



2010-11

ASIO Report to Parliament

ISSN 0815-4562

© Commonwealth of Australia [2011]

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, 3–5 National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>.



Australian Government

**Australian Security
Intelligence Organisation**

Director-General of Security

11 October 2011

eA1213405

The Hon Robert McClelland 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 2011.

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 sincerely

David Irvine

David Irvine

ASIO

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 Review	vii
Guide to the Report	xi
ASIO's Role and Functions	xii
Organisational Structure	xiii
ASIO's Funding, Outcome and Program Structure	xvii
Executive Summary	xviii
Part 1: Threats and the Security Environment 2010–11	1
The Security Environment 2010–11 and Outlook	3
Part 2: Program Performance 2010–11	11
Security Intelligence Analysis and Advice	13
Security Intelligence Investigations and Capabilities	37
Foreign Intelligence Collection	52
Part 3: Outcomes & Highlights	53
Part 4: Accountability	57
ASIO and Accountability	59
Part 5: Corporate Management	79
People	81
Corporate Capabilities	94
Corporate Strategy and Governance	94
Legislation	102
Information Services	103
Property	106
Financial Services	109
Corrections to ASIO Annual Report 2009–10	110
Part 6: Financial Statements	111
Statement by the Director-General of Security	113
Part 7: Appendices & Indices	153
Appendix A: Agency Resource Statement 2010–11	155
Appendix B: Expenses and Resources Table 2010–11	156
Appendix C: List of Proscribed Terrorist Organisations (30 June 2011)	157
Appendix D: Mandatory Reporting Requirements under section 94 of the ASIO Act	158
Appendix E: Workforce Statistics	159
Compliance Index	164
Glossary	169
Index	171

Director-General's Review

A security intelligence organisation in a democratic society plays a key role in protecting that society and its citizens from covert threats both external and internal. Its primary purpose is investigative and predictive; to foresee and to prevent those threats from being realised, before its citizens are harmed or killed or its national security weakened.

In this sense, it is appropriate to consider ASIO as representing a protective capability, operating quietly in the background of national affairs. Similar to Australia's Defence Force, this security intelligence capability must be maintained and adapted to meet a rapidly changing threat and operