12 NTAC produced 593 assessments, compared with 575 products in the previous reporting period.

The 2011 Commonwealth Heads of Government Meeting in Perth and the visits by Her Majesty the Queen and the President of the United States of America (USA) were a particular focus for NTAC. The lead-up to the London Olympics also required specific consideration by NTAC.

Over the reporting period NTAC also produced assessments relevant to the global security environment following the Arab Spring. These provided advice pertaining to the threat to Australian interests within Australia and overseas, and to foreign interests in Australia.

Business Liaison Unit

The ASIO Business Liaison Unit (BLU) was established to bridge the gap between ASIO providing advice to government and the need for private industry to receive advice. Information relevant to the security of Australia and its interests is available via subscription to the BLU website. Subscription is free and grants access to many assessments on the current security environment and information on ways to mitigate threats to security. Reports are necessarily unclassified and allow Australian businesses to consider their own security position and potential matters impacting the security of their companies.

Critical infrastructure protection advice

The term 'critical infrastructure' is used to define assets which, if unavailable for an extended period, would impact significantly on the economic or social wellbeing of Australia; examples include banking and finance, communications or health infrastructure. ASIO provides assessments of the potential terrorist threat to a variety of critical infrastructure in order to identify and address vulnerabilities and inform risk mitigation strategies. ASIO also undertakes engagement campaigns with relevant industry stakeholders to inform them of the threats.

Critical infrastructure by its very nature poses a potential target for those who wish to do harm to Australia and so careful consideration must be given to matters having an impact on the security of critical infrastructure. No single element of critical infrastructure stands alone and the potential for threats against auxiliary assets must also be considered.

Assessments on critical infrastructure are provided to Australian state and territory governments and to relevant industry stakeholders to inform policy and protective security measures.

Performance 2011–12

Over the reporting period ASIO provided 25 briefing sessions on potential or specific threats to critical infrastructure and produced 22 critical infrastructure reports. These reached over 153 government and private sector stakeholders.

In 2011–12 BLU published 43 reports to a broad audience.

Owners and operators of critical infrastructure also access up-to-date reporting via the BLU website, (www.blu.asio.gov.au).

Cyber-security advice

ASIO provides threat advice to government and the private sector regarding cyber-espionage. ASIO's advice seeks to contextualise cyber-threats in the broader security landscape. An understanding of the context within which cyber-espionage occurs is essential to developing a considered approach to security. ASIO's advice is informed by a variety of sources, including ASIO's own investigations, international intelligence partners and domestic agencies, such as the Defence Signals Directorate (DSD) and the Attorney-General's Department.

Performance 2011–12

ASIO works closely and cooperatively with domestic and international agencies and with industry on matters pertaining to cyber-security. In March 2012 the Attorney-General announced the establishment of the Australian arm of the Council of Registered Ethical Security Testers (CREST). CREST Australia is the product of coordinated engagement with industry involving ASIO, CERT Australia and DSD and will have an important role in establishing clear and agreed standards for cyber-security testing. These standards will help the business sector to be confident that the work conducted by CREST-accredited IT professionals is completed with integrity, accountability and to agreed standards.

CREST Australia is affiliated with CREST Great Britain, further reinforcing Australia's international relationships on matters of cyber-security.

ASIO's representation within the Cyber Security Operations Centre continues to galvanise key relationships with DSD, CERT Australia and the Australian Federal Police (AFP). Over the reporting period, ASIO continued to work with Australian and international partners to increase Australia's capability to identify and counter cyber-espionage targeting Australia and its interests. ASIO also supported the development of Australia's whole-of-nation cyber security policy with specialised reporting and advice.

Advice on chemical, biological, radiological, nuclear and explosive weaponry

ASIO provides specialist intelligence advice to government and the private sector on weaponry used by extremists, both in Australia and overseas. ASIO maintains specialist knowledge on explosives and weaponry, including chemical, biological, radiological and nuclear (CBRN) weaponry. This is enhanced through national, international and industry partnerships—particularly with Defence Intelligence Organisation and its insight from defence-related scientific and technical expertise.

ASIO's advice assists in the development of policy and regulations applicable to relevant sectors. It also gives insight into key indicators of individuals or groups attempting to acquire, develop or use weaponry, including the acquisition of precursor chemicals and components—increasing the likelihood of proactive detection and reporting of groups or individuals attempting to acquire goods for the purposes of conducting a terrorist act.

Within ASIO, such specialist intelligence advice further strengthens our capability to identify, investigate and assess threats involving terrorist weaponry.

Performance 2011–12

Over the reporting period ASIO provided 22 reports to domestic stakeholders and international partners, and presented 16 tailored presentations, addressing threats and trends in extremists' use of weaponry, explosives and CBRN agents.

Advice for special events

ASIO's contribution to the security of special events, both domestic and international, has grown in recent years, as events which draw large crowds and high-profile attendees or have particular media attention might be considered high-value targets for extremists.

Domestically, ASIO works closely with the Australian Government, and state and territory law enforcement agencies to coordinate security intelligence surrounding an event to ensure a seamless flow of advice to governments and event organisers.

For large-scale international events, ASIO provides security intelligence advice for the protection of Australians and Australian interests overseas. This includes, but is not limited to, National Threat Assessment Centre threat assessment advice.

Performance 2011–12

ASIO provided security intelligence support for a number of special events during the reporting period, including the:

- Rugby World Cup in New Zealand, September–October 2011;
- Royal visit to Australia by Her Majesty Queen Elizabeth II, October 2011;
- Commonwealth Heads of Government Meeting (CHOGM), Perth, October 2011;
- Asia-Pacific Economic Cooperation forum in the USA, November 2011;
- Visit to Australia by the President of the USA, November 2011;
- East Asia Summit in Indonesia, November 2011;
- Annual ANZAC Day commemorations in Turkey and France, April 2012; and
- NATO – International Security Assistance Force summit in the USA, May 2012.

Culminating in October 2011, ASIO provided significant security intelligence support for CHOGM, held in Perth. The event was opened by Her Majesty Queen Elizabeth II as the climax of a broader royal visit to Australia and was attended by heads of government, foreign ministers and official delegates from over 50 Commonwealth countries.

ASIO's contribution to the planning and delivery of security for CHOGM 2011 spanned a period from 2009 to 2012. ASIO activity over the period included intelligence collection support, the publication of an extensive body of threat assessments and country reports, the provision of protective security advice to the event organiser (CHOGM 2011 Taskforce) and security checking of persons requiring accreditation for access to the event. Throughout, ASIO worked closely with both Commonwealth and Western Australian law enforcement agencies and other relevant authorities.

For the Rugby World Cup in New Zealand in September–October 2011, ASIO worked closely with New Zealand counterparts to support security planning and intelligence functions implemented for the event.

ASIO also assigned significant resources to support the security of the London 2012 Olympic and Paralympic Games, held from 27 July to 9 September 2012. A significant element of ASIO's response to this event involved working closely with British authorities in the planning and implementation of security for the event.

Security planning is now underway for Australia's hosting of the G20 leaders summit in 2014, the Asian Football Confederation Asian Cup and the Cricket World Cup both in 2015, and ANZAC centenary commemorations 2014–18.

Proscription-related advice

The proscribing of a group as a terrorist organisation under the *Criminal Code Act 1995* is a powerful tool which can be used to deter support to groups undertaking terrorist activities. ASIO provides advice against the criteria specified in the Criminal Code as to why a group may be considered for proscription by the Attorney-General.

Once an organisation is listed under the proscription framework, a number of offences will apply to membership or support of the listed organisation. The duration of a listing spans three years at which time it is reviewed against the criteria in the Criminal Code. Under the Criminal Code, the Parliamentary Joint Committee on Intelligence and Security may review the listing of organisations as terrorist organisations.

ASIO's security intelligence collection activities are not restricted to proscribed terrorist organisations.

Performance 2011–12

ASIO provided advice on 10 terrorist groups for consideration in the proscription process.

Groups proscribed, re-listed and delisted in Australia in 2011–12

Over the reporting period five organisations were re-listed and two were de-listed. No new groups were listed. As at 30 June 2012, 17 organisations were officially listed (ref page 128).

Intelligence reporting

As both a collector and assessor of security intelligence, ASIO is uniquely placed to provide a range of reporting, assessment and advice to domestic stakeholders and foreign partners. ASIO strives to provide reporting in forms that best meet customer needs and to facilitate this has developed a range of easily identifiable product and a program of ongoing customer engagement. Most reporting is necessarily classified. ASIO's line of published product includes:

- ASIO analytical reports (AAR): contain security intelligence, strategic and thematic analysis and assessment. AARs also provide strategic context on issues of current or emerging security concern and provide background on current investigative cases. Detailed or complex analysis is supported in a range of ways, including by tailored briefs or visual representation of data.
- ASIO threat assessments (ATA): generally produced by the National Threat Assessment Centre (NTAC), ATAs contain assessments of threats to Australia's domestic and overseas interests; threats to foreign interests in Australia; threats from terrorism, politically motivated violence and foreign intelligence services, and threats to special events. ATAs might be written to fulfill a specific advice requirement or in response to a line of reporting which indicates a change to the security environment.
- ASIO intelligence reports (AIR): contain single-source, unassessed intelligence, including incidental foreign intelligence, obtained through our security intelligence activities. The format recognises that ASIO's security intelligence operations occasionally generate unique intelligence that addresses the information requirements of other assessment, policy and operational agencies.
- Research and monitoring reports (RMR): provide a summation of all source reporting on a specific topic or area. These are particularly helpful in supporting considered analysis on matters of security interest.

Performance 2011–12

In 2011–12, ASIO produced 3,000 products, which were shared with over 350 partners in Australia and overseas. To ensure ASIO products are useful and meet the needs of clients, ASIO maintains a rolling program of direct engagement to facilitate the provision of feedback on ASIO reporting. All ASIO products offer readers the opportunity to provide feedback through a variety of mechanisms. During the reporting period, ASIO received more than 350 pieces of feedback relating to the usefulness, timeliness and quality of ASIO reporting, over 98 per cent of which was positive.

Security assessment advice

ASIO's security assessments are an important component of Australia's national security defences. They are a mechanism for providing security advice to inform certain government decision-making processes such as the granting of visas or the granting of access to sensitive government information. Security assessments can range from a simple check of personal details against ASIO's intelligence holdings to an in-depth intelligence investigation. The ASIO Act prescribes that ASIO security assessment advice may be in the form of either non-prejudicial advice, a qualified security assessment or an adverse security assessment.

Passports

The ability of the Australian Government to cancel or refuse to issue an Australian passport is a key measure in support of the security of Australia. Australia takes seriously its obligations to the international community to act in the prevention of Australian's participating in terrorist attacks overseas. The legal foundations for this action are in the *Australian Passports Act 2005* and the *Foreign Passports (Law Enforcement and Security) Act 2005*.

Citizenship

ASIO may also issue security assessments in relation to applications for Australian citizenship under the *Australian Citizenship Act 2007*. In 2011–12 ASIO issued one adverse security assessment in relation to a citizenship application, as a result of which the Minister for Immigration and Citizenship refused the application.

Visa security assessments

ASIO conducts security assessments of individuals, including irregular maritime arrivals (IMAs) in relation to permanent, temporary and protection visas. This process is used to identify individuals who pose a risk to the security of Australia.

Irregular maritime arrivals

In March 2011 ASIO commenced operation of a streamlined security assessment framework for IMAs which enabled ASIO to focus resources on cases requiring complex intelligence investigation. The 2011–12 period marks the first full year that this process has been operating.

ASIO continues to identify individuals of security concern. Since 2009, ASIO has issued 63 adverse security assessments in relation to IMAs. The majority of those adverse security assessments have been issued in relation to politically motivated violence.

On 25 June 2012 the Australian National Audit Office (ANAO) tabled in parliament its audit on the Security Assessment of Individuals.[1] The aim of the audit was to assess the effectiveness and timeliness of ASIO's security assessments, and is the first ANAO audit to focus primarily on ASIO.

The audit found ASIO staff were well-trained and followed clearly defined procedures in conducting security assessments and that ASIO was 100 per cent compliant in all cases reviewed (over 400). The report made four recommendations in relation to specific operational issues, to which ASIO has agreed.

Further information relevant to the audit can be found on page 50.

Counter-terrorism security assessments

Counter-terrorism security assessments are conducted to assess the suitability of a person on counter-terrorism grounds to access areas or materials that are restricted, such as Australia's air and maritime ports, other security sensitive facilities, access to dangerous goods or accreditation to special events. Requests for counter-terrorism security assessments are received by ASIO from AusCheck and the Australian Federal Police, with the vast majority requested by AusCheck for aviation and maritime security identification cards.

In 2011–12, ASIO completed 153,644 counter-terrorism security assessments, a 40 per cent increase on those completed for 2010–11. No adverse or qualified counter-terrorism security assessments were issued in 2011–12.

[1] ANAO, 2012. *Security Assessment of Individuals.*[online] Available at:<www.anao.gov.au/publications/auditreports>

Personnel security assessments

Personnel security assessments are conducted to assess the suitability of a person to have access to Australian Government information or areas to which access is restricted on security grounds. As a requirement of the Protective Security Policy Framework, Commonwealth agencies are required to seek an ASIO security assessment for Negative Vetting 1 & 2 and Top Secret Positive Vetting level security clearances.

In addition, ASIO also provides personnel security assessments relating to baseline level clearances where there is an identified issue of possible security concern. ASIO can provide personnel security assessment advice regarding persons who may not have security clearances but who otherwise have access to Australian Government information or areas to which access is restricted on security grounds.

Since its establishment in late 2010, the Australian Government Security Vetting Agency (AGSVA) has taken responsibility for security clearance vetting for Commonwealth agencies, except for a small number of exempt agencies (of which ASIO is one). ASIO therefore receives the vast majority of personnel security assessment requests from AGSVA, with the remainder received directly from the AGSVA-exempt agencies.

In 2011–12, ASIO issued one qualified and five adverse personnel security assessments. During the same period ASIO produced 21 security intelligence country threat assessments. These assessments are required when an agency is seeking a waiver for a security-cleared, non-Australian citizen to access security classified resources originating from a third country.

Performance in 2011–12

Visa security assessments

Type of entry	Number of assessments completed 2010–11	Number of assessments completed 2011–12
Temporary visas	16,223	**12,623**
Permanent residence	11,724	**5,708**
Onshore protection	957	**319**
Offshore refugee/humanitarian	1,906	**687**
IMAs	3,586	**4,760**
Total	34,396	**24,097**

The reduction in the number of visa security assessments reflects a drop in the number of referrals, from an improved referral process targeting high-risk categories. The referral framework is an intelligence-led, risk-managed system that ensures ASIO can focus more closely on cases that require an intelligence investigation.

Counter-terrorism security assessments

Type of access	Assessments completed 2010–11	Assessments completed 2011–12
Aviation Security Identification Card (ASIC)	67,501	**85,939**
Maritime Security Identification Card (MSIC)	30,421	**52,373**
Dangerous goods (ammonium nitrate/ explosives)	9,101	**9,852**
Australian Nuclear Science and Technology Organisation (ANSTO)	1,274	**1,829**
Special events	666	**3,301**
Flight crew	203	**202**
National health security	N/A	**148**
Total	109,166	**153,644**

The increase in the number of counter-terrorism security checks is, in large part, due to MSIC assessments being reviewed every two years. CHOGM resulted in an increase of special events security assessments.

Personnel security assessments

Type of access	Assessments completed 2010–11	Assessments completed 2011–12
Top Secret Positive Vetting	3,100	**2,172**
Negative Vetting Level 2	7,512	**7,070**
Negative Vetting Level 1	20,487	**18,542**
Other	N/A	**17**
Total	31,099	**27,801**

Litigation, including support to prosecutions

In 2011–12, ASIO was involved in over 58 litigation matters, including criminal (in particular, terrorism) prosecutions and judicial and administrative review of security assessments. The volume of litigation involving ASIO remained high, producing a significant workload.

Performance in 2011–12

Four of the men convicted in the operation Pendennis proceedings in Melbourne in 2008 faced further charges of conspiracy to do an act in preparation for, or planning, a terrorist act. On 1 July 2011, following extensive litigation in the Supreme Court of Victoria and the Victorian Court of Criminal Appeal, the Supreme Court permanently stayed these charges as 'oppressive'.

On 16 December 2011, the three men convicted of conspiring to undertake acts in preparation for a terrorist act—planning an armed assault on Australian Defence Force personnel at Holsworthy Barracks—were each sentenced to 18 years imprisonment with a non-parole period of 13 years and 6 months. All three have applied to appeal their sentences. The Commonwealth Director of Public Prosecutions has applied to appeal the sentences as manifestly inadequate.

On 3 March 2012 the High Court heard an appeal against the New South Wales Court of Criminal Appeal's overturning of Belal Khazaal's conviction for making a document in connection with a terrorist act. As at the end of 2011–12, the High Court's decision was reserved.

During 2011–12, the Administrative Appeals Tribunal heard three challenges to adverse security assessments, affirming one and reserving its decisions on the remaining two. In July 2011, an irregular maritime arrival applied to the Federal Court for review of an adverse security assessment issued in 2009, alleging denial of procedural fairness. The Director-General of Security decided that changed circumstances warranted a review of the assessment and the applicant discontinued. A new adverse security assessment was issued in May 2012. The applicant challenged the procedural fairness in which this security assessment was reached, along with the indefinite nature of the consequent immigration detention, in the High Court. The High Court heard the matter on 18, 19 and 21 June 2012 and reserved its judgement.

Program 2

Protective security advice enhances physical, technical, procedural, personnel and information security.

- Protective security risk reviews
- Top secret certifications
- Technical surveillance counter measures
- Security equipment evaluation
- Protective security training
- Protective security policy framework

Protective security advice

Protective security risk reviews

ASIO's T4 section provides protective security risk reviews (PSRR) and vulnerability assessments for government and the private sector. These reports examine physical, information, administration and personnel security risks.

The Council of Australian Governments (COAG) has accepted a recommendation from the National Counter Terrorism Committee that T4 undertake PSRRs every two years on Australian Government vital critical infrastructure assets. These PSRRs make recommendations relating to operational security, consistent with government policy requirements. They are aimed at mitigating security risks and vulnerabilities.

T4 utilises security intelligence from ASIO's domestic and international intelligence sources and engages with foreign partners on sensitive technical matters. T4 works closely with ASIO's Critical Infrastructure Protection Directorate and NTAC, and uses their threat assessments to inform its protective security recommendations for government and private assets. T4 also participates in international security forums to share information on protective security practices and technology and to inform its approach to the security environment in Australia.

Performance 2011–12

In 2011–12, T4 completed four PSRRs and/or vulnerability assessments, focusing predominantly on nationally vital critical infrastructure assets. T4 also provided protective security advice on some of the venues which hosted the Commonwealth Heads of Government Meeting in October 2011, in Perth.

Top secret certifications

ASIO is the nominated authority for the physical security certification for a facility to hold Top Secret security-classified information, including the ability to hold discussions at the Top Secret level. Re-certification takes place every five years.

Government and private sector agencies that provide direct support to government functions at the Top Secret level are assessed for suitability to receive certification. This is conducted against a risk management framework, identifying areas where the compromise or loss of information would have a catastrophic impact.

Performance 2011–12

T4 undertook the certification of 42 sites in 2011–2012. This is an increase from 28 sites in 2010–11.

Technical surveillance counter-measures

Technical surveillance counter-measures (TSCM) are a means to detect surveillance by technical means, such as listening devices.

In order to ensure that highly classified or sensitive discussions are not compromised through technical means (for instance, listening devices), T4 provides TSCM advice and assistance to Australian Government departments and agencies.

T4 also participates in an inter-agency TSCM working group in providing a coordinated approach to TSCM work across government. The group's focus includes improving training opportunities, information sharing on equipment and techniques, and developing uniform standards and competency levels across agencies.

Performance 2011–12

For reasons of national security the outcomes of this activity are not detailed in this report.

Security equipment evaluation

T4 has an ongoing program of testing and evaluating physical security products and equipment such as alarms and locks. This testing ensures that products are suitable for use in Australian Government facilities, meet manufacturers' claims and identify clearly specific applications and limitations. From this program an extensive list of equipment is produced for use by government security managers and consultants.

T4 also provides engineering advice to the Australian Government on the suitability of a range of technologies. In order to keep abreast of changes in technology and ensure it remains at the forefront of evaluation methodology, ASIO continues to engage with security specialists in Australia and overseas.

Performance 2011–12

In 2011–12, ASIO completed 29 security equipment evaluations, three locksmith evaluation courses, three container maintenance courses and nine classified waste evaluations.

In 2011, ASIO recommended the suspension of the Security Construction and Equipment Committee (SCEC) security equipment testing program for a period of 12 months. The program suspension allowed ASIO to redesign the program to align better with government protective security priorities and to gradually replace the Security Equipment Catalogue with the Security Equipment Evaluated Product List by 2014. The SEEPL will be limited to those security products assessed as meeting the requirements for specialised high security or administrative security categories.

The program for evaluating security equipment was reopened in July this year. The program, which aligns with the Australian Government's Protective Security Policy Framework, focuses on priority product categories that have been identified by the Australian Government and endorsed by the Protective Security Policy Committee.

Protective security training

T4 conducts a range of training courses in protective security, including for security advisers and other security personnel from Australian Government agencies.

This training equips participants with the skills and knowledge required to manage the security responsibilities of their respective agencies.

T4 also trains SCEC-endorsed security zone consultants—who assist with establishing appropriate physical security environments for the protection of official information and assets—and locksmiths to work with SCEC-endorsed security containers and locks.

Performance 2011–12

In 2011–12, T4 delivered four agency security adviser courses and three training courses for the Attorney-General's Department's Protective Security Training Centre.

Protective security policy framework

ASIO makes a significant contribution to whole-of-government protective security policy development through the Protective Security Policy Committee and the Inter-Agency Security Forum.

Through these forums, in 2011–12 ASIO continued to provide advice and guidance to inform the Protective Security Policy Framework.

Program 3

Security intelligence investigations fulfil intelligence collection requirements through all-source security intelligence collection; complex tactical investigations; analysis; and engagement with national and international partners.

- Counter-terrorism investigations
- Counter-espionage investigations
- Foreign interference investigations
- Violent protest and communal violence investigations
- Border integrity
- Counter proliferation

Security intelligence investigations

"ASIO is continuing to conduct literally hundreds of investigations of possible terrorist intentions or activities in Australia."

The Director-General of Security, Security in Government Conference SES Breakfast 5 July 2011

Counter-terrorism investigations

ASIO operational and analytical officers investigate threats to Australia from terrorism. The investigations of these threats include terrorism within Australia and the terrorist threat to Australians and Australian interests abroad. In undertaking investigations ASIO also provides advice to government and other agencies as part of ASIO's risk mitigation strategies. This includes operations to disrupt activity and can include referrals to law enforcement partners.

The terrorist threat to Australia and Australian interests is real and persistent. It involves people based in Australia either directly engaged in, or providing support to, terrorist activities. Over the reporting period, changes in the global security environment had a direct impact on the operational tempo of ASIO investigations. Ongoing theatres of war, particularly Afghanistan, continued to be a source of ideological motivation for Australia-based extremists. Regional instability, especially in Lebanon, Syria, Somalia and Yemen, continues to attract Australians who wish to engage in violent conflict.

Performance 2011–12

ASIO reports its performance of counter-terrorism investigations in the classified Part 3 component of its annual report.

Counter Terrorism Control Centre

The Counter Terrorism Control Centre (CTCC) was established in ASIO in 2010 to ensure high-level collaboration and cooperation in setting and managing counter-terrorism priorities for Australia's counter-terrorism community, the evaluation of agency performance against those requirements and the effective collection and distribution of counter-terrorism information.

Over the reporting period the CTCC created a standardised framework for evaluating the performance of members of the Australian intelligence community. This framework is scheduled to be implemented over the next reporting period and will allow the CTCC to bilaterally evaluate agencies' performance against set target areas.

Counter-espionage investigations

ASIO works to identify and investigate acts of espionage, or attempted espionage, against Australian interests. In doing so ASIO provides advice to government and industry stakeholders on the harm caused by espionage and the ways and means to mitigate this risk.

"Despite the rise in cyber-espionage, ASIO has not seen a reduction in the intensity of other, more traditional, forms of espionage."

The Director-General of Security, Security in Government Conference 26 July 2011

Espionage activities against Australian interests pose an enduring and first-order threat and have the potential to damage Australia's security, including defence, intelligence, scientific and technical capabilities, trade and economy, and international relations. Espionage may pose a threat to the welfare of individual Australians through coercion or threatened violence.

The prevalence of espionage against Australian interests continues to be of security concern. Traditional forms of espionage remain relevant and are often employed in concert with more technical means. Espionage is not limited to government institutions, with a large array of private sector information vulnerabilities also being exploited. The damage caused by espionage to Australia is difficult to quantify as the nature of the threat is one that has the potential to go unnoticed until significant damage is sustained.

Performance 2011–12

ASIO reports its performance of counter-espionage investigations in the classified Part 3 component of its annual report.

Over the reporting period, ASIO conducted an expansive outreach and security awareness campaign across both government and private sectors. This has been instrumental in counter-espionage measures being considered and applied by individual organisations and industry stakeholders and has enabled more proactive reporting of instances of suspected espionage.

In 2011–12 ASIO continued to develop its investigative and operational capacity and enhance government and industry awareness of cyber-security threats. ASIO's ongoing work with the DSD-hosted Cyber Secrity Operations Centre has contributed to the coordination of operational responses to cyber-security threats.

Contact Reporting Scheme

Traditional forms of espionage often include unusual contact of a suspicious nature with foreign nationals. The identification and reporting of such behaviour is one way to mitigate this espionage threat. As such, ASIO's promotion and ongoing maintenance of the Contact Reporting Scheme continued over the reporting period.

Foreign interference investigations

Acts of foreign interference are defined in the ASIO Act as 'activities relating to Australia that are carried on by or on behalf of, are directed or subsidised by or are undertaken in active collaboration with, a foreign power, being activities that:

- are clandestine or deceptive and;
  - (i) are carried on for intelligence purposes;
  - (ii) are carried on for the purpose of affecting political or governmental processes; or
  - (iii) are otherwise detrimental to the interests of Australia; or
- involve a threat to any person.'

Performance 2011–12

ASIO reports its performance on foreign interference investigations in the classified Part 3 component of its annual report.

Violent protest and communal violence investigations

The right to engage in lawful dissent is protected in Australia, including by the ASIO Act. Section 17A of the ASIO Act clearly states that 'the Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent, and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly'.

However, ASIO has a responsibility to investigate individuals actively seeking to engage in violent protest.

The promotion of communal violence—being the promotion of violence between different groups in the Australian community—was also the subject of ASIO investigation over the reporting period.

ASIO uses the collection and analysis of intelligence to identify those who seek to engage in violent protest activity or to promote violence between communities within Australia. Investigations and analysis of the potential for violent protest or communal violence is provided to government and law enforcement agencies to inform policy and tactical decision-making processes.

Performance 2011–12

Over the reporting period ASIO investigated and identified individuals seeking to cause harm to people or property during protest activity.

In 2011–12 many of the specific tensions and national issues from around the world had the potential to be reflected in Australia. However, no communal violence resulted over the reporting period.

Border integrity investigations

The amendment of the ASIO Act in June 2010 to include border integrity resulted in an increased focus of ASIO's investigative capability on the prevention of people smuggling. This includes the identification and investigation of individuals or groups engaged in people smuggling.

ASIO's investigation of people with links to maritime people-smuggling networks is part of a whole-of-government effort to ensure the integrity of Australia's borders. In undertaking this work, ASIO engages with the Australian Customs and Border Protection Service and the Australian Federal Police, as well as international partners. This work informs government bodies who are operationally engaged in the prevention of people smuggling.

Performance 2011–12

ASIO reports its performance on border integrity investigations in the classified Part 3 component of its annual report.

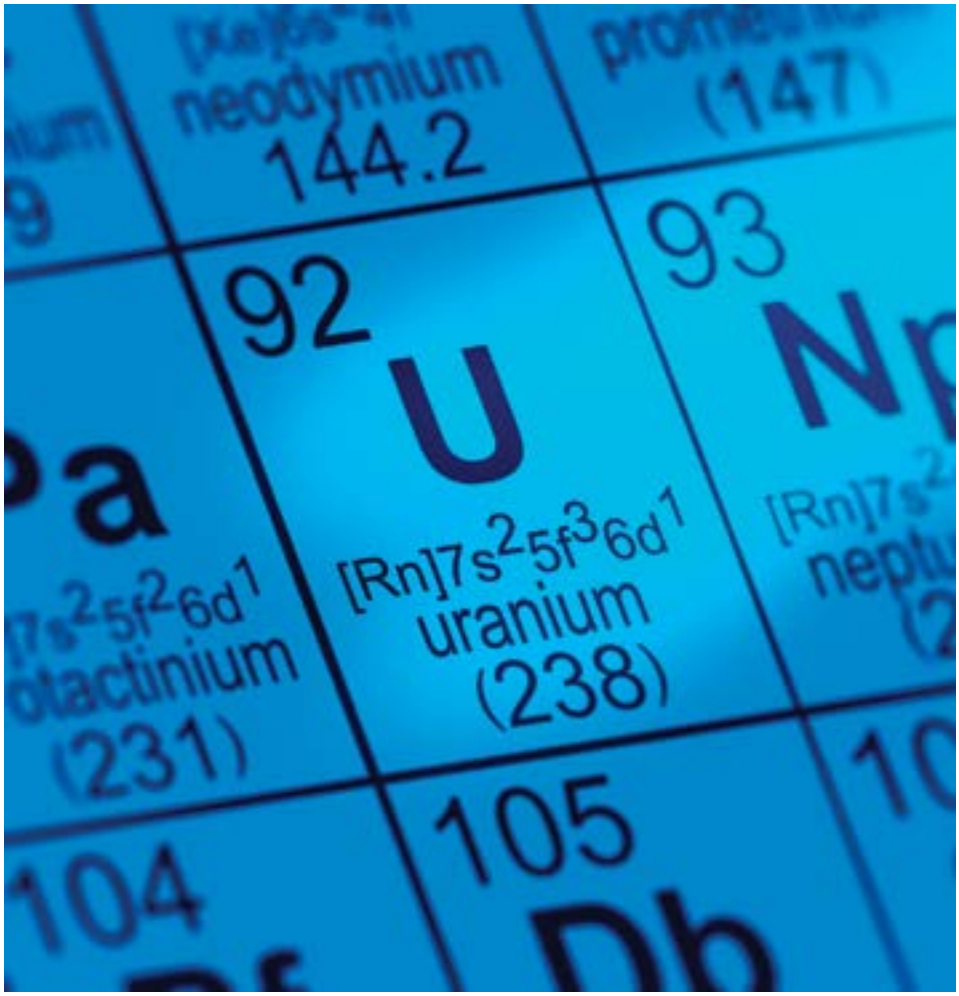
Counter-proliferation investigations

Australia takes seriously its international treaty and United Nations Security Council resolutions obligations in the prevention of the proliferation of Weapons of Mass Destruction (WMDs). The detection and investigation of individuals or state actors seeking to use Australian sources to acquire prohibited goods is integral to the international effort against the proliferation of WMDs.

ASIO conducts investigations and operations targeting both state and non-state actors who seek to procure items of technology or material which could lead to the provision of WMDs.

Performance 2011–12

ASIO reports on its performance of counter-proliferation investigations in the classified Part 3 component of its annual report.



Program 4

Investigative, analytical and operational capability supports ASIO's function via intelligence collection capability, research and development for collection and analysis, and engagement with national and international partners.

- Special powers under warrant
- Technical collection capability
- Telecommunications interception
- Data exploitation
- Research and development
- Commonwealth technical response capability
- Physical surveillance capability
- Human-source intelligence collection
- Language capability
- International engagement
- Foreign intelligence collection

Investigative, analytical and operational capability

"In order to carry out its investigative functions, ASIO has been given a number of special powers. These are considered controversial by some, but successive governments have confirmed them as necessary for the protection of National Security."

The Director-General of Security, Bray Oration 19 September 2011

Special powers under warrant

ASIO exercises a range of intelligence collection capabilities under warrant, including capabilities referred to in the ASIO Act as 'special powers'. Like other investigative agencies, legislation grants ASIO powers to collect certain types of intelligence under warrant. These powers include the deployment of listening devices, telecommunications interception capabilities, tracking devices, the ability to examine postal articles, the remote access of computers and to enter and search premises. ASIO also has the ability to use questioning and questioning and detention warrants, which are issued subject to particularly stringent criteria. The use of questioning and detention warrants is considered only in extreme counter-terrorism cases where the severity of the situation requires it.

The collection of intelligence under warrant operations continues to be of high value to ASIO investigations. The criteria for obtaining warrants are strictly prescribed and complemented by the Attorney-General's Guidelines. Warrants have a limited duration and, with the exception of short-term emergency warrants available under the ASIO Act, ASIO must seek agreement from the Attorney-General and satisfy tests set out in the relevant legislation before a warrant will be issued. ASIO's warranted activities are scrutinised regularly by the Inspector-General of Intelligence and Security. ASIO's deployment of warrant powers follows strictly the principle of proportionality—the means for obtaining information is proportionate to the gravity of the threat.

Performance 2011–12

Due to the sensitive nature of ASIO special powers under warrant, outcomes for the reporting period cannot be listed.

Technical collection capability

ASIO's technical collection capabilities complement its human intelligence collection activities and make an important contribution to every priority investigation. These capabilities must meet the challenges presented by the full range of ASIO's targets.

Sustained investment, research and development, combined with close cooperation with national and international partners is essential in maintaining this nationally important capability. Challenges for ASIO's technical collection capability include the rate of technological change, the increasing complexity and diversification of the telecommunications environment in Australia, the increasing volume of data requiring analysis and growing global interconnectivity.

Performance 2011–12

ASIO reports on performance of its technical collection capability in the classified Part 3 component of its annual report.

Telecommunications interception

Telecommunications interception remains a core technical capability which supports ASIO's operational and investigative work.

Under warrant, ASIO has the ability to intercept telecommunications services for a prescribed period of time against a defined target.

Performance 2011–12

During the reporting period ASIO, as the lead Australian Government agency for telecommunications interception technical advice, worked closely with other operational agencies and policy departments to develop strategies to address the ever-changing telecommunications interception challenge. Increased collaboration, technical exchange and burden sharing between agencies are critical components of this approach.

In 2011–12, ASIO continued its pilot of the National Interception Technical Assistance Centre (NiTAC) aimed at helping telecommunications intercepting agencies develop and maintain interception capabilities in an increasingly complex technical environment. The NiTAC continued to provide support to development of the government's policy relating to telecommunications interception.

The NiTAC works closely with interception agencies to ensure they understand the knowledge, skills and techniques necessary to maintain a high-quality telecommunications interception capability.

In keeping with its lead role in maintaining the investigative value of telecommunications interception, and to satisfy not only its own requirements but also those of the 16 other agencies involved in interception, ASIO collaborated with key players in the telecommunications industry.

ASIO also worked closely with industry partners on the development of new capabilities and provided important interception advice to a number of industry participants during the reporting period.

Data exploitation

In order to fulfill effectively its intelligence responsibilities, which includes the timely analysis of large volumes of information from diverse sources, ASIO maintains a range of advanced data exploitation capabilities. These capabilities are being constantly refined to address new business requirements and changes in the security environment.

Effort is being focused on reducing the number of separate data delivery and analysis systems, thereby reducing their associated maintenance overheads. Such work is also being conducted by several of ASIO's major national and international partners and, where possible, the Organisation is leveraging their experience and capabilities to maximise the return on its investment in this area.

Performance 2011–12

A particularly successful strategy pursued by the Organisation during 2011–12 was the embedding of more data analysts within core investigative areas. These embedded analysts were able to offer unique insights into investigations and to facilitate the transfer of high-level interpretative skills to investigators. They were heavily drawn upon in major investigations. Continued investment in this capability will be essential to maintain its effectiveness.

ASIO research and development

In addition to direct engagement with Australian universities and research providers including the CSIRO, ASIO maintained its involvement with the government's National Security Science and Innovation Strategy. The strategy's focus includes encouraging innovative approaches and solutions to national security challenges.

ASIO continued to work closely with domestic and international partners on emerging technologies. Key domestic partners include the Department of the Prime Minister and Cabinet and the Defence Science and Technology Organisation.

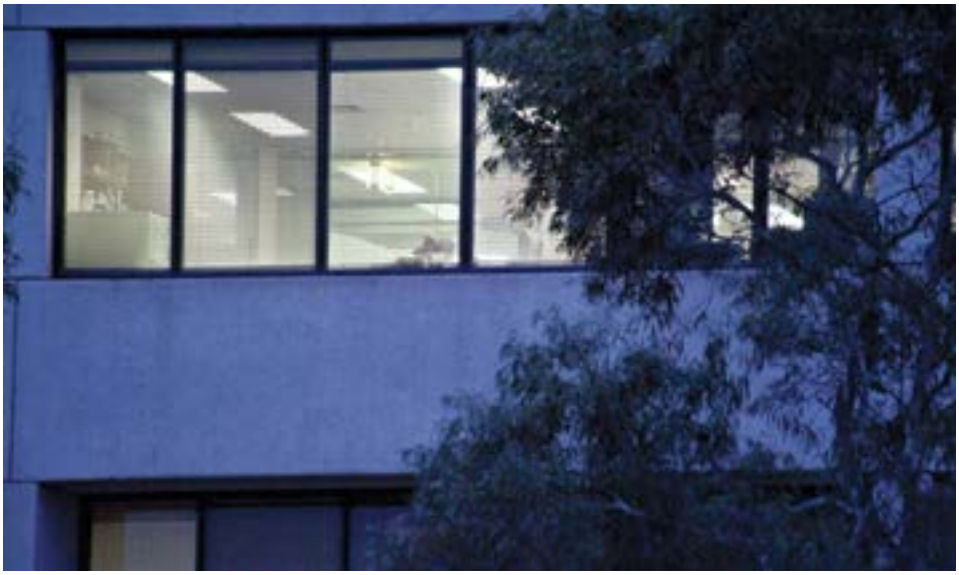
Commonwealth Technical Response Capability

The Commonwealth Technical Response Capability (CTRC) provides a framework which enables state and territory law enforcement agencies to utilise, at short notice, ASIO and Australian Federal Police technical capabilities in response to a major terrorist incident or in support of a significant event. These include surveillance and technical collection capabilities.

The ability for ASIO to work cooperatively with partner agencies in the field of technical collection not only enhances the security at events where the CTRC is deployed, but enables shared learning and technical outcomes. As with other key capabilites, it requires continued investment to maintain its effectiveness.

Performance 2011–12

These capabilities were deployed, and produced valuable outcomes, in support of Western Australian Police's successful operation protecting the Commonwealth Heads of Government Meeting and associated events in Perth in October 2011.



Physical surveillance capability

ASIO surveillance capability is deployed as an intelligence collection function and to assist the development of complex operations. ASIO surveillance measures include both static and mobile capabilities.

ASIO surveillance officers undertake their work in challenging environments, often where the deployment of other methods of intelligence collection is not viable. The range of intelligence collection obtained via the use of surveillance is considerable. ASIO surveillance also provides support to operations, assisting with logistical considerations or enhancing the safety of ASIO officers.

Performance 2011–12

Surveillance reporting continued to identify activities of potential national security concern and provided unique insights which opened new lines of investigation and enabled other operational activities.

ASIO continued to work closely with surveillance teams from Australian and overseas agencies, particularly in support of counter-terrorism investigations, and participated in joint training exercises.

Human-source intelligence collection

Human-source intelligence is of particular value in providing lead intelligence on threats to national security and providing context or 'joining the dots' in a security intelligence investigation.

Intelligence collection occurs in line with a defined set of National Intelligence Priorities and to fulfil identified intelligence gaps. It also occurs against a broad and robust set of accountability measures, both within the Organisation and from external bodies, such as the Inspector-General of Intelligence and Security.

Performance 2011–12

Over the reporting period, ASIO maintained a human-source base capable of providing timely, reliable and comprehensive reporting against defined intelligence priorities and requirements.

The Community Contact Program

The Community Contact Program is a longstanding ASIO initiative, comprising ongoing engagement with members of communities represented in Australia. Through the Community Contact Program, ASIO collects information on threats or interference emanating from within, or directed towards, a variety of communities.

This program also serves to explain ASIO's role and functions in protecting Australia and ensures positive ASIO engagement with communities is maintained and issues of potential security interest are proactively identified.

Language capability

ASIO invests in, and maintains, a significant foreign language capability as part of its overall national security intelligence capability. This ensures language is no barrier in the collection and analysis of intelligence or liaison with counterparts.

ASIO's language capability is predominantly deployed to assist ASIO investigations, particularly counter-terrorism and counter-espionage. The quality and timeliness of ASIO's language capability is a continual focus and is supported through training and liaison with key domestic and international partners.

Performance 2011–12

Over the reporting period ASIO's language capabilities maintained sufficient coverage for operational requirements. ASIO's language capability was broadened with the ongoing recruitment of linguists in identified areas of requirement.

International engagement

International liaison relationships enable ASIO to draw on the expertise and capability of overseas partners and to enhance our ability to pursue intelligence investigations which transcend national boundaries.

ASIO engages with partners through liaison meetings, exchanges of information and reporting, international visits and conferences, joint training and capability development initiatives, formal secondments and staff exchanges.

Security threats against Australia emanate from many different parts of the world. The transnational nature of security threats demands international cooperation between security agencies. To maximise its effectiveness, ASIO engages with, and receives support from, a number of international partners.

Performance 2011–12

Over the reporting period, budgetary pressures have resulted in a reduction of scope to ASIO's international engagement. This reduction was undertaken taking into with consideration of security intelligence priorities.

ASIO has offices in key international locations to maintain and manage relationships with overseas partners. At the end of this reporting period, the Attorney-General had authorised ASIO to liaise with 340 authorities in 125 countries.

ASIO ensures its international engagement complements and supports that of other Australian Intelligence Community partners and those efforts are coordinated to glean optimal intelligence outcomes.

ASIO officers adhere to specific protocols which regulate the exchange of information with overseas services. These incorporate strict accountability measures, including auditing by the Inspector-General of Intelligence and Security.

Foreign intelligence collection in Australia

In addition to its security intelligence function, ASIO has the statutory authority to collect foreign intelligence (under warrant) in Australia on matters relating to Australia's:

- national security;
- foreign relations; or
- national economic well-being.

ASIO exercises its foreign intelligence collection powers at the request of the Minister for Foreign Affairs or the Minister for Defence and in collaboration with Australia's primary foreign intelligence agencies, the Australian Secret Intelligence Service and the Defence Signals Directorate. ASIO may also collect incidental foreign intelligence through our security intelligence investigations and liaison with overseas partners.

Performance reporting of ASIO's foreign intelligence collection activities is set against the National Intelligence Priorities and comprises both quantitative measures (consisting of warrants, operations and outputs) and qualitative measures (predominantly meeting sponsor intelligence requirements). Foreign intelligence collection outcomes are only reported on in the classified component of the Annual Report.

Part 3

Outcomes and highlights

This section of the report has been excluded in its entirety from the unclassified *Report to Parliament* for reasons of national security.

Part 4

ASIO and accountability

"ASIO is an organisation working in the public interest, for the protection of the public, its successes can rarely be published."

The Director-General of Security, Address to the Sydney Institute
24 January 2012

Many of ASIO's activities occur outside the public view. However, ASIO is subject to comprehensive accountability and oversight authorities that ASIO activities are subject to include the Attorney-General, the Independent National Security Legislation Monitor, the Parliamentary Joint Committee on Intelligence and Security, the Senate Standing Committee on Legal and Constitutional Affairs, the Inspector-General of Intelligence and Security and the Australian National Audit Office.

Attorney-General

One of the key accountability pillars of the ASIO Act is that it sets the parameters of ASIO's role as a security intelligence organisation in Australia's democracy and the organisations unambiguous responsibility through the Attorney-General to the government.

It is within this accountability context, and in line with the Director-General's obligation to keep ASIO free from any influences or considerations not relevant to ASIO's functions, that ASIO prepares its advice on investigations and operations; formulates policies and procedures; conducts security assessments; manages its staffing; and interprets and complies with legislation.

The Hon. Nicola Roxon MP was sworn in as Attorney-General on 14 December 2011.

Attorney-General's Guidelines

Under sections 8A(1) and 8A(2) of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), the Attorney-General issued guidelines to the Director-General of Security, dated 10 December 2007, which are observed by ASIO in the performance of its functions of obtaining, correlating, evaluating and communicating intelligence relevant to security. Apart from articulating the governing principles of ASIO's work, the Attorney-General's guidelines:

- specify how ASIO should go about obtaining, correlating, evaluating and communicating intelligence relevant to security; and
- define politically motivated violence and provide guidance on the investigation of violent protest activities.

The guidelines stipulate that information is to be obtained by ASIO in a lawful, timely and efficient manner, and investigations are to be conducted with as little intrusion into individual privacy as possible—consistent with the national interest.

The means by which ASIO obtains information are determined by the gravity of the threat to security and the likelihood of its occurrence. The intensity of ASIO investigations and activities is proportionate to the threat to security. Where the threat is assessed as serious, or where it emerges quickly, a greater degree of intrusion may be necessary.

The guidelines give guidance on interpreting the definition of politically motivated violence contained in section 4 of the ASIO Act. Politically motivated violence includes acts or threats of violence that are intended or likely to achieve a political objective, whether in Australia or elsewhere, including acts or threats carried out for the purpose of influencing the policy or behaviours of a government, whether in Australia or elsewhere.

National Security Committee of Cabinet

The National Security Committee of Cabinet (NSC), chaired by the Prime Minister, is the authoritative ministerial decision-making body on Australia's national security effort. This includes consideration of national security priorities and resourcing, as well as agency performance against priorities set by the NSC.

The Secretaries' Committee on National Security (SCNS) provides support to the NSC through the consideration and coordination of matters put to the NSC. The Director-General of Security, who sets ASIO's security intelligence priorities, participates in NSC meetings and is a member of SCNS.

Parliamentary oversight

Parliamentary Joint Committee on Intelligence and Security

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

- review the administration and expenditure of 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—*Border Security Legislation Amendment Act 2002, Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* and *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 ASIO Act; 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.

For ASIO, review of administration and accountability occurs through the provision of a report each financial year on administration and expenditure and attendance at PJCIS hearings on matters of administration and expenditure. In 2011–12, ASIO submitted both an unclassified and classified review of administration and expenditure for the previous reporting period and attended a PJCIS hearing.

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 responsible for the review of activities of the Australian intelligence community, to ensure agencies act legally, with propriety and in compliance with ministerial guidelines and directives and with due regard for human rights.

The IGIS regularly conducts inspections and monitoring of ASIO activities, with particular attention to operational activities. The IGIS also has the power to inquire into public complaints, conduct inquiries referred by Government and initiate 'own motion' inquiries.

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

The IGIS provided a copy of the report to the Attorney-General in June 2012 with the report containing three recommendations. The first recommendation relates to ASIO providing risk mitigation advice to DIAC to allow a person subject to an adverse security assessment to enter community detention where DIAC has identified significant health, welfare or other exceptional issues. ASIO considers that the suggested approach may be outside its current legislative remit.

ASIO agreed to the other two recommendations relevant to recording decision making and maintaining ASIO's policy and training documentation for interviews, particularly with regard to mental health considerations.

On 10 January 2011, the Inspector-General of Intelligence and Security announced an inquiry into the actions of Australian intelligence agencies (and DFAT, AFP, AGD and PM&C) in relation to Mr Mamdouh Habib's overseas detention in 2001–2005.

ASIO gave full cooperation to the IGIS throughout the inquiry. The IGIS had full access to ASIO's records and officers. On 23 March 2012 the unclassified version of the IGIS's report was released. The IGIS found that no Australian agency or official:

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

ASIO accepted the recommendations from the IGIS relevant to its policies and procedures. These relate to engagement with, and the provision of information to, foreign authorities.

Reviews

Australian National Audit Office report on security assessments of individuals

The Australian National Audit Office (ANAO) report on its audit of security assessments of individuals was tabled in parliament on 25 June 2012. The aim of the audit was to assess the effectiveness of ASIO's arrangements in providing timely and soundly based security assessments of individuals to client agencies. It is the first ANAO audit to focus primarily on ASIO.

The audit found that ASIO has a sound governance framework in place, including risk management arrangements that are updated regularly, and found 100 per cent compliance in all security assessment cases reviewed (over 400). The report also found

that all cases examined complied fully with ASIO's processes and procedures and that there were quality assurance processes in place for the small proportion of security assessments that resulted in prejudicial advice.

The report made four recommendations, which relate to: implementing quality assurance processes for non-prejudicial assessments; sustaining risk-based 'triaging' for irregular maritime arrivals cases; formalising agency relationships; and strengthening workforce planning strategies for the security assessment areas. ASIO agreed to all recommendations.

Joint Select Committee on Australia's Immigration Detention Network

On 16 June 2011 the parliament established the Joint Select Committee on Australia's Immigration Detention Network to consider and report on the management, resourcing, potential expansion and potential alternative solutions to Australia's immigration detention network. Part of the inquiry naturally looked to ASIO security assessments.

The report, handed down in March 2012, included recommendations on the appeal and review of adverse security assessments and the inclusion of provisions for periodic internal reviews of security assessments. Also included in the report were suggested courses of action for individuals assessed to be asylum seekers, but who are subject to indefinite detention or cannot be repatriated. ASIO welcomed the report and agreed in principle or in part to four of the six recommendations specific to ASIO security assessments. Consideration and implementation of the recommendations will continue over the 2012–13 reporting period.

Independent Review of the Intelligence Community

In December 2011 the Report of the Independent Review of the Intelligence Community (IRIC) was issued by the Prime Minister. Two forms of the report were released: an unclassified and a highly classified version.

The IRIC provided a summary of observations of the Australian intelligence community (AIC) by independent reviewers Robert Cornall AO and Dr Rufus Black. The review was positive about the AIC's increasing collaboration and willingness to work more effectively with the national security community. It also concluded the investment made in building up the intelligence agencies had been justified and rewarded with more capability and increased performance.

ASIO welcomes the findings, particularly as they relate to ASIO's commitment to enhancing our strategic impact through shared effort in the National Security Community.

Independent National Security Legislation Monitor

The Office of the Independent National Security Legislation Monitor (INSLM) was formally established by the *Independent National Security Legislation Monitor Act 2010*.

In April 2011 the government appointed Mr Bret Walker SC as INSLM to review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation, and report the findings to the Prime Minister and the parliament. The INSLM's first report, dated 16 December 2011, drew on his work for the first six months of his appointment, set out a number of questions and issues being considered by the INSLM, and notified a provisional agenda for the work of the INSLM for the coming year. ASIO is committed to working with the INSLM and over the reporting period provided information and support to this work.

Internal audits and fraud control

Audit

The financial year 2011–12 marked another year of change and development with the implementation of changes to the *Financial Management and Accountability Act 1997* (FMA Act) increasing the focus on risk management. In response to these changes ASIO has transitioned the Audit and Evaluation Committee to the Audit and Risk Committee (ARC) reflecting the accountability and management of risk within ASIO and in compliance with section 45 of the FMA Act and regulation 22C of the Financial Management and Accountability Regulations. ASIO aligned the changes required into the ARC charter, ensuring the ARC work plan meets all requirements set out in the FMA Act.

The Director-General of Security has appointed an independent chair of the ARC. The ARC provides independent assurance and assistance to the Director-General on ASIO's risk, control and compliance framework, and its financial statement responsibilities. It also advises the Director General on the annual Audit Work Program. This work program includes performance, compliance and assurance audits.

The focus of ASIO's audit program is to improve performance by providing a value-add service to ASIO business areas by identifying workplace efficiencies as well as validating compliance with relevant legislation and established practices and processes. One major review completed in 2011–12 into credit card management, the identified opportunities for streamlining management of Australian Government credit cards. ASIO intends to expand the performance audit capability program next year, in recognition these audits assist ASIO to consistently achieve workplace improvement.

ASIO completed sampling and fieldwork to assist the Australian National Audit Office in conducting their financial statements audit across operational expenditure for the Organisation. There were no issues identified in this work requiring rectification.

ASIO maintains a training regime for internal and external members of the ARC to maintain currency and awareness of government policy, requirements and expectations.

Fraud control

Current arrangements for fraud prevention, detection, investigation, reporting and data collection are in place via the ASIO Fraud Control Plan 2011–13 and the ASIO Fraud Policy: Fraud risk and control in ASIO.

ASIO is committed to minimising the incidence of fraud and is continually seeking to enhance fraud prevention and detection mechanisms. To this end, throughout 2011–12 ASIO's fraud control and detection processes were redesigned with the aim to consolidate responsibility and the accountability for all aspects of fraud control into one independent area within the Internal Audit Unit.

All ASIO staff and contractors undertake mandatory training in ethics and values, code of conduct, fraud and audit. This training is undertaken at the commencement of employment and every three years thereafter and ensures that ASIO's values and code of conduct are embedded into our culture, systems and procedures.

In coming years the Organisation is seeking to integrate its fraud risk assessment with the enterprise risk assessment conducted under the Strategic Risk Management Framework.

During the reporting period, there were three allegations of fraud, with two allegations confirmed. These issues were resolved through administrative actions, which included adjustment of leave entitlements and increased management oversight. No external allegations of fraud were reported.

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

Audit of assumed identities

Assumed identities and commercial cover are utilised to protect ASIO officers' identities and prevent the potential compromise of ASIO operational activities. The authority for this is drawn from Part IAC of the *Commonwealth Crimes Act 1914*; under which stringent audit requirements are applied six-monthly. Additionally there are a small number of authorities maintained under the *NSW Law Enforcement and National Security (Assumed Identities) Act 2010* also audited six monthly.

Across all of these audits compliance was found with each of the Acts in terms of appropriate delegations being exercised for all authorisations, variations and cancellations completed during the period.

Security in ASIO

Security in ASIO

Security in ASIO is paramount to continuing the effective conduct of ASIO operations and investigations. This occurs through a variety of mechanisms, all of which support the protection of information, people and business systems. The very nature of ASIO's work necessitates uncompromised compliance with security best practice and the expectations of all ASIO staff is set against these requirements.

Personnel security

Personnel security in ASIO comprises integrated personnel security risk management strategies, policies and procedures, which are stringently applied and regularly reviewed.

An ASIO officer must maintain a security clearance during the course of their employment. This requires high standards of behaviour in both professional and personal life, and comes with the expectation of reporting to the Organisation anything which might impact an officer's ability to maintain the required level of clearance.

ASIO supports this requirement with the provision of psychological health services, including an Employee Assistance Program to proactively address issues of health and wellbeing of ASIO staff, as well as potential vulnerabilities before they arise.

Security awareness sessions are incorporated into ASIO introductory and ongoing training programs. All staff must attend a security awareness program within six months of commencement and attend a refresher program every five years.

Governance and policy

The ASIO Security Committee provides a senior executive forum for the development and maintenance of security risk management best practice, the endorsement of security strategies and the provision of assurance to the Director-General of Security.

ASIO undertakes a program of continual review, maintenance and update of security policy, as informed by the Australian Government Protective Security Policy Framework.

The robust security culture within ASIO begins with sound leadership, advice and policy—all of which have a foundation in the ASIO Security Committee.

Information Technology Security

The ongoing audit and investigation of ICT security incidents provides a strong component of accountability for the proper use of ASIO systems.

Efforts on the protection of ASIO's ICT remain focused on cyber attacks directed at ASIO's externally connected systems and information assurance relating to the implementation of new ICT projects and applications.

Outreach

ASIO engages effectively and works with partners—traditional and new, business and industry, academia and the wider community. ASIO is committed to this important aspect of its work and is dependent on the support and cooperation of its partners and the Australian community. Without this support, ASIO's ability to protect the security and safety of Australians would be compromised.

An enduring concern—but unfortunate reality—is the often unfounded speculation and commentary about ASIO's activities. Where possible, ASIO provides public comment, and engages with the media and other interested parties. However, ASIO follows standard government policy in not commenting upon intelligence operations, neither confirming nor denying.

More broadly, ASIO undertakes a range of outreach and engagement initiatives to promote greater awareness of ASIO's work while nurturing a greater sense of trust and shared understanding with partners and the public.

Speeches by the Director-General of Security to various forums, engagement with the media, ASIO-initiated partnership forums and documents such as its unclassified annual report, are some of the mechanisms through which ASIO engages with the public sphere.

Partnership forum

ASIO's program of senior executive and senior officer partnership forums with State and Federal Government continued throughout 2011–12. This program is an integral part of ASIO's outreach and engagement initiatives. The forums provide participants with first-hand insights into the work of, and challenges facing, ASIO. These forums are an opportunity to collaborate, debate and share ideas—as well as presenting an occasion to build professional networks and explore potential partnering options.

Stakeholder satisfaction survey

The annual stakeholder satisfaction survey provides ASIO with valuable insight into the level of satisfaction of key partners, and the extent to which ASIO supports the attainment of partner agency outcomes. Feedback is sought on partners' level of satisfaction with their engagement with ASIO, their views on ASIO's collaboration, stakeholder focus, capabilities and people and their evaluation of the quality, timeliness and accessibility of ASIO information and advice.

For the first time the Stakeholder Satisfaction Survey was extended to include an email survey to seek broader feedback across several sectors and levels of stakeholders. On 22 September 2011, an invitation to participate in the email component of the 2011 Stakeholder Satisfaction Survey was sent to 151 of ASIO's stakeholders at Senior Executive Service Band 1 and Executive Level 2 levels from a range of Commonwealth, state/territory and private industry stakeholders. The survey achieved a response rate of 21.2 per cent. Stakeholders continued to report high levels of satisfaction with their engagement with ASIO. The email component was conducted in conjunction with face-to-face interviews, providing clients the opportunity to contextualise comments relevant to ASIO performance. Over the past year, a number of Commonwealth agencies noted a significant improvement in their engagement with ASIO, citing relationship-building activities like partnership forums, at both the SES and middle-management level, as key to this improvement.

In the next reporting period ASIO will survey a wider set of Commonwealth agencies than in previous years, reflective of organisational interaction with an increasingly broader range of government agencies.

Public statements and media

Throughout 2011–12, ASIO continued to engage publicly through speeches and appearances by the Director-General of Security. On these occasions he spoke publicly on a number of occasions covering topics such as the security environment, emerging threats and cyber-security.

Transcripts of public speeches by the Director-General of Security are available on the ASIO website (www.asio.gov.au).

Part 5

Corporate management

"Part of my job as Director-General of Security is to ensure that ASIO is as best equipped as it can be, in an age of constant change, in terms of technology and the training and professionalism of its officers to be able to identify and deal with the current and future threat environments."

The Director-General of Security, address to the Sydney Institute
24 January 2012

People

The 2011–12 reporting period marked the conclusion of significant workforce growth over the past decade for ASIO. Throughout the year, ASIO worked to refocus its people strategy efforts towards one of consolidation with emphasis on innovative ways to attract, build and retain a highly capable workforce comprised of a range of professional disciplines, expertise and backgrounds in a competitive job market. An integral part of this was the continuing adoption of ASIO's Human Capital Framework.

Continuing to invest in a skilled workforce is a key part of maintaining ASIO's nationally important security intelligence capability.

Human capital framework

ASIO's Human Capital Framework, introduced in 2010, provides a single strategic system for managing and building people capability, with improvements coming from the synergies obtained when bringing together disparate people management processes and functions. During 2011–12 significant improvements were made against all four key elements of the framework.

The key elements of the Human Capital Framework are:

- **people strategy and workforce planning** — supporting executive decision making, strategic workforce planning, and the management of sourcing and retention strategies;
- **selection, evaluating and vetting** — attracting and selecting talent and the core recruitment processes;
- **capability management, learning and development** — managing the performance of the workforce and ensuring continuous professional development; and
- **agility management, human resource services and support** — human resource policies and practices that create and manage agility in the workforce.

People strategy and workforce planning

The Review of ASIO Resourcing, conducted by Mr Allan Taylor AM in 2005, identified 1,860 full-time staff as the endpoint target for ASIO. As part of the government's 2012–13 Budget and consistent with the government's fiscal policy, ASIO's approved endpoint was reduced in February 2012 to 1,760, although the Organisation realistically can only afford an endpoint of 1,730. In response, the Staffing and Resource Allocation Review has been initiated to prioritise and realign staffing allocations to ensure ASIO's ongoing capability to meet its key obligations to government. Further staff reductions may be necessary.

Strategic workforce planning remains an integral part of ASIO's Human Capital Framework. Workforce planning activities continued throughout 2011–12, underpinning ASIO's longer term vision of ensuring that people capability requirements, now and into the future, support Organisational goals and deliver operational outcomes.

Significant developments include the introduction of a new ASIO job family model and the inaugural workforce sourcing plan. The plan provides tactical interpretation of the ASIO Strategic Workforce Plan while the new job family model allows greater segmentation of our workforce, which facilitates analysis and planning of the workforce; assists in defining development activities; enhances staff and manager discussions on career planning; and assists the development of targeted recruitment strategies.

A revised *ASIO Strategic Workforce Plan 2013–2016* will be finalised in 2012–13 as ASIO continues to identify, manage and mitigate specific workforce risks and ensures it has the workforce capacity and capability to respond to current and future priorities.

Staff survey

In April 2012 ASIO conducted a staff survey to obtain workforce perceptions of, and levels of satisfaction with, a number of key people and cultural indicators. A strong and representative response rate of 72 per cent was achieved. As a consequence of implementing and delivering specific corporate and people management/development initiatives, ASIO has attained results indicating significant areas of improvement since the 2009 survey.

The survey confirmed the requirement for new initiatives planned for implementation during 2012–13, such as a new domestic posting policy and a career management portal.

2012 ASIO staff survey highlights

- Over 98 per cent of ASIO staff support the Organisation's mission.
- Over 93 per cent of staff believe that the Organisation has a clear set of values in relation to expected behaviours.
- Over 89 per cent of staff feel that they cooperate to get the job done.
- Over 89 per cent of staff report that they are innovative and always looking for better ways of doing things.

Employment framework

ASIO's ninth workplace agreement commenced on 21 June 2011, with a nominal expiry date of 30 June 2014. The agreement introduced initiatives to acknowledge the already significant contribution made by staff to ASIO's program of organisational change and business modernisation.

With the objective of ensuring ASIO has contemporary employment and people management frameworks and policies, a major project was initiated to review all terms and conditions of employment and produce an easy to read, single document. This project will be delivered in the first half of 2012–13 and will facilitate decision making, identify opportunities for refining employment conditions and facilitate comparative benchmarking with other agencies.

Selection, evaluation and vetting

With an affordable endpoint of 1,730 staff, ASIO will achieve this target during 2012–13. In 2011–12, ASIO welcomed 147 new staff to the Organisation, with 84 per cent engaged on an ongoing basis. As at 30 June 2012, ASIO employed 1,812 staff, representing 1,721 full-time equivalents. ASIO experienced a decrease in its separation rate during the reporting period, from 5.9 per cent in 2010–11 to 4.7 per cent in 2011–12.

Operational capability through a highly effective intelligence officer cadre remains a key priority for ASIO. Given the long lead times required to develop this capability—to recruit and train intelligence officers—and accounting for separation, recruitment of intelligence officers will continue on a regular basis throughout 2012–13.

In recent years, ASIO's recruitment marketing strategy has broadly focused on optimising exposure, using a mixed media approach to promote recruiting opportunities. This approach typically yielded large volumes of applicants, not necessarily converting to high-quality candidates.

ASIO has worked throughout the reporting period to reform recruitment strategies and practices. New strategies included targeted marketing; smaller, more frequent campaigns; mechanisms to reduce the number of unsuitable candidates; and an increased focus on strategic selection and assessment. Selection panels were provided with detailed training for each recruitment process, helping to ensure consistency and alignment with ASIO's People Capability Framework. These strategies increased efficiency and effectiveness, dramatically reducing expenditure on recruitment advertising and resource effort; reducing the annual volume of applications to be managed; and increasing the number of suitable quality candidates.

Being the primary point of reference and application, ASIO's website was refreshed as part of ongoing recruiting campaigns throughout the year. ASIO's expenditure on recruitment advertising decreased from $1.06 million in 2010–11 to $398,592 in 2011–12.

Capability management, learning and development

ASIO's People Capability Framework is a guide for all staff in relation to strategic workforce planning, recruitment, promotion, induction and orientation, performance management, learning and leadership and individual career planning. It also provided a key reference for ASIO supervisors in exercising their leadership responsibilities and supporting other staff. From an individual perspective, it is a cornerstone document, providing salient and practical information and a cohesive point of reference across the Organisation.

The framework is also important as a bridging reference for ASIO staff in relation to the broader professional environment by describing the capabilities and behaviours that are needed as ASIO delivers broader and more complex outcomes to the Australian Government.

Staff placements

In late 2011, an internal project was initiated to determine the issues influencing the effectiveness of ASIO's existing Transfer Framework Policy. A number of recommendations resulted from this scoping exercise, forming the basis for a full review, which commenced in February 2012.

As a result of the review process, a conceptual design of a new domestic posting policy was the subject of staff and leadership consultation throughout the Organisation through the latter part of 2011–12. This new approach focuses on improved responsiveness to organisational capability requirements through direct alignment with the internal ASIO Intelligence Coordination Committee priorities and improved individual career pathways and capability development. This approach continues building ASIO's long-term organisational capability, and as part of the Human Capital Framework is integrated with the workforce plan. The new policy will be released in the first quarter of 2012–13.

Staff exchange between Australian and international partners is a valuable activity in promoting job enrichment and professional development for ASIO staff. The value of such exchange is both professional and personal and provides hands-on opportunities to share information, learn new techniques and gain a broader understanding of contemporary national and international security issues.

ASIO remained committed to its outreach with regard to staff placements, with placements to and/or from the following government agencies:

- Attorney-General's Department;
- Australian Federal Police;
- Australian Government Solicitor;
- Australian Secret Intelligence Service;
- Defence Intelligence Organisation;
- Defence Security Authority;
- Defence Signals Directorate;
- Department of Foreign Affairs and Trade;
- 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 Regional Australia;
- Department of the Treasury; and
- New South Wales Police.

ASIO also participated in exchanges with the following foreign partner agencies.

- United States Federal Bureau of Investigation;
- Canadian Security Intelligence Service;
- British Security Service; and
- New Zealand Security Intelligence Service.

Training and professional development

ASIO is highly committed to the ongoing development of its officers. Training and professional development are key components in maintaining ASIO's security intelligence capability by supporting and continuing to develop professional and highly competent staff.

ASIO's training and professional development are a rich mix of internal programs and external government and private sector opportunities. This provides a diverse range of learning opportunities and skills development to support ASIO's diverse professional disciplines.

Throughout 2011–12, ASIO continued to support its strong learning culture via support for external study. ASIO officers are able to access study assistance, aimed at supporting staff and encouraging efforts in undertaking continuing education that is relevant to ASIO. This assistance may include leave to attend lectures, tutorials and examinations as well as financial support.

In 2011–12, 147 officers enrolled in external study programs. Fields of study included law, international relations, business management, information technology and education. ASIO also provided 19 officers language training through partial and fully funded support.

Performance management framework

Following on from extensive development work in early 2011, from July ASIO implemented Enhancing Performance—ASIO's system to manage, build and deliver capability within its workforce. This has resulted in a more meaningful dialogue between ASIO staff regarding performance management, development opportunities and career progression.

Leadership and management skills

Work continued throughout 2011–12 to enhance ASIO's leadership development. Leadership and management skills development remains an ongoing commitment and is an important component of the overall development suite of training.

Throughout the reporting period, ASIO's leadership program continued to prepare leaders for managing ASIO in a more complex and changing security environment, as well as exposing officers to broader leadership and management methodology and practice. Initiated in 2010, the leadership program remains on target to ensure all identified leadership positions—Executive Level 1 to Senior Executive Service (SES) Band 1—have completed the program by 2013.

New leadership-focused initiatives in 2011–12 include the introduction of a specific SES Career Development Strategy. Launched in March 2012, this strategy aims to ensure ASIO remains well placed with a strong and effective senior leadership team to meet both current and future needs.

E-learning

ASIO's e-learning environment has become an integral component of the overall learning environment, allowing officers to access a diverse range of training and information packages, integrating learning into their work schedule. ASIO's extensive e-learning capability provides an alternate mode of training and professional development as well as being a highly convenient and valuable point of reference. During the reporting period ASIO developed eight new e-learning modules with a focus on workplace behaviour, workplace health and safety and using ASIO systems.

Intelligence training

ASIO's Intelligence Development Program (IDP) is recognised by peer agencies as an exemplar of best practice entry-level intelligence officer training. The IDP training remains a cornerstone of ASIO's intelligence training program, and provides essential foundational and core skills training for both ASIO case officers and analysts. Two Intelligence Development Programs were completed between July 2011 and June 2012, with a total of 32 officers graduating from the programs as either analysts or case officers.

During the reporting period an important design feature of the IDP was the increased flexibility to enable greater access to training modules by staff working in intelligence roles to build particular knowledge and skill sets. During January–June 2012, 44 participants accessed this training.

Following a review into ASIO's intelligence training strategy in November 2011, a dedicated post-IDP training unit was established. Working in close collaboration with the core intelligence divisions, the unit developed and delivered a range of advanced and specialised intelligence courses to address the ongoing development needs for officers throughout their ASIO careers.

Agility management, human resource services and support

Diversity, harassment and discrimination

ASIO maintained its strong commitment as an equal opportunity employer. Throughout the year, ASIO continued its endeavours to provide an equitable, inclusive work environment—one that embraces diversity as well as providing a supportive professional environment.

Results from ASIO's staff survey in June 2012, demonstrate the success of the anti-bullying and harassment campaign, 'Silence Hurts', with a marked reduction in reported or witnessed incidents. The campaign proved to be highly successful in encouraging and supporting staff to both recognise and address inappropriate behaviour, and promoting points of contact. An important outcome from the campaign has been the reinvigoration of the harassment contact network. This network provides an alternate mechanism for staff to seek advice and support.

The next phase of the 'Silence Hurts' campaign is currently under development and will commence in late 2012 to continue the momentum in positive workplace change since its introduction.

ASIO code of conduct

ASIO staff consistently demonstrate distinguished personal and professional behaviours and conduct, in accord with ASIO's Code of Conduct. The code provides a strong and unambiguous definition of the expected standard of the professional and personal behaviours expected of an ASIO officer. Importantly, the code provides a reference and context of these expectations, specifically in context with ASIO's mission, functions, the operating environment and unique role.

The 2012 ASIO staff survey found that over 90 per cent of ASIO staff believe the Organisation has a clear set of values in relation to expected behaviours and that they have a good or very good understanding of these values.

The Code of Conduct is available on ASIO's website (www.asio.gov.au).

Workplace health and safety

The provision of a safe and healthy work environment remains a key priority for ASIO. To this end, ASIO promotes a culture of personal accountability for work health and safety aligned with three key themes of:

- safe work practices, and the systems to support these practices, must be embedded as daily business;
- managed risks and early intervention, essential for performance; and
- informed decision making and sound judgment is required to demonstrate accountability.

Subsequently, and in preparation for the new Work Health and Safety (WHS) laws, in 2011–12 ASIO:

- developed a WHS Risk Program;
- identified WHS 'Officer' roles as a due diligence requirement;
- provided ongoing information and education to staff and managers;
- collaborated internally and externally on the implementation and implication of the legislation; and
- maintained a strong relationship with Comcare.

During 2011–12, absence due to work related injuries decreased by over 20 per cent compared to 2010–11 and by nearly 35 per cent compared to 2009–10.

Reporting period	Absence due to work injuries(weeks)
2011–12	302.55
2010–11	380.80
2009–10	457.66
2008–09	362.03
2007–08	313.98

In 2011–12, no notifications were made to Comcare, investigations conducted, nor notices issued under applicable legislation.

To promote physical, mental and social health and wellbeing, ASIO held its annual health program in November 2011. The event was to encourage, inform and motivate ASIO's staff to make positive and sustainable lifestyle choices for long-term health and wellbeing. Based on three key themes: motivate, educate and activate, the program offered a range of activities and information forums designed to inspire and provide tools to develop further knowledge.

Staff and Family Liaison Office

Approaching its third year of operation, the Staff and Family Liaison area is one of the important contributors to ASIO's holistic and integrated wellbeing services. It provides a number of integrated services aimed at supporting staff and their families.

In 2011–12 the Staff and Family Liaison Office provided support to staff moving interstate, counselling and referral services for staff members and their families and support for the families of staff members who are unable to be contacted for periods of time.

The Staff and Family Liaison Office delivered two successful family information events in 2012. These initiatives provide immediate family members with a broader understanding of ASIO and the implications of working in the Organisation. They are designed to assist family members and provide an opportunity to acknowledge families for their ongoing support.

ASIO Ombudsman

ASIO employs an external Ombudsman as an independent arbiter to address staff concerns. The Ombudsman assists staff in the event that they consider themselves to have been treated unfairly within the Organisation—after internal mechanisms for resolution have been exhausted. The Ombudsman's role is to provide a discrete, informal mechanism to manage concerns in an impartial manner while being transparent and objective.

The Ombudsman provides a biannual update to the ASIO Executive Board on the general nature of activities, with more detailed provision to the Director-General as required.

In 2011–12, the Ombudsman independently initiated formal reviews into two staff complaints, as well as responding informally to staff queries. No matters were referred by the Director-General to the Ombudsman for formal investigation.

Senior Executive performance pay

As part of workplace agreement negotiations in 2010–11, the system of payment of performance bonuses for Senior Executive Service (SES) staff was abolished and no SES staff received a bonus in 2011–12.

Property

New central office

This project is a purpose built facility, designed to cater for ASIO's technical and accommodation needs—with an estimated design life of a minimum 50 years. As the tenant agency, ASIO has an ongoing and keen interest in this project. Throughout the reporting period, ASIO has continued to work closely with key project stakeholders such as the Department of Finance and Deregulation and the Managing Contractor.

Throughout 2011–12, significant progress was achieved in the construction of ASIO's new central office. In addition, ASIO undertook a significant readiness program in preparation for taking possession and relocating into the new central office.

Construction works peaked in April 2011, with more than 900 subcontractors on site. The work program continued throughout 2011–12, with the majority of construction works scheduled for completion in late 2012. In May 2012, the project schedule was revised on advice from the Managing Contractor, resulting in the date from which ASIO is expected to take possession being adjusted from late 2012 to April 2013. In addition, the project has experienced cost overruns totalling $41.6 million, which equates to an increase of 7 per cent over the approved budget of $589.2 million. 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.

Estate and asset management

ASIO follows a rigorous planned review regime to optimise its facility, plant and equipment management. In anticipation of the move to ASIO's new central office building, a key focus has been the effective management of current assets including equipment and facilities. In instances where new equipment will be installed in the new central office, ASIO invested in minor repairs to extend the life cycle of current assets which will not be relocated.

Efforts throughout 2011–12 focused on the management of current assets and the identification and purchase of assets for movement into ASIO's new central office.

Environmental performance

ASIO is committed to reducing its carbon footprint and implemented various green initiatives during the reporting period to achieve this goal, including:

- saving 180,000 kilowatt hours or 0.9 per cent of total electrical energy consumption, compared to the previous year and despite an expansion of ASIO's IT service infrastructure reducing:
  - energy consumption in data centres by installing motion detectors limiting the times lights are on;
  - energy consumption by 52.2 per cent in information vaults by installing energy efficient lighting; and
  - operating times for building lighting and air-conditioning;
- reducing the distance travelled by corporate vehicles by 461,893 kilometers;
- developing an Environmental Management System, aimed at identifying and controlling the environmental impacts of ASIO; and
- halving the volume of water used to process shredded paper waste.

ASIO also participated in the fifth consecutive Earth Hour event on 31 March 2012.

Financial services

Purchasing

Throughout 2011–12, ASIO continued its practice of adhering to the Commonwealth Procurement Rules and associated Commonwealth Procurement Guidelines. This involved exercising contemporary procurement advice and methodology in order to ensure ASIO procurement activities are effectively managed and deliver value for money.

Details of ASIO's agreements, contracts and standing offers may be made available to members of parliament as a confidential briefing or to the Parliamentary Joint Committee on Intelligence and Security.

Consultants

During 2011-12, 11 new consultancy contracts were entered into involving total actual expenditure of $373,414. In addition, 8 ongoing consultancy contracts were active during 2011-12, involving total actual expenditure of $1,672,244.

Subject to authorised exemptions for the protection of national security, a list of consultancy contracts let to the value of $10,000 or more, inclusive of GST, and the total value of each of those contracts over the life of each contract may be made available to members of parliament as a confidential briefing or to the Parliamentary Joint Committee on Intelligence and Security on request.

Competitive tendering and contracting

ASIO released nine open tenders during 2011–12. Other approaches to market were not advertised publicly for reasons of national security.

Corporate strategy and governance

Strategic reform

During 2011–12 ASIO made considerable progress in the pursuit of organisational change and business modernisation through the implementation of a Roadmap of Key Initiatives. The Roadmap is an important contribution to ASIO being able to maintain its nationally important security intelligence capability into the future.

Notable highlights delivered under the Roadmap include:

- a new streamlined, accountable and more efficient warrants process;
- the development of a robust, reliable case management function supporting clearer prioritisation, tasking and reporting to enhance accountability; and
- the establishment of a new corporate governance committee structure to ensure ASIO is managing resources and risk effectively.

ASIO will remain committed to evaluating and modernising our business systems, processes, technical capability and people strategies in 2012–13.

ASIO's governance committees

In 2011–12 ASIO undertook a review and reform program of ASIO's governance arrangements, including the role and structure of ASIO's corporate committees. In January, a new ASIO committee structure was established to support planning, resource management, risk management, performance monitoring, and accountability and compliance within ASIO.

Under the structure the ASIO Executive Board was established and the number of supporting committees reporting to the board was reduced from nine to four.

The revised ASIO Corporate Committee Framework places particular emphasis on the role of communications and leadership within ASIO. The deliberations and outcomes of ASIO's corporate committees are considered in regular meetings of the ASIO Senior Executive and ASIO Consultative Council.

ASIO Executive Board

At the core of ASIO's corporate governance structure is the high-level executive committee, the ASIO Executive Board. It is chaired by the Director-General, with ASIO's two Deputy Directors-General as the other members.

The Executive Board is ASIO's primary advisory committee to support the Director-General in the governance of the Organisation. It sets the strategic direction of ASIO and acts as the principal forum for managing priorities and resources.

Supporting committees

A number of corporate committees and subcommittees operate in support of the Executive Board. Corporate committees do not assume ultimate decision-making power on matters going to the control of the Organisation—this remains the responsibility of the Director-General.

Intelligence Coordination Committee (ICC)

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

Workforce Capability Committee (WCC)

The WCC considers issues surrounding ASIO's workforce to ensure it is sufficiently sized, skilled, equipped and accommodated to meet the current and future capability needs of the Organisation. The Security Committee and Work Health and Safety Committee operate as sub-committees of the WCC.

ASIO Security Committee (ASC)

The ASC reviews and addresses key issues relevant to the security of ASIO people, property and information technology systems. The committee also provides a consultative forum for the development of security policies.

Work Health and Safety Committee (WHSC)

The WHSC is a mechanism for ensuring staff consultation and cultural integration of safety requirements into the Organisation. The Committee provides strategic guidance and direction on legislative requirement under the *Work Health and Safety Act 2012*.

Finance Committee (FC)

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

New Building Committee (NBC)

The NBC meets each month to provide senior internal governance for the New Building Project, ensuring that the needs of ASIO are effectively and correctly incorporated into building design. The NBC is also responsible for ensuring that the Organisation is prepared to execute a secure transition whilst maintaining its obligations to protect Australia, its people and its interests.

Audit and Risk Committee (ARC)

The ARC provides independent assurance and assistance to the Director-General on ASIO's risk, fraud control and compliance framework, and its financial statement responsibilities. The ARC (in accordance with the Internal Audit Mandate) sets priorities for audit, fraud control and evaluation planning and considers the findings of internal audits and evaluations and ensures management-endorsed recommendations were implemented. The committee has an independant Chair as appointed by the Director-General of Security.

Communications and leadership meetings

Senior Executive Meeting (SEM)

SEM is chaired by the Director-General and attended by the Deputy Directors-General and First Assistant Directors-General. It is a regular forum allowing for the open exchange of emerging corporate and operational issues.

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 on the Organisation.

ASIO Consultative Council (ACC)

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

ASIO Strategic Plan 2011–13

Over the reporting period, ASIO engaged in considered business planning and related investment activities as defined by the goals established in the ASIO Strategic Plan 2011–13.

ASIO Strategic Plan 2011–13

Our mission: to identify and investigate threats to security and provide advice to protect Australia, its people and its interests.

Our vision: the intelligence edge for a secure Australia.

Our work: ASIO will continue to deliver and report to government on four key programs, supporting the government's aim of a secure Australia in a secure region:

- **Security intelligence analysis and advice** to inform stakeholders and our own work in countering terrorism, espionage and other threats to national security. This includes strategic, investigative and complex analysis; threat assessments; policy contribution; support to prosecutions; and advice in regard to border integrity, cyber security and critical infrastructure protection.
- **Protective security advice** to enhance physical, technical, procedural, personnel and information security.
- **Security intelligence investigations and capabilities** to fulfil intelligence collection requirements through all-source security intelligence collection; complex tactical investigations; research and development for technical collection and analysis; and engagement with national and international partners.
- **Foreign intelligence collection** in Australia at the request of the Minister for Foreign Affairs or the Minister for Defence, as well as incidentally through security intelligence investigations.

Effective enabling functions underpin each program in the areas of:

- services to provide support and expertise to the Organisation in people development and management, financial services, information infrastructure and services and property management;
- executive services to provide corporate governance, accountability, strategic coordination and legal and policy advice; and
- security practice in personnel, physical, information and counter-intelligence security to provide assurance to government, our partners and the public.

Our goals

Our four key strategic goals and measures of continuing success will be:

Strengthen intelligence collection and analysis capability

We are leading edge in the collection, management and analysis of intelligence.

We share information with all who need it, when they need it, in a form they can readily use.

Enhance strategic impact

We are active and influential in shaping Australia's response to the national and international security environment.

We ensure that our capabilities and capacity also help our partners.

Build and manage the workforce of the future

We are professional and highly competent with the flexibility, initiative and agility to anticipate and adapt to change.

We exemplify excellence in security, confidentiality and integrity.

Improve business processes and practices

We focus our resources and effort on high value, productive activities.

We build quality and accountability into everything we do.

Our values

Excellence

- We produce high quality, relevant, timely advice.
- We display strong leadership and professionalism.
- We improve through innovation and learning.

Integrity

- We are ethical and work without bias.
- We maintain confidentiality and the security of our work.
- We respect others and value diversity.

Accountability

- We are responsible for what we do and for our outcomes.
- We are accountable to the Australian community through the government and the Parliament.

Cooperation

- We build a common sense of purpose and mutual support.
- We communicate appropriately in all our relationships.
- We foster and maintain productive partnerships.

Risk management

ASIO is committed to a comprehensive, coordinated and systematic approach to managing risk. ASIO's Strategic Risk Management Framework provides an ongoing means for ASIO's senior management to assess, manage and treat strategic risks to the Organisation.

The Strategic Risk Management Framework was reviewed during 2011–12 to ensure that ASIO was best placed to indentify high level risks and mitigate them. Consideration of risk is built into ASIO's decision making processes, project management framework and business planning arrangements.

Using this framework, ASIO is also able to demonstrate that risks and performance issues are escalated, reviewed, considered and addressed by ASIO senior management.

ASIO internal performance reporting

ASIO conducts internal performance reporting quarterly. The reporting is designed to capture cross-organisational input regarding ASIO's performance against stated benchmarks. This allows all divisions to contribute to the evaluation of the Organisation's performance.

ASIO's internal performance reporting is considered by the ASIO Executive Board, allowing for rigorous assessment and oversight of performance and informed decision making relevant to priorities, resourcing and risk.

Enterprise resilience

During the reporting period, the focus of enterprise resilience has been on preparing ASIO for its scheduled move in 2013 to a new central office. This work has included a review of priority business functions, business continuity and disaster recovery planning, the update and implementation of emergency management planning documentation, training and procedures and the annual review of the Organisation's strategic risk management processes.

In order to ensure that ASIO is well prepared to effectively manage a range of unforeseen events within limited resources, the Organisation's Enterprise Resilience framework includes Integrated Security, Business Continuity, Emergency Management and Strategic Risk Management.

Information services

Release of ASIO records

ASIO's records are requested for a range of reasons, including: personal and family history, academic research, and the production of documentary programs and publication.

ASIO is an exempt agency under the *Freedom of Information ACT 1982,* but is subject to the release of its records under the *Archives Act 1983*, which, until recently, provided for public access to all Commonwealth records over 30 years old. This was amended in January 2011 to allow access to records over 20 years old. The transition period of this change will result in full implementation by 2020.

The transition period requires ASIO to assess records in two-year increments, as opposed to the previous one year. It is therefore expected that there will be an increase in the quantity of records requiring assessment which ASIO will have to manage in order to complete requests within the 90 day period.

As part of this release process, ASIO's public research officers work with the National Archives of Australia, to assess any requested records holdings against subsection 33(1) of the Archives Act to determine whether any part of the record—regardless of age—should be redacted. This is to ensure that sensitive information remains protected, under the themes of national security, international relations, privacy or safety concerns.

During 2011–12, ASIO received 631 applications for access to records, an increase from 409 in 2010–11. A total of 505 requests were completed during the reporting period. ASIO assessed 68,608 pages in 2011–12, representing an increase from 48,096 pages in 2010–11.

Type of request	2011–12
Number of requests	631
Number of pages reviewed	68,608
Number of requests completed within 90 days	341
Number of reconsiderations made	4
Number of reconsiderations rejected	1

Applicants dissatisfied with exemptions by ASIO can request a reconsideration of the decision. Four reconsiderations were conducted in 2011–12, with the majority lodged by a single researcher. Changes were made to ASIO exemptions for one of the four reconsiderations. The exempted material was from an overseas liaison partner who upon referral gave approval for the release of the information. Applicants may also lodge an appeal with the Administrative Appeals Tribunal regarding the exemption, or if their request is not completed within 90 days. No appeals were lodged with the AAT in 2011–12.

Applicants also have the ability to lodge a complaint with the Inspector-General of Intelligence and Security if they have concerns with the process to access ASIO records. Over the reporting period no complaints were made to the IGIS regarding the release of ASIO information.

Subject of assessment	2009–10	2010–11	2011–12
Percentage of folios released without exemption	61	57	62
Percentage of folios released with partial exemption	31	41	36
Percentage of folios claimed as totally exempt	2	2	2
Percentage of folios completed within 90 days	86	86	66
Total folios assessed	65,952	48,906	68,608

Moving ASIO records to the new ASIO building

While ASIO mainly uses virtual files, it also manages a large collection of highly classified paper files that need to be moved securely to the new ASIO building. Plans for this significant logistical activity are in place and have been included in ASIO's broader plans for the move to the new building. Contingency measures have also been devised to ensure the records migration task will be completed in the allotted timeframe. Important parts of the intended process were tested and refined in 2011–12.

ASIO records authority

During the reporting period ASIO worked closely with the NAA to undertake the scheduled review of ASIO's Records Authority. In line with NAA's standard practice, the revised Records Authority will be publicly available through the NAA website early in the 2012–13 reporting period.

Official history of ASIO

The progress of ASIO's official history continued through 2011–12, with the concurrent development of the two volumes. The first volume covering 1949–1963 is scheduled for completion in 2013. While the second volume, 1963–1989 is due to be completed in 2015.

The Australian National University (ANU) research team headed by Professor David Horner AM is keenly focused on drawing from a vast array of sources to deliver an accurate and insightful account of ASIO's past, in order to provide the first comprehensive and independent record of the role that ASIO has played since post-World War II. To date, 3000 ASIO files have been accessed by Professor Horner and the ANU History of ASIO team.

Of particular interest is the richness and depth of material being accessed through a range of information sources—ASIO's records and interviews with former prime ministers, director's-general, as well as former ASIO officers.

The History of ASIO project team has been able to locate and interview 15 of the original '49ers' who joined, or were recruited, at the time of the Organisation's inception. In all cases these former officers have been able to provide a remarkable and unique insight into the early years of the Organisation and Australia's role in post-war/Cold War history.

Corrections to the ASIO annual report 2010–11

The following statements in the 2010–11 *Report to Parliament* were identified as incorrect:

- On page 84 of the ASIO 2010–11 *Report to Parliament* the total number of staff employed was reported as 1,769, representing 1,684 full time equivalents. The correct total number of staff employed was 1,767 representing 1,683 full time equivalents. The separation rate during 2010–11 was reported as 5.8 per cent. The correct separation rate for 2010–11 was 5.9 per cent; and
- on page 159 of the ASIO 2010–11 *Report to Parliament*, in Table 6: Composition of workforce 2005–06 to 2010–11, the figures reported for ongoing fulltime staff and non-ongoing casual staff were incorrect. The table below provides the correct information:

	2010–11
Ongoing full-time (excl DG)	1,511
Non-ongoing full time[1]	50
Ongoing part time	148
Non-ongoing part time	16
Non-ongoing casual	42
Total	1,767

[1] Includes attachments and locally engaged staff held against positions in the structure.

Part 6

Financial statements

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2012 are based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.

David Irvine
Director-General of Security

17 September 2012

Australian National Audit Office

INDEPENDENT AUDITOR'S REPORT

To the Attorney-General

I have audited the accompanying financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2012, which comprise: a Statement by the Director-General of Security; Statement of Comprehensive Income; Balance Sheet; Statement of Changes in Equity; Cash Flow Statement; Schedule of Commitments; Schedule of Contingencies; and Notes to and forming part of the Financial Statements comprising a Summary of Significant Accounting Policies and other explanatory information.

Director–General of Security's Responsibility for the Financial Statements

The Director-General of Security is responsible for the preparation of financial statements that give a true and fair view in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards, and for such internal control as is necessary to enable the preparation of the financial statements that give a true and fair view and are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

My responsibility is to express an opinion on the financial statements based on my audit. I have conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. These auditing standards require that I comply with relevant ethical requirements relating to audit engagements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the Australian Security Intelligence Organisation's preparation of the financial statements that give a true and fair view in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Australian Security Intelligence Organisation's internal control. An audit also includes evaluating the appropriateness of the accounting policies used and the reasonableness of accounting estimates made by the

GPO Box 707 CANBERRA ACT 2601
19 National Circuit BARTON ACT 2600
Phone (02) 6203 7300 Fax (02) 6203 7777

Director-General of Security of the Australian Security Intelligence Organisation, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

Independence

In conducting my audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

Opinion

In my opinion, the financial statements of the Australian Security Intelligence Organisation:

(a) have been prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards; and

(b) give a true and fair view of the matters required by the Finance Minister's Orders including the Australian Security Intelligence Organisation's financial position as at 30 June 2012 and of its financial performance and cash flows for the year then ended.

Australian National Audit Office

Rebecca Reilly
Executive Director

Delegate of the Auditor-General

Canberra

17 September 2012

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2012

	Notes	2012 $ '000	2011 $ '000
EXPENSES			
Employee benefits	3A	**208,386**	186,529
Suppliers	3B	**146,299**	159,528
Depreciation and amortisation	3C	**40,173**	39,035
Finance costs	3D	**807**	328
Write-down and impairment of assets	3E	**434**	550
Sale of assets	3F	**137**	(24)
Foreign exchange losses — non-speculative		**2**	1
Total expenses		**396,238**	385,947
Less:			
OWN-SOURCE INCOME			
Own-source revenue			
Sale of goods and rendering of services	4A	**22,388**	7,613
Total own-source revenue		**22,388**	7,613
Gains			
Other gains	4B	**232**	577
Total gains		**232**	577
Total own-source income		**22,620**	8,190
Net cost of services		**373,618**	377,757
Revenue from government	4C	**328,124**	344,883
Deficit attributable to the Australian Government		**(45,494)**	(32,873)
OTHER COMPREHENSIVE INCOME			
Changes in asset revaluation reserves		**-**	-
Total comprehensive loss attributable to the Australian Government		**(45,494)**	(32,873)

The above statement should be read in conjunction with the accompanying notes.

BALANCE SHEET
as at 30 June 2012

	Notes	2012 $ '000	2011 $ '000
ASSETS			
Financial assets			
Cash		**12,775**	18,885
Trade and other receivables	5A	**234,183**	304,240
Other financial assets	5B	**4,378**	594
Total financial assets		**251,336**	323,719
Non-financial assets			
Land and buildings	6A,D	**212,695**	111,966
Infrastructure, plant and equipment	6B,D	**78,779**	81,466
Intangibles	6C,E	**15,440**	6,884
Other non-financial assets	6F	**15,503**	14,144
Total non-financial assets		**322,417**	214,460
Total assets		**573,753**	538,179
LIABILITIES			
Payables			
Suppliers	7A	**14,785**	9,499
Lease incentives	7B	**2,756**	3,312
Other payables	7C	**9,297**	10,262
Total payables		**26,838**	23,073
Provisions			
Employee provisions	8A	**58,867**	45,472
Restoration obligations	8B	**9,979**	7,105
Total provisions		**68,846**	52,577
Total liabilities		**95,684**	75,650
Net assets		**478,069**	462,529
EQUITY			
Parent equity interest			
Contributed equity		**488,079**	427,045
Reserves		**8,102**	8,102
Retained surplus (deficit)		**(18,112)**	27,382
Total equity		**478,069**	462,529

The above statement should be read in conjunction with the accompanying notes.

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2012

	Retained Earnings		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2012	2011	**2012**	2011	**2012**	2011	**2012**	2011
	$'000	$'000	**$'000**	$'000	**$'000**	$'000	**$'000**	$'000
Opening balance	**27,382**	60,255	**8,102**	8,102	**427,045**	392,187	**462,529**	460,544
Comprehensive income								
Deficit for the period	**(45,494)**	(32,873)	**-**	-	**-**	-	**(45,494)**	(32,873)
Total comprehensive income	**(45,494)**	(32,873)	**-**	-	**-**	-	**(45,494)**	(32,873)
Transactions with owners								
Distributions to owners								
Return of appropriation	**-**	-	**-**	-	**-**	(31,020)	**-**	(31,020)
Total distributions to owners	**-**	-	**-**	-	**-**	(31,020)	**-**	(31,020)
Contributions by owners								
Equity injection — appropriation	**-**	-	**-**	-	**41,806**	61,186	**41,806**	61,186
Departmental capital budget	**-**	-	**-**	-	**19,228**	4,692	**19,228**	4,692
Total contributions by owners	**-**	-	**-**	-	**61,034**	65,878	**61,034**	65,878
Closing balance attributable to the Australian Government	**(18,112)**	27,382	**8,102**	8,102	**488,079**	427,045	**478,069**	462,529

The above statement should be read in conjunction with the accompanying notes.

CASH FLOW STATEMENT
for the period ended 30 June 2012

	Notes	2012 $ '000	2011 $ '000
OPERATING ACTIVITIES			
Cash received			
Appropriations		**427,493**	351,409
Sales of goods and rendering of services		**20,202**	8,857
Net GST received		**11,041**	13,196
Other cash received		**12,463**	3,443
Total cash received		**471,198**	376,905
Cash used			
Employees		**195,772**	180,786
Suppliers		**168,935**	179,073
Section 31 receipts transferred to OPA		**19,856**	3,606
Total cash used		**384,562**	363,465
Net cash from operating activities	9	**86,636**	13,440
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		**884**	634
Total cash received		**884**	634
Cash used			
Purchase of property, plant and equipment		**133,806**	48,960
Purchase of intangibles		**13,859**	3,228
Total cash used		**147,665**	52,188
Net cash used by investing activities		**(146,781)**	(51,554)
FINANCING ACTIVITIES			
Cash received			
Appropriations — contributed equity		**54,034**	39,474
Total cash received		**54,034**	39,474
Net cash from financing activities		**54,034**	39,474
Net increase or (decrease) in cash held		**(6,110)**	1,360
Cash and cash equivalents at the beginning of the reporting period		**18,885**	17,525
Cash and cash equivalents at the end of the reporting period		**12,775**	18,885

The above statement should be read in conjunction with the accompanying notes.

SCHEDULE OF COMMITMENTS
as at 30 June 2012

	Notes	2012 $ '000	2011 $ '000
BY TYPE			
Commitments receivable			
Sublease rental income		**1,993**	589
Net GST recoverable on commitments		**11,962**	11,787
Total commitments receivable		**13,955**	12,376
Commitments payable			
Capital commitments			
Land and buildings	A	**36,716**	130,529
Infrastructure, plant and equipment	A	**15,885**	2,250
Intangibles		**275**	-
Total capital commitments		**52,876**	132,779
Other commitments			
Operating leases	B	**91,063**	101,300
Other commitments		**29,713**	31,693
Total other commitments		**120,776**	132,993
Net commitments by type		**159,697**	253,396

Commitments are GST inclusive where relevant.

No contingent rentals exist. There are no renewal or purchase options available to ASIO.

A. Buildings, plant and equipment commitments are primarily contracts for purchases of fit-out, furniture and fittings for a new building.

B. Operating leases included are effectively non-cancellable and comprise:

- *Agreements for the provision of motor vehicles to senior executive and other officers*
- *Leases for office accommodation*

  Various arrangements apply to the review of lease payments:

  - annual review based on upwards movement in the consumer price index (CPI);
  - biennial review based on the CPI; and
  - biennial review based on market appraisal.

SCHEDULE OF COMMITMENTS
continued

	Notes	2012 $ '000	2011 $ '000
BY MATURITY			
Commitments receivable			
Sublease rental income			
One year or less		**976**	589
From one to five years		**1,017**	-
Total operating lease income		**1,993**	589
Other commitments receivable			
One year or less		**5,584**	4,238
From one to five years		**5,206**	5,851
Over five years		**1,172**	1,697
Total other commitments receivable		**11,962**	11,786
Commitments payable			
Capital commitments			
One year or less		**52,876**	132,475
From one to five years		**-**	305
Total capital commitments		**52,876**	132,780
Operating lease commitments			
One year or less		**22,805**	23,174
From one to five years		**55,370**	59,449
Over five years		**12,888**	18,677
Total operating lease commitments		**91,063**	101,300
Other commitments			
One year or less		**26,058**	24,933
From one to five years		**3,655**	6,760
Total other commitments		**29,713**	31,693
Net commitments by maturity		**159,697**	253,398

The above schedule should be read in conjunction with the accompanying notes.

SCHEDULE OF CONTINGENCIES
as at 30 June 2012

	2012 $ '000 Claims for damages or costs	2011 $ '000
Contingent liabilities		
Balance from previous period	-	-
New	-	-
Total contingent liabilities	-	-
Net contingent liabilities	-	-

Details of each class of contingent liabilities and assets, including those not included above because they cannot be quantified or are considered remote, are disclosed in Note 10: Contingent Liabilities and Assets.

The above schedule should be read in conjunction with the accompanying notes.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

for the year ended 30 June 2012

Note 1: Summary of significant accounting policies

1.1 Objective of ASIO

ASIO is an Australian Government-controlled entity. It is a not-for-profit entity. The objective of ASIO is to provide advice, in accordance with the ASIO Act, to ministers and appropriate agencies and authorities, to protect Australia and its people from threats to national security.

ASIO is structured to meet the outcome: *To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government.*

ASIO activities contributing towards the outcome are classified as departmental. Departmental activities involve the use of assets, liabilities, revenues and expenses controlled or incurred by ASIO in its own right.

The continuing existence of ASIO in its present form and with its present programs is dependent on government policy and on continuing appropriations by parliament.

1.2 Basis of preparation of the financial statements

The financial statements have been prepared in accordance with:

- Finance Minister's Orders (FMOs) for reporting periods ending on or after 1 July 2011; and
- Australian Accounting Standards and interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial statements have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets and liabilities at fair value or amortised cost. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position.

The financial statements are presented in Australian dollars and values are rounded to the nearest thousand dollars unless otherwise specified.

Unless an alternative treatment is specifically required by an accounting standard or the FMOs, assets and liabilities are recognised in the balance sheet when, and only when, it is probable that future economic benefits will flow to ASIO or a future sacrifice of economic benefits will be required and the amounts of the assets or liabilities can be reliably measured.

However, assets and liabilities arising under agreements equally proportionately unperformed are not recognised unless required by an accounting standard. Liabilities and assets that are unrecognised are reported in the Schedule of Commitments or the Schedule of Contingencies.

Unless alternative treatment is specifically required by an accounting standard, income and expenses are recognised in the Statement of Comprehensive Income when, and only when, the flow or consumption or loss of economic benefits has occurred and can be reliably measured.

1.3 Significant accounting judgements and estimates

In the process of applying the accounting policies listed in this note, ASIO has made the following judgements that have the most significant impact on the amounts recorded in the financial statements:

> The fair value of land and buildings has been taken to be the market value of similar properties as determined by an independent valuer. In some instances, ASIO buildings are purpose built and may in fact realise more or less in the market.

No accounting assumptions or estimates have been identified that have a significant risk of causing a material adjustment to carrying amounts of assets and liabilities within the next reporting period.

1.4 New Australian accounting standards

Adoption of new Australian accounting standard requirements

No accounting standard has been adopted earlier than the application date as stated in the standard. Other new standards and amendments to standards that were issued prior to the signing of the statement by the Director-General and are applicable to the current reporting period did not have a financial impact, and are not expected to have a future financial impact on the entity.

Future Australian accounting standard requirements

New standards, amendments to standards or interpretations that have been issued by the Australian Accounting Standards Board but are effective for future reporting periods will have no material financial impact on future reporting periods.

1.5 Revenue

Revenue from the sale of goods is recognised when:

- the risks and rewards of ownership have been transferred to the buyer;
- the seller retains no managerial involvement or effective control over the goods;
- the revenue and transaction costs incurred can be reliably measured; and
- it is probable that the economic benefits associated with the transaction will flow to the entity.

Revenue from the rendering of services is recognised by reference to the stage of completion of contracts at the reporting date. The revenue is recognised when:

- the amount of revenue, stage of completion and transaction costs incurred can be reliably measured; and
- the probable economic benefits associated with the transaction will flow to the entity.

The stage of completion of contracts at the reporting date is determined by reference to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

Receivables for goods and services, which have 30-day terms, are recognised at nominal amounts due less any impairment allowance amount. Collectability of debts is reviewed at the end the of reporting period. Allowances are made when collectability of the debt is no longer probable.

Revenue from government

Amounts appropriated for departmental output appropriations for the year (adjusted for any formal additions and reductions) are recognised as revenue from government when ASIO gains control of the appropriation, except for certain amounts that relate to activities that are reciprocal in nature, in which case revenue is recognised only when it has been earned.

Appropriations receivable are recognised at their nominal amounts.

1.6 Gains

Resources received free of charge

Resources received free of charge are recognised as gains when, and only when, a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense.

Resources received free of charge are recorded as either revenue or gains depending on their nature.

Sale of assets

Gains from disposal of assets are recognised when control of the asset has passed to the buyer.

1.7 Transactions with the government as owner

Equity injections

Amounts appropriated which are designated as 'equity injections' for a year (less any formal reductions) and Departmental Capital Budgets (DCBs) are recognised directly in Contributed Equity in that year.

Distributions to owners

The FMOs require that distributions to owners be debited to contributed equity unless it is in the nature of a dividend. In 2010–11 ASIO relinquished control of appropriation funding of $31.02 million.

1.8 Employee benefits

Liabilities for 'short-term employee benefits' (as defined in *AASB 119 Employee Benefits*) and termination benefits due within 12 months of the balance date are measured at their nominal amounts.

The nominal amount is calculated with regard to the rates expected to be paid on settlement of the liability.

Other employee benefit liabilities are measured as the net total of the present value of the defined benefit obligation at the end of the reporting period minus the fair value at the end of the reporting period of plan assets (if any) out of which the obligations are to be settled directly.

Leave

The liability for employee entitlements includes provision for annual leave and long service leave. No provision has been made for sick leave, as all sick leave is non-vesting and the average sick leave taken in future years by employees of ASIO is estimated to be less than the annual entitlement for sick leave.

The leave liabilities are calculated on the basis of employees' remuneration at the estimated salary rates that apply at the time the leave is taken, including ASIO's employer superannuation contribution rates, to the extent that the leave is likely to be taken during service rather than paid out on termination.

Separation and redundancy

Provision is made for separation and redundancy benefit payments. ASIO recognises a provision for terminations when it has developed a detailed formal plan for the terminations and has informed those employees affected that it will carry out the terminations.

Superannuation

Staff of ASIO are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS), the PSS accumulation plan (PSSap) or other complying superannuation funds.

The CSS and PSS are defined benefit schemes for the Australian Government. The PSSap and other complying funds are defined contribution schemes.

The liability for defined benefits is recognised in the financial statements of the Australian Government and is settled by the Australian Government in due course. This liability is reported by the Department of Finance and Deregulation's administered schedules and notes.

ASIO makes employer contributions to the employees' superannuation scheme at rates determined by an actuary to be sufficient to meet the current cost to the Government. ASIO accounts for the contributions as if they were contributions to defined contribution plans.

Superannuation payable as at 30 June represents outstanding contributions for the final fortnight of the year.

1.9 Leases

A distinction is made between finance leases and operating leases. Finance leases effectively transfer from the lessor to the lessee substantially all the risks and rewards incidental to ownership of leased assets. An operating lease is a lease that is not a finance lease. In operating leases, the lessor effectively retains substantially all such risks and benefits.

Where an asset is acquired by means of a finance lease, the asset is capitalised at either the fair value of the lease property or, if lower, the present value of minimum lease payments at the inception of the contract and a liability recognised at the same time and for the same amount.

The discount rate used is the interest rate implicit in the lease. Leased assets are amortised over the period of the lease. Lease payments are allocated between the principal component and the interest expense.

Operating lease payments are expensed on a straight line basis which is representative of the pattern of benefits derived from the leased assets.

1.10 Cash

Cash is recognised at its nominal amount. Cash includes:

- cash on hand; and
- demand deposits in bank accounts with an original maturity of three months or less that are readily convertible to known amounts of cash and subject to insignificant risk of changes in value.

1.11 Financial assets

ASIO classifies its financial assets as 'loans and receivables'.

Financial assets are recognised and derecognised upon 'trade date'.

Effective interest method

The effective interest method is a method of calculating the amortised cost of a financial asset and of allocating interest income over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash receipts through the expected life of the financial asset or, where appropriate, a shorter period.

Receivables

Trade receivables and other receivables that have fixed or determinable payments that are not quoted in an active market are classified as 'loans and receivables'. Loans and receivables are measured at amortised cost using the effective interest method less impairment. Interest is recognised by applying the effective interest rate.

Impairment of financial assets

Financial assets are assessed for impairment at the end of each reporting period.

Financial assets held at cost - if there is objective evidence that an impairment loss has been incurred, the amount of the impairment loss is valued at cost.

1.12 Financial liabilities

Financial liabilities are recognised and derecognised upon 'trade date'.

Other financial liabilities

Other financial liabilities are initially measured at fair value, net of transaction costs. These liabilities are subsequently measured at amortised cost using the effective interest method, with interest expense recognised on an effective yield basis.

The effective interest method is a method of calculating the amortised cost of a financial liability and of allocating interest expense over the relevant period. The effective interest rate is the rate that exactly discounts estimated future cash payments through the expected life of the financial liability or, where appropriate, a shorter period.

Supplier and other payables are recognised at amortised cost. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced).

1.13 Contingent liabilities and contingent assets

Contingent Liabilities and Contingent Assets are not recognised in the balance sheet but are reported in the relevant schedules and notes. They may arise from uncertainty as to the existence of a liability or asset or represent an existing liability or asset in respect of which the amount cannot be reliably measured. Contingent Assets are reported when settlement is probable, but not virtually certain, and contingent liabilities are recognised when settlement is greater than remote.

1.14 Acquisition of assets

Assets are recorded at cost on acquisition except as stated below. The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken. Financial assets are initially measured at their fair value plus transaction costs where appropriate.

Assets acquired at no cost, or for nominal consideration, are initially recognised as assets and revenues at their fair value at the date of acquisition, unless acquired as a consequence of restructuring of administrative arrangements. In the latter case, assets are initially recognised as contributions by owners at the amounts at which they were recognised in the transferor's accounts immediately prior to the restructuring.

1.15 Property, plant and equipment

Asset recognition threshold

Purchases of property, plant and equipment are recognised initially at cost in the balance sheet, except for purchases costing less than $4,000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

The initial cost of an asset includes an estimate of the cost of dismantling and removing the item and restoring the site on which it is located. This is particularly relevant to restoration obligation provisions in property leases taken up by ASIO where there exists an obligation to restore the property to its original condition. These costs are included in the value of ASIO's leasehold improvements with a corresponding provision for the restoration obligation recognised.

Revaluations

Fair values for each class of asset are determined as shown below:

Asset class	Fair value measured at:
Land	market selling price
Buildings	market selling price
Leasehold	depreciated replacement cost
Plant and equipment	market selling price

Following initial recognition at cost, property, plant and equipment are carried at fair value less accumulated depreciation and accumulated impairment losses. Valuations are conducted with sufficient frequency to ensure that the carrying amounts of assets do not materially differ from the assets' fair values as at the reporting date. The regularity of independent valuations depends upon the volatility of movements in market values for the relevant assets.

Revaluation adjustments are made on a class basis. Any revaluation increment is credited to equity under the heading of 'asset revaluation reserve' except to the extent that it reverses a previous revaluation decrement of the same asset class that was previously recognised in the surplus/deficit. Revaluation decrements for a class of assets are recognised directly in the surplus/deficit except to the extent that they reverse a previous revaluation increment for that class.

Any accumulated depreciation as at the revaluation date is eliminated against the gross carrying amount of the asset and the asset restated to the revalued amount.

Depreciation

Depreciable property, plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to ASIO using, in all cases, the straight-line method of depreciation. Leasehold improvements are depreciated on a straight-line basis over the lesser of the estimated useful life of the improvements or the unexpired period of the lease.

Depreciation rates (useful lives), residual values and methods are reviewed at each reporting date and necessary adjustments are recognised in the current or current and future reporting periods, as appropriate.

Depreciation rates applying to each class of depreciable asset are based on the following useful lives:

	2012	2011
Buildings on freehold land	**25–40 years**	25–40 years
Leasehold improvements	**lease term**	lease term
Plant and equipment	**2–20 years**	2–20 years

Impairment

All assets were assessed for impairment at 30 June 2012. Where indications of impairment exist, the asset's recoverable amount is estimated and an impairment adjustment made if the asset's recoverable amount is less than its carrying amount.

The recoverable amount of an asset is the higher of its fair value less costs to sell and its value in use. Value in use is the present value of the future cash flows expected to be derived from the asset. Where the future economic benefit of an asset is not primarily dependent on the asset's ability to generate future cash flows, and the asset would be replaced if ASIO were deprived of the asset, its value in use is taken to be its depreciated replacement cost.

Derecognition

An asset is derecognised upon disposal or when no further future economic benefits are expected from its use or disposal.

1.16 Intangibles

ASIO's intangibles comprise internally developed and purchased software for internal use. These assets are carried at cost less accumulated amortisation and accumulated impairment losses.

Software is amortised on a straight-line basis over its anticipated useful life. The useful life of ASIO's software is 4–5 years (2010–11: 4–5 years).

All software assets were assessed for indications of impairment as at 30 June 2012.

1.17 Taxation

ASIO is exempt from all forms of taxation except fringe benefits tax and the goods and services tax (GST).

Revenues, expenses and assets are recognised net of GST:

- except where the amount of GST incurred is not recoverable from the Australian Taxation Office; and
- except for receivables and payables.

Note 2: Events after the balance sheet date

On 22 August 2012 the Director-General of Security announced a voluntary redundancy program targeted at Senior Executive Service officers. This was in response to an evaluation of the Organisation's future needs against ongoing financial budget pressures. Acceptance of redundancies is voluntary and, at the date of signing the financial statements, none had been finalised. The financial effect could not, therefore, be determined. (2011: Nil).

Note 3: Expenses

	2012 $ '000	2011 $ '000
Note 3A: Employee benefits		
Wages and salaries	**156,495**	143,365
Superannuation:		
Defined contribution plans	**4,726**	10,001
Defined benefit plans	**22,156**	17,574
Leave and other entitlements	**23,126**	14,552
Separation and redundancies	**1,883**	1,037
Total employee benefits	**208,386**	186,529
Note 3B: Suppliers		
Provision of goods — related entities	**664**	1,160
Provision of goods — external entities	**7,528**	7,833
Rendering of services — related entities	**26,638**	31,372
Rendering of services — external entities	**88,798**	95,412
Operating lease rentals — related entities:		
minimum lease payments	**3,850**	3,468
Operating lease rentals — external entities:		
minimum lease payments	**16,378**	18,540
Workers' compensation premiums	**2,443**	1,743
Total supplier expenses	**146,299**	159,528
Note 3C: Depreciation and amortisation		
Depreciation		
Infrastructure, plant and equipment	**23,403**	21,124
Buildings	**11,525**	11,071
Total depreciation	**34,928**	32,195
Amortisation — Intangibles — computer software	**5,245**	6,840
Total depreciation and amortisation	**40,173**	39,035
Note 3D: Finance costs		
Unwinding of discount — restoration obligations	**807**	328

	2012 $ '000	2011 $ '000

Note 3E: Write-down and impairment of assets

Asset write-downs from:		
Impairment of receivables	**21**	4
Write-down of land and buildings	**-**	325
Write-down of property, plant and equipment	**355**	158
Write-down of intangible assets	**58**	63
Total write-down and impairment of assets	**434**	550

Note 3F: Sale of assets

Infrastructure, plant and equipment		
Proceeds from sale	**(884)**	(634)
Carrying value of assets sold	**1,021**	610
Net loss from sale of assets	**137**	(24)

Note 4: Income

Note 4A: Sale of goods and rendering of services

Provision of goods — related entities	**12**	15
Provision of goods — external entities	**7**	145
Rendering of services — related entities	**18,063**	5,653
Rendering of services — external entities	**3,000**	230
Rental income — related entities	**1,261**	1,555
Rental income — external entities	**45**	15
Total sale of goods and rendering of services	**22,388**	7,613

Note 4B: Gains

Resources received free of charge	**115**	110
Other	**117**	467
Total gains	**232**	577

	2012 $ '000	2011 $ '000

Note 4C: Revenue from government

Appropriation — Departmental appropriations	**328,124**	344,883

Note 5: Financial assets

Note 5A: Trade and other receivables

Goods and services		
Related entities	**5,497**	2,908
External entities	**246**	115
Total receivables for goods and services	**5,743**	3,023
Appropriations receivable for existing programs	**226,225**	298,738
GST receivable from the Australian Taxation Office	**2,215**	2,479
Total trade and other receivables (gross)	**234,183**	304,240
Less impairment allowance account:	**-**	-
Total trade and other receivables (net)	**234,183**	304,240

All receivables are expected to be recovered in no more than 12 months.

Receivables are aged as follows:		
Not overdue	**231,437**	303,911
Overdue by:		
less than 30 days	**589**	150
30 to 60 days	**63**	102
61 to 90 days	**1,874**	9
more than 90 days	**220**	68
Total receivables (gross)	**234,183**	304,240

Reconciliation of the impairment allowance account	**Goods & services**	Goods & services
Opening balance	**-**	-
amounts written off	**-**	-
Closing balance	**-**	-

	2012 $ '000	2011 $ '000

Note 5B: Other financial assets

Accrued revenue	**4,378**	594

All accrued revenue is expected to be recovered in no more than 12 months.

Note 6: Non-financial assets

Note 6A: Land and buildings

Land at fair value	**1,515**	1,515
Buildings on freehold land		
fair value	**7,746**	7,653
accumulated depreciation	**(1,192)**	(530)
Total buildings on freehold land	**6,554**	7,123
Leasehold improvements		
work in progress	**150,074**	40,472
fair value	**78,139**	75,910
accumulated depreciation	**(23,587)**	(13,054)
Total leasehold improvements	**204,626**	103,328
Total land and buildings (non-current)	**212,695**	111,966

No indicators of impairment were found for land and buildings.

Note 6B: Infrastructure, plant and equipment

Infrastructure, plant and equipment		
work in progress	**139**	96
fair value	**126,713**	106,917
accumulated depreciation	**(48,073)**	(25,547)
Total Infrastructure, plant and equipment (non-current)	**78,779**	81,466

No indicators of impairment were found for infrastructure, plant and equipment.

	2012 $ '000	2011 $ '000

Note 6C: Intangibles

Computer software		
purchased — at cost	**16,827**	13,602
internally developed — in progress	**1,892**	165
internally developed — in use	**23,313**	14,799
accumulated amortisation	**(25,467)**	(20,557)
accumulated impairment	**(1,125)**	(1,125)
Total computer software	**15,440**	6,884
Total intangibles (non-current)	**15,440**	6,884

No indicators of impairment were found for intangibles.

Note 6D: Reconciliation of the opening and closing balances of property, plant and equipment (2011–12)

	Land	Buildings	Buildings—leasehold improvement	Infrastructure, plant & equipment	Total
	$'000	$'000	$'000	$'000	$'000
As at 1 July 2011					
Gross book value	**1,515**	**7,653**	**116,381**	**107,013**	**232,562**
Accumulated depreciation and impairment	**-**	**(530)**	**(13,054)**	**(25,547)**	**(39,131)**
Net book value 1 July 2011	**1,515**	**7,123**	**103,328**	**81,466**	**193,431**
Additions by purchase	**-**	**93**	**112,161**	**22,092**	**134,346**
Depreciation expense	**-**	**(662)**	**(10,863)**	**(23,403)**	**(34,928)**
Disposals	**-**	**-**	**-**	**(1,377)**	**(1,377)**
Net book value 30 June 2012	**1,515**	**6,554**	**204,626**	**78,779**	**291,474**
Net book value as at 30 June 2012 represented by:					
Gross book value	**1,515**	**7,746**	**228,213**	**126,852**	**364,326**
Accumulated depreciation and impairment	**-**	**(1,192)**	**(23,587)**	**(48,073)**	**(72,852)**
	1,515	**6,554**	**204,626**	**78,779**	**291,474**

Reconciliation of the opening and closing balances of property, plant and equipment (2010–11)

As at 1 July 2010					
Gross book value	1,515	7,653	88,828	87,893	185,889
Accumulated depreciation and impairment	-	(105)	(2,470)	(5,555)	(8,130)
Net book value 1 July 2010	1,515	7,548	86,358	82,338	177,759
Additions by purchase	-	-	27,941	21,017	48,958
Depreciation expense	-	(424)	(10,647)	(21,123)	(32,194)
Disposals	-	-	(325)	(768)	(1,093)
Net book value 30 June 2011	1,515	7,123	103,328	81,466	193,431
Net book value as at 30 June 2011 represented by:					
Gross book value	1,515	7,653	116,381	107,013	232,562
Accumulated depreciation and impairment	-	(530)	(13,054)	(25,547)	(39,131)
	1,515	7,123	103,328	81,466	193,431

Note 6E: Reconciliation of the opening and closing balances of intangibles (2011–12)

	Computer software		
	Internally developed	Purchased	Total
	$'000	$'000	$'000
As at 1 July 2011			
Gross book value	**14,964**	**13,602**	**28,566**
Accumulated amortisation and impairment	**(11,418)**	**(10,264)**	**(21,682)**
Net book value 1 July 2011	**3,546**	**3,338**	**6,884**
Additions by purchase or internally developed	**10,241**	**3,617**	**13,858**
Amortisation expense	**(3,250)**	**(1,994)**	**(5,245)**
Disposals — other	**-**	**(58)**	**(58)**
Net book value 30 June 2012	**10,536**	**4,904**	**15,440**
Net book value as at 30 June 2012 represented by:			
Gross book value	**25,205**	**16,827**	**42,032**
Accumulated amortisation and impairment	**(14,669)**	**(11,923)**	**(26,592)**
	10,536	**4,904**	**15,440**

Reconciliation of the opening and closing balances of intangibles (2010–11)

As at 1 July 2010			
Gross book value	21,002	17,884	38,886
Accumulated amortisation and impairment	(15,816)	(12,511)	(28,327)
Net book value 1 July 2010	5,186	5,373	10,559
Additions by purchase or internally developed	1,560	1,668	3,228
Amortisation expense	(3,200)	(3,639)	(6,840)
Disposals - other	-	(63)	(63)
Net book value 30 June 2011	3,545	3,339	6,884
Net book value as at 30 June 2011 represented by:			
Gross book value	14,964	13,602	28,566
Accumulated amortisation and impairment	(11,418)	(10,264)	(21,682)
	3,545	3,339	6,884

Note 6F: Other non-financial assets

	2012 $ '000	2011 $ '000
Prepayments	**15,503**	12,585
Other debtors	**-**	1,559
Total other non-financial assets	**15,503**	14,144
Total other non-financial assets are expected to be recovered in:		
No more than 12 months	**13,993**	13,908
More than 12 months	**1,510**	236
	15,503	14,144

No indicators of impairment were found for other non-financial assets.

Note 7: Payables

Note 7A: Suppliers

Trade creditors and accruals	**14,785**	9,499
Supplier payables expected to be settled within 12 months:		
Related entities	**3,562**	141
External entities	**11,223**	9,358
	14,785	9,499

Settlement is usually made within 30 days.

Note 7B: Lease incentives

Lease incentives	**2,756**	3,312
Lease incentives are expected to be settled in:		
No more than 12 months	**588**	577
More than 12 months	**2,168**	2,735
	2,756	3,312

Note 7C: Other payables

Salaries and wages	**4,241**	3,955
Superannuation	**778**	1,845
Unearned income	**110**	791
Fringe benefits tax	**856**	665
Rent payable	**3,312**	3,006
Total other payables	**9,297**	10,262

Rent payable is expected be settled over properties' various remaining lease terms (1 to 8 years). All other payables are expected to be settled in no more than 12 months.

Note 8: Provisions

	2012 $ '000	2011 $ '000

Note 8A: Employee provisions

Leave	**57,465**	44,360
Redundancies	**520**	-
Superannuation	**882**	1,112
Total employee provisions	**58,867**	45,472
Employee provisions are expected to be settled in:		
No more than 12 months	**40,194**	30,522
More than 12 months	**18,673**	14,950
	58,867	45,472

Note 8B: Restoration obligations

Restoration obligations	**9,979**	7,105
Restoration obligations are expected to be settled in:		
No more than 12 months	**260**	17
More than 12 months	**9,719**	7,088
	9,979	7,105
Carrying amount 1 July 2011	**7,105**	
Revaluations	**2,067**	
Unwinding of discount or change in discount rate	**807**	
Closing balance	**9,979**	

ASIO currently has agreements for the leasing of premises which have provisions requiring ASIO to restore the premises to their original condition at the conclusion of the lease. ASIO has made a provision to reflect the present value of this obligation.

Note 9: Cash flow reconciliation

	2012 $ '000	2011 $ '000
Reconciliation of cash per balance sheet to cash flow statement		
Report cash as per:		
Cash flow statement	**12,775**	18,885
Balance sheet	**12,775**	18,885
Reconciliation of net cost of services to net cash from operating activities:		
Net cost of services	**(373,618)**	(377,757)
Add revenue from government	**328,124**	344,883
Adjustments for non-cash items		
Depreciation/amortisation	**40,173**	39,035
Net write-down of non-financial assets	**413**	546
Net loss on disposal of assets	**137**	(24)
Changes in assets/liabilities		
(Increase)/decrease in receivables	**77,057**	2,368
(Increase)/decrease in accrued revenue	**(3,784)**	280
(Increase)/decrease in prepayments	**(1,359)**	(1,855)
Increase/(decrease) in employee provisions	**13,395**	3,574
Increase/(decrease) in restoration obligations	**2,874**	308
Increase/(decrease) in reorganisation costs	**-**	(305)
Increase/(decrease) in lease incentives	**(556)**	(557)
Increase/(decrease) in supplier payables	**4,744**	(653)
Increase/(decrease) in other payables	**(965)**	3,596
Net cash from/(used by) operating activities	**86,636**	13,440

Note 10: Contingent liabilities and assets

Quantifiable contingencies

The schedule of contingencies reports no contingent liabilities in respect of claims for damages/costs (2011: Nil).

Unquantifiable contingencies

At 30 June 2012, ASIO had a number of legal claims against it. ASIO has denied liability and is defending the claims. It is not possible to estimate amounts of any eventual payments that may be required in relation to these claims (2011: Nil).

Significant remote contingencies

ASIO does not have any significant remote contingencies.

Note 11: Remuneration of auditors

Financial statement audit services are provided free of charge to ASIO by the Australian National Audit Office. No other services were provided by the Auditor-General.

	2012 $	2011 $
Fair value	**115,000**	110,000

Note 12: Senior executive remuneration

Note 12A: Senior executive expense for the reporting period

	2012	2011
Short-term employee benefits:		
Salary	**11,465,960**	9,076,719
Annual leave accrued	**941,931**	823,379
Performance bonuses	**-**	536,654
Motor vehicle and other allowances	**1,500,039**	1,364,059
Total short-term employee benefits	**13,907,930**	11,800,811
Post-employment benefits		
Superannuation	**2,383,594**	2,008,325
Other long-term benefits		
Long-service leave accrued	**308,613**	268,456
Termination benefits	**247,197**	673,112
Total	**16,847,334**	14,750,704

Note 12A includes the portion of employees' remuneration relating to SES acting arrangements and part-year services where their total remuneration for the year is greater than $150,000.

Note 12A is prepared on an accrual basis and therefore performance bonus expenses disclosed will differ from the cash 'bonus paid' in note 12B.

Note 12B: Average annual reportable remuneration paid to substantive senior executives during the reporting period

Average annual reportable remuneration	Senior executives	Reportable salary	Contributed superannuation	Bonus paid	Total
	No.	$	$	$	$
2012					
Total remuneration:					
$0 to $150,000	**6**	**40,527**	**15,417**	**3,749**	**59,693**
$150,000 to $180,000	**4**	**129,476**	**34,799**	**7,735**	**172,010**
$180,000 to $210,000	**5**	**140,444**	**49,399**	**8,772**	**198,614**
$210,000 to $240,000	**22**	**175,996**	**45,652**	**7,685**	**229,333**
$240,000 to $270,000	**14**	**193,612**	**50,003**	**8,201**	**251,817**
$270,000 to $300,000	**11**	**216,745**	**57,845**	**11,158**	**285,748**
$300,000 to $330,000	**2**	**232,688**	**68,643**	**12,464**	**313,795**
$360,000 to $390,000	**1**	**282,866**	**79,159**	**4,827**	**366,852**
$450,000 to $480,000	**1**	**347,221**	**116,690**	**-**	**463,910**
Total	**66**				
2011					
Total remuneration:					
$0 to $150,000	11	69,070	16,366	4,028	89,465
$150,000 to $180,000	5	132,748	30,746	7,089	170,584
$180,000 to $210,000	12	148,743	40,070	5,649	194,461
$210,000 to $240,000	17	166,838	47,224	8,862	222,924
$240,000 to $270,000	15	192,156	49,849	9,621	251,625
$270,000 to $300,000	6	205,317	62,914	10,719	278,949
$300,000 to $330,000	1	239,698	53,134	12,071	304,902
$420,000 to $450,000	1	321,764	107,288	-	429,053
Total	68				

This table reports substantive senior executives who were employed by ASIO during the reporting period. Each row is an averaged figure based on headcount for individuals in that band.

Reportable salary includes gross payments as reported on employees' payment summaries (less bonuses paid, which are separated out and disclosed in the 'bonus paid' column) and reportable fringe benefits (prior to 'grossing up' to account for income tax benefits).

The contributed superannuation amount is the average actual superannuation contributions paid on behalf of senior executives in that reportable remuneration band, including any salary-sacrificed amounts, as per individuals' payslips.

Bonus paid represents average actual bonuses paid during the reporting period in that reportable remuneration band.

Various salary-sacrifice arrangements were available to senior executives including superannuation, motor vehicle and expense payment fringe benefits. Salary-sacrifice benefits are reported in the reportable salary column, excluding salary sacrificed superannuation, which is reported in the contributed superannuation column.

Note 12C: Other highly paid staff

Average annual reportable remuneration	Staff	Reportable salary	Contributed superannuation	Bonus paid	Total
	No.	$	$	$	$
2012					
Total remuneration:					
$150,000 to $180,000	**109**	**129,962**	**30,545**	**73**	**160,580**
$180,000 to $210,000	**15**	**150,519**	**38,240**	**1,442**	**190,201**
$210,000 to $240,000	**6**	**176,604**	**38,919**	**2,325**	**217,847**
Total	**130**				
2011					
Total remuneration:					
$150,000 to $180,000	76	127,060	32,069	-	159,128
$180,000 to $210,000	10	149,761	39,604	762	190,127
Total	86				

This table reports staff:

- who were employed by ASIO during the reporting period;
- whose reportable remuneration was $150,000 or more for the reporting period; and
- who were not required to be disclosed in Table B.

Each row is an averaged figure based on headcount for individuals in that band.

Reportable salary includes gross payments as reported on employees' payment summaries (less bonuses paid, which are separated out and disclosed in the 'bonus paid' column) and reportable fringe benefits (prior to 'grossing up' to account for income tax benefits).

The contributed superannuation amount is the average actual superannuation contributions paid on behalf of senior executives in that reportable remuneration band , including any salary-sacrificed amounts, as per individuals' payslips.

Bonus paid represents average actual bonuses paid during the reporting period in that reportable remuneration band.

Various salary-sacrifice arrangements were available to other highly paid staff including superannuation, motor vehicle and expense payment fringe benefits. Salary-sacrifice benefits are reported in the reportable salary column, excluding salary-sacrificed superannuation, which is reported in the contributed superannuation column.

Note 13: Financial instruments

Note 13A: Categories of financial instruments

	2012 $'000	2011 $'000
Financial assets		
Loans and receivables		
Cash	**12,775**	18,885
Trade receivables	**5,743**	3,023
Accrued revenue	**4,378**	594
Carrying amount of financial assets	**22,896**	22,502
Financial liabilities		
At amortised cost		
Trade creditors and accruals	**14,785**	9,499
Carrying amount of financial liabilities	**14,785**	9,499

Note 13B: Net income and expense from financial assets

There is no net income from financial assets through the profit and loss for the period ending 30 June 2012 (2011: Nil). The total expense from financial assets through the profit and loss for the period ending 30 June 2012 was $20,619 (2011: $4,246).

Note 13C: Net income and expense from financial liabilities

There is no net income and expense from financial liabilities through profit or loss for the period ending 30 June 2012 (2011: Nil).

Note 13D: Fair value of financial instruments

	2012 $'000 Carrying amount	2012 $'000 Fair value	2011 $'000 Carrying amount	2011 $'000 Fair value
Financial assets				
Loans and receivables				
Cash	**12,775**	**12,775**	18,885	18,885
Trade receivables (net)	**5,743**	**5,743**	3,023	3,023
Accrued revenue	**4,378**	**4,378**	594	594
Total	**22,896**	**22,896**	22,502	22,502
Financial liabilities				
At amortised cost				
Trade creditors and accruals	**14,785**	**14,785**	9,499	9,499

Note 13E: Credit risk

ASIO's maximum exposures to credit risk at the reporting date in relation to each class of recognised financial assets is the carrying amount of those assets as indicated in the Balance Sheet.

ASIO is exposed to minimal credit risk in relation to potential debtor default. ASIO provides for this risk through the recognition of an allowance for impairment where necessary.

ASIO manages its debtors by undertaking recovery processes for those receivables which are considered to be overdue. The risk of overdue debts arising is negated through the implementation of credit assessments on potential customers.

ASIO's credit risk profile has not changed from the prior financial year.

The following table illustrates ASIO's gross exposure to credit risk, excluding any collateral or credit enhancements.

	2012	2011
	$'000	$'000
Financial assets		
Loans and receivables		
Cash	**12,775**	18,885
Trade receivables	**5,743**	3,023
Accrued revenue	**4,378**	594
Total financial assets	**22,896**	22,502
Financial liabilities		
At amortised cost		
Trade creditors and accruals	**14,785**	9,499

The credit quality of financial instruments not past due or individually determined as impaired:

	2012	2011	**2012**	2011
	$'000	$'000	**$'000**	$'000
	Not past due nor impaired		Past due or impaired	
Loans and receivables				
Cash[1]	**12,775**	18,885	**-**	-
Trade receivables[2]	**2,997**	2,694	**2,746**	329
Accrued revenue[3]	**4,378**	594	**-**	-
Total loans and receivables	**20,150**	22,173	**2,746**	329

[1] Cash is subject to minimal credit risk, as cash holdings are held with the Reserve Bank of Australia.

[2] Trade and other receivables are subject to minimal credit risk, the majority of which will be recovered on a timely basis.

[3] Accrued revenue is subject to minimal credit risk as full recovery is expected.

Ageing of financial assets that are past due but not impaired

	0 to 30 days $'000	31 to 60 days $'000	61 to 90 days $'000	90+ days $'000	Total $'000
2012					
Loans and receivables					
Trade and other receivables	**589**	**63**	**1,874**	**220**	**2,746**
2011					
Loans and receivables					
Trade and other receivables	150	102	9	68	329

Note 13F: Liquidity risk

ASIO has no significant exposures to any concentrations of liquidity risk.

ASIO analyses measures of liquidity, such as the relationship between current assets and current liabilities. Such processes, together with the application of full cost recovery, ensure that at any point in time ASIO has appropriate resources available to meet its financial obligations as and when they fall due.

ASIO manages liquidity risk by ensuring all financial liabilities are paid in accordance with terms and conditions on demand. ASIO's liquidity risk profile has not changed from 2010–11.

The following table illustrates the maturities for financial liabilities.

	$'000 On demand	$'000 within 1 year	$'000 1 to 5 years	$'000 > 5 years	$'000 Total
2012					
At amortised cost					
Trade creditors and accruals	**-**	**14,785**	**-**	**-**	**14,785**
2011					
At amortised cost					
Trade creditors and accruals	-	9,499	-	-	9,499

Note 13G: Market risk

ASIO holds basic financial instruments that do not expose it to certain market risks.
ASIO's market risk profile has not changed from 2010–11. ASIO is not exposed to 'Currency risk', 'Other price risk' or 'Interest rate risk'.

Note 14: Appropriations

Note 14A: Annual appropriations

	Appropriation Act		FMA Act					
	Annual appropriation	Appropriations reduced	Section 30	Section 31 (GST excl.)	Section 32	Total appropriation	Appropriation applied	Variance
	$ '000	$ '000	$ '000	$ '000	$ '000	$ '000	$ '000	$ '000
2012								
Departmental								
Ordinary annual services	**347,352**	**-**	**12,346**	**19,856**	**-**	**379,554**	**(409,476)**	**(29,922)**
Other services								
Equity	**41,806**	**-**	**-**	**-**	**-**	**41,806**	**(90,505)**	**(48,699)**
Total Departmental	**389,158**	**-**	**12,346**	**19,856**	**-**	**421,360**	**(499,981)**	**(78,621)**
2011								
Departmental		-						
Ordinary annual services	373,447	-	2,756	12,934	(320)[1]	388,817	(369,842)	18,975
Other services								
Equity	61,186	-	-	-	-	61,186	(34,782)	26,404
Total Departmental	434,633	-	2,756	12,934	(320)	450,003	(404,624)	45,380

1. Transferred under subsection 32(2) of the *Financial Management and Accountability Act 1997* — date of effect 17 November 2010.

Note 14B: Departmental Capital Budgets

	Appropriation Act						
	Annual Capital Budget	Appropriations reduced	Total Capital Budget Apprioriations	Payments for non-financial assets	Payments for other purposes	Total payments	Variance
	$ '000	$ '000	$ '000	$ '000	$ '000	$ '000	$ '000
2012							
Departmental							
Ordinary annual services							
Departmental Capital Budget	19,228	-	19,228	(12,228)	-	(12,228)	7,000
Total Departmental	**19,228**	**-**	**19,228**	**(12,228)**	**-**	**(12,228)**	**7,000**
2011							
Departmental							
Ordinary annual services							
Departmental Capital Budget	28,244	(23,552)[1]	4,692	(4,692)	-	(4,692)	-
Total Departmental	28,244	(23,552)	4,692	(4,692)	-	(4,692)	-

1. Reduced under subsection 12(2) of *Appropriation Act (No.1) 2010–2011* — date of effect 30 June 2012.

Note 14C: Unspent departmental annual appropriations

	2012 $ '000	2011 $ '000
Appropriation Act (No.1) 2011–12	**239,002**	-
Appropriation Act (No.2) 2011–12	-	-
Appropriation Act (No.1) 2010–11	-	268,924
Appropriation Act (No.2) 2010–11	-	48,699
Total	**239,002**	317,623

Note 14D: Disclosure by agent in relation to annual appropriations

	2012		2011	
	DoFD **$ '000**	**DFAT** **$ '000**	DoFD $ '000	DFAT $ '000
Total payments	**90,505**	**13,295**	28,782	11,065

Agent payments to the Department of Finance and Deregulation relate to the construction of a new building.

Agent payments to the Department of Foreign Affairs and Trade relate to services overseas.

Note 15: Compensation and debt relief

No payments were made during the reporting period under the 'Defective Administration Scheme' (2011: Nil).

Note 16: Reporting of outcomes

	2012 $ '000	2011 $ '000
Expenses		
Departmental	**396,238**	385,947
Income from non-government sector		
Departmental		
Activities subject to cost recovery	**(3,007)**	(376)
Other	**(254)**	(491)
	(3,261)	(867)
Other own-source income		
Departmental	**(19,452)**	(7,333)
Net cost of outcome delivery	**373,525**	377,796

Net costs shown include intra-government costs that are eliminated in calculating the actual Budget Outcome.

Note 17: Restructuring

As a result of a restructuring of administrative arrangements, ASIO transferred responsibility for the following function to the Department of the Prime Minister and Cabinet (PM&C) on 8 November 2010: Cyber Policy Coordination. No assets or liabilities were transferred — only appropriation funding of $320,000. No income or expenses were incurred by ASIO prior to the transfer and none assumed by PM&C.

Note 18: Net cash appropriation arrangements

	2012 $ '000	2011 $ '000
Total comprehensive income (loss) plus depreciation and amortisation expenses previously funded through revenue appropriations	**(5,321)**	(6,162)
Less depreciation and amortisation expenses previously funded through revenue appropriation	**(40,173)**	(39,035)
Total comprehensive loss as per statement of comprehensive income	**(45,494)**	(32,873)

From 2010–11, the government introduced net cash appropriation arrangements, where revenue appropriations for depreciation and amortisation expenses ceased. Entities now receive a separate capital budget provided through equity appropriations. Capital budgets are to be appropriated in the period when cash payment for capital expenditure is required.

Part 7

Appendices and indices

Appendix A

Agency resource statement 2011–12

	Actual available appropriations for 2011–12 $'000	Payments made 2011–12 $'000	Balance remaining $'000
Departmental appropriation			
Prior year departmental appropriation	250,039	250,039	-
Departmental appropriation	328,124	110,902	217,222
S.31 Relevant agency receipts	19,856	19,856	-
S.30 Receipts	12,346	12,346	-
	610,365	**393,143**	**217,222**
Departmental non-operating			
Prior year equity injections	48,699	48,699	-
Equity injections	41,806	41,806	-
Departmental capital budget	19,228	12,228	7,000
	109,733	**102,733**	**7,000**
Total resourcing and payments	**720,099**	**495,877**	**224,222**

Appendix B

Expenses and resources table 2011–12

	Budget 2011–12 $'000	Actual expenses 2011–12 $'000	Variation 2011–12 $'000
Departmental expenses			
Ordinary annual services (Appropriation Bill No.1)	332,724	395,945	(63,221)
Expenses not requiring appropriation in the budget year	70,248	40,288	29,960
Total expenses for outcome 1	**402,972**	**436,233**	**(33,261)**

	2010–11	2011–12	Variation
Average staffing levels (number)	1,662	1,683	21

Appendix C

List of proscribed terrorist organisations (30 June 2012)

Group	Initial Listing	Date last listed
Abu Sayyaf Group (ASG)	14 Nov 2002	29 Oct 2010
Al-Qa'ida	21 Oct 2002	22 Jul 2010
Al-Qa'ida in the Arabian Peninsula (AQAP)	19 Jul 2010	
Al-Qa'ida in Iraq (AQI)	2 Mar 2005	29 Oct 2010
Al-Qa'ida in the Islamic Maghreb (AQIM)	14 Nov 2002	22 Jul 2010
Al-Shabaab	22 Aug 2009	
Ansar al-Islam	27 Mar 2003	09 Mar 2012
Hamas' Izz al-Din al-Qassam Brigades	09 Nov 2003	08 Sep 2009
Hizballah's External Security Organisation (ESO)	5 June 2003	10 May 2012
Islamic Movement of Uzbekistan (IMU)	11 Apr 2003	09 Mar 2012
Jaish-e-Mohammed (JeM)	11 April 2003	09 Mar 2012
Jamiat ul-Ansar (JuA)	14 Nov 2002	29 Oct 2010
Jemaah Islamiyah (JI)	27 Oct 2002	22 Jul 2010
Kurdistan Workers Party (PKK)	17 Dec 2005	08 Sep 2009
Lashkar-e Jhangvi (LeJ)	11 Apr 2003	09 Mar 2012
Lashkar-e-Tayyiba (LeT)	09 Nov 2003	08 Sep 2009
Palestinian Islamic Jihad (PIJ)	3 May 2004	08 Sep 2009

In March 2009 the Attorney-General announced the delisting of the Islamic Army of Aden and Asbat al-Ansar.

Appendix D

Mandatory reporting requirements for Questioning and Questioning and Detention Warrants under section 94 of the ASIO Act

Section	Description	Number
94(1a)(a)	The total number of requests made under Division 3 of Part III to issuing authorities during the year for the issue of warrants under that Division	0
94(1A)(b)	The total number of warrants issued during the year under that Division	0
94(1A)(c)	The total number of warrants issued during the year under section 34E	0
94(1A)(d)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year under section 34E and the total of all those hours for all those persons	0
94(1A)(e)	The total number of warrants issued during the year under section 34G	0
94(A)(f)(i)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued during the year under section 34G	0
94(A)(f)(ii)	The number of hours each person spent in detention under such a warrant	0
94(A)(f)(iii)	The total of all those hours for all those persons	0
94(1A)(g)	The number of times each prescribed authority had persons appear for questioning before him or her under warrants issued during the year	0

Appendix E

Workforce statistics

Table 1: Composition of workforce 2006–07 to 2011–12

	2006–07	2007–08	2008–09	2009–10	2010–11	2011–12
Ongoing full time (excl DG)	1,125	1,263	1,452	1,460	1,511	1,546
Non-ongoing full time[1]	55	52	49	40	50	37
Ongoing part time	94	108	116	134	148	168
Non-ongoing part time	18	12	19	18	16	18
Non-ongoing casual	64	57	54	39	42	43
Total	1,356	1,492	1,690	1,691	1,767	1,812

[1] Includes Secondees and locally engaged staff held against positions in the structure.

Table 2: SES equivalent classification and gender 2006–07 to 2011–12 (Does not include the Director-General)

		2006–07	2007–08	2008–09	2009–10	2010–11	2011–12
Band 1	Female	7	6	7	6	8	10
	Male	17	29	35	35	38	36
Band 2	Female	2	2	4	4	4	5
	Male	8	11	12	10	10	8
Band 3	Male	1	2	2	2	2	1
Total		35	50	60	57	62	60

Table 3: Representation of designated groups within ASIO at 30 June 2012

Group	Total Staff [1]	Women	Non-English Speaking Background	Aboriginal and Torres Strait Islander	People with a disability	Available EEO Data [2]
SES (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 1and 2	90	13	6	0	2	85
Engineers Grades 1and 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 translates to APS Level 6.

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

Table 4: Percentage of representation of designated groups in ASIO 2006–07 to 2011–12

Group	2006–07	2007–08	2008–09	2009–10	2010–11	2011–12
Women[1]	45.5	45.4	44.6	44.3	44.3	44.3
Non-English Speaking Background	5.6	4.4	5.6	6.9	6.0	5.7
Aboriginal Torres Strait Islander	0.3	0.3	0.2	0.2	0.3	0.4
People with a disability	1.2	1.4	1.4	1.2	1.2	1.2

1 Percentages for women are based on total staff. Percentages for other groups are based on staff for which EEO data was available.

Appendix F

ASIO salary classification structure at 30 June 2012

ASIO MANAGERS			
SES Band 3	$221,293		minimum point
SES Band 2	$174,910		minimum point
SES Band 1	$146,702		minimum point
AEO3	$120,516		
AEO2	$109,331	to	$120,516
AEO1	$96,405	to	$109,331

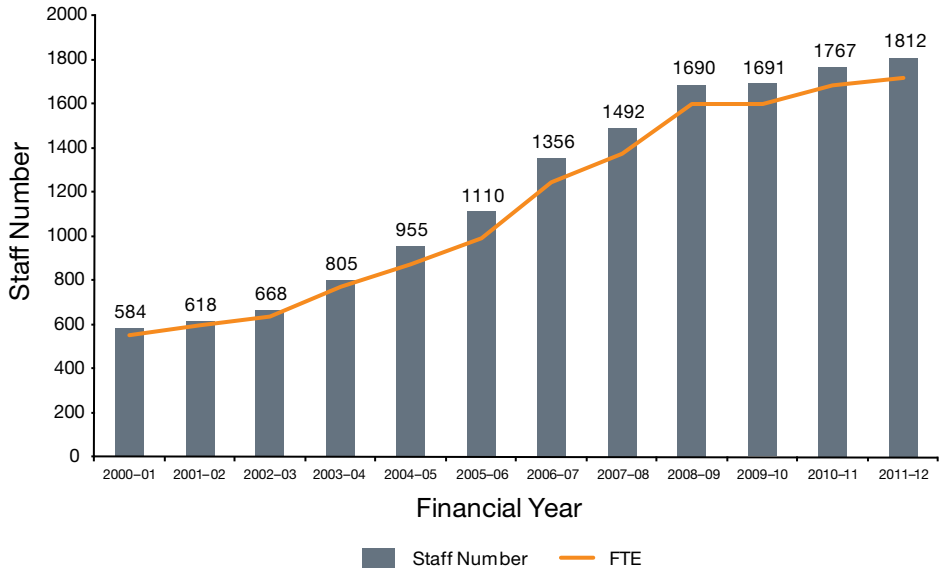
INTELLIGENCE OFFICERS			
IO	$73,613	to	$83,965

ASIO OFFICERS			
ASIO Officer 5	$73,613	to	$83,965
ASIO Officer 4	$60,712	to	$68,241
ASIO Officer 3	$52,944	to	$58,485
ASIO Officer 2	$46,623	to	$51,574
ASIO Officer 1	$41,325	to	$45,554

ASIO ITOs			
SITOA	$120,516		
SITOB	$109,331	to	$120,516
SITOC	$96,405	to	$104,061
ITO2	$73,613	to	$83,965
ITO1	$57,048	to	$66,273

ASIO ENGINEERS			
SIO(E)5	$122,430		
SIO(E)4	$109,331	to	$120,516
SIO(E)3	$96,405	to	$104,061
SIO(E)2	$73,613	to	$83,965
SIO(E)1	$57,048	to	$66,273

ASIO staff numbers 2001–12



Compliance Index

Part of Report	Description	Requirement	Page
	Letter of transmittal	Mandatory	iii
	Table of contents	Mandatory	v
	Index	Mandatory	141
	Glossary	Mandatory	139
	Contact officer(s)	Mandatory	Back cover
	Internet home page address and Internet address for report	Mandatory	Back cover
Review by Secretary			
	Review by departmental secretary	Mandatory	vii
	Summary of significant issues and developments	Suggested	vii–xi
	Overview of department's performance and financial results	Suggested	xi
	Outlook for following year	Suggested	2
	Significant issues and developments – portfolio	Portfolio departments – suggested	Not applicable
Departmental Overview			
	Role and functions	Mandatory	xiii
	Organisational structure	Mandatory	vii–xi
	Outcome and program structure	Mandatory	xi, 8
	Where outcome and program structures differ from PB Statements/PAES or other portfolio statements accompanying any other additional appropriation bills (other portfolio statements), details of variation and reasons for change	Mandatory	Not applicable
	Portfolio structure	Portfolio departments – Mandatory	Not applicable
Report on Performance			
	Review of performance during the year in relation to programs and contributions to outcomes	Mandatory	Part 2
	Actual performance in relation to deliverables and KPIs set out in PB Statements/PAES or other portfolio statements	Mandatory	Part 2

Part of Report	Description	Requirement	Page
	Where performance targets differ from the PBS/PAES, details of both former and new targets, and reasons for the change	Mandatory	Not applicable
	Narrative discussion and analysis of performance	Mandatory	Part 2
	Trend information	Mandatory	Throughout
	Significant changes in nature of principal functions/ services	Suggested	Not applicable
	Performance of purchaser/provider arrangements	If applicable, suggested	Not applicable
	Factors, events or trends influencing departmental performance	Suggested	Part 1
	Contribution of risk management in achieving objectives	Suggested	75
	Social inclusion outcomes	If applicable, mandatory	Not applicable
	Performance against service charter customer service standards, complaints data, and the department's response to complaints	If applicable, mandatory	49, 56, 66
	Discussion and analysis of the department's financial performance	Mandatory	xi, Part 6
	Discussion of any significant changes from the prior year, from budget or anticipated to have a significant impact on future operations	Mandatory	ix
	Agency resource statement and summary resource tables by outcomes	Mandatory	xi, 126
Management and Accountability Corporate Governance			
	Agency heads are required to certify that their agency comply with the Commonwealth Fraud Control Guidelines	Mandatory	iii
	Statement of the main corporate governance practices in place	Mandatory	70–72
	Names of the senior executive and their responsibilities	Suggested	–
	Senior management committees and their roles	Suggested	70–72
	Corporate and operational planning and associated performance reporting and review	Suggested	75

Part of Report	Description	Requirement	Page
	Approach adopted to identifying areas of significant financial or operational risk	Suggested	75
	Policy and practices on the establishment and maintenance of appropriate ethical standards	Suggested	54–55
	How nature and amount of remuneration for SES officers is determined	Suggested	66
External Scrutiny			
	Significant developments in external scrutiny	Mandatory	viii, 48–52
	Judicial decisions and decisions of administrative tribunals	Mandatory	22
	Reports by the Auditor-General, a Parliamentary Committee or the Commonwealth Ombudsman	Mandatory	51
Management of Human Resources			
	Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	Mandatory	58–64
	Workforce planning, staff turnover and retention	Suggested	59–60
	Impact and features of enterprise or collective agreements, individual flexibility arrangements (IFAs), determinations, common law contracts and AWAs	Suggested	60
	Training and development undertaken and its impact	Suggested	62–64
	Work health and safety performance	Suggested	65
	Productivity gains	Suggested	–
	Statistics on staffing	Mandatory	130
	Enterprise or collective agreements, IFAs, determinations, common law contracts and AWAs	Mandatory	60
	Performance pay	Mandatory	66
	Assessment of effectiveness of assets management	If applicable, mandatory	69
	Assessment of purchasing against core policies and principles	Mandatory	69

Part of Report	Description	Requirement	Page
	The annual report must include a summary statement detailing the number of new consultancy services contracts let during the year; the total actual expenditure on all new consultancy contracts let during year (inclusive of GST); the number of ongoing consultancy contracts that were active in the reporting year; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST). The annual report must include a statement noting that information on contracts and consultancies is available through the AusTender website.	Mandatory	69
	Absence of provisions in contracts allowing access by the Auditor-General	Mandatory	Not applicable
	Contracts exempt from the AusTender	Mandatory	69
	Financial Statements	Mandatory	Part 6
Other Mandatory Information			
	Work health and safety (Schedule 2, Part 4 of the *Work Health and Safety Act 2011*)	Mandatory	65
	Advertising and Market Research (Section 311A of the *Commonwealth Electoral Act 1918*) and statement on advertising campaigns	Mandatory	61
	Ecologically sustainable development and environmental performance (Section 516A of the *Environment Protection and Biodiversity Conservation Act 1999*)	Mandatory	xi, 68
	Compliance with the agency's obligations under the *Carer Recognition Act 2010*	If applicable, mandatory	Not applicable
	Grant programs	Mandatory	Not applicable
	Disability reporting – explicit and transparent reference to agency-level information available through other reporting mechanisms	Mandatory	131
	Information Publication Scheme statement	Mandatory	Not applicable
	Correction of material errors in previous annual report	If applicable, mandatory	79
	List of Requirements	Mandatory	Appendix

Glossary

AAR	ASIO Analytical Report
AASB	Australian Accounting Standards Board
AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
AIC	Australian intelligence community
AIR	ASIO Intelligence Report
ANAO	Australian National Audit Office
ANU	Australian National University
APEC	Asia Pacific Economic Cooperation
AQEA	al-Qa'ida in East Africa
AQAP	al-Qa'ida in the Arabian Peninsula
ARC	Audit and Risk Committee
ASC	ASIO Security Committee
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ATA	ASIO Threat Assessment
AWP	Audit Work Program
BLU	Business Liaison Unit
CBRN	chemical, biological, radiological, nuclear (weaponry)
CHOGM	Commonwealth Heads of Government Meeting
COAG	Council of Australian Governments
CPI	consumer price index
CREST	Council of Registered Ethical Security Testers
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CSOC	Cyber Security Operations Centre
CSS	Commonwealth Superannuation Scheme
CTCC	Counter Terrorism Control Centre
CTRC	Commonwealth Technical Response Capability
DCB	departmental capital budgets
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation

DSD	Defence Signals Directorate
DFAT	Department of Foreign Affairs and Trade
EEO	equal employment opportunity
EMS	Environmental Management System
FC	Finance Committee
FMO	Finance Minister's Orders
GST	goods and services tax
ICC	Intelligence Coordination 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
IRIC	Independent Review of the Intelligence Community
ISA	*Intelligence Services Act 2001*
ISAF	International Security Assistance Force
NAA	National Archives of Australia
NBC	New Building Committee
NCTC	National Counter-Terrorism Committee
NiTAC	National Interception Technical Assistance Centre
NSC	National Security Committee of Cabinet
NTAC	National Threat Assessment Centre
ONA	Office of National Assessments
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PM&C	Department of the Prime Minister and Cabinet
PSPF	Protective Security Policy Framework
PSS	Public Sector Superannuation Scheme
PSSap	Public Sector Superannuation Scheme Accumulation Plan
PSSR	Protective Security Risk Review
RMR	Research and Monitoring Report
SCEC	Security Construction and Equipment Committee
SCNS	Secretaries' Committee on National Security

SEC	Security Equipment Catalogue
SEEPL	Security Equipment Evaluated Product List
SEM	Senior Executive Meeting
SES	Senior Executive Service
SSAN	security sensitive ammonium nitrates
TSCM	technical surveillance counter-measures
WCC	Workforce Capability Committee
WHSC	Work Health and Safety Committee
WMD	weapons of mass destruction

Index

Symbols

A

B

C

D

E

F

G

H

I

Q

R

S

T

U

V

W

Y

Contact and Internet details

Written inquiries

The Director-General of Security
ASIO Central Office
GPO Box 2176
CANBERRA ACT 2601

General inquiries

Central Office switchboard
Tel: (02) 6249 6299
1800 020 648 (toll free)
Fax: (02) 6257 4501

Media inquiries

Media Liaison Officer
Tel: (02) 6249 8381
Fax: (02) 6262 9547

Website

www.asio.gov.au

State and territory offices

Australian Capital Territory	(02) 6249 6299
Victoria	(03) 9654 8985
New South Wales	(02) 9281 0016
Queensland	(07) 3831 5980
South Australia	(08) 8223 2727
Western Australia	(08) 9221 5066
Tasmanian residents	1800 020 648
Northern Territory	(08) 8981 2374

Supplementary Information

The ASIO Strategic Plan 2011–13 provides further information on the activities and management of ASIO.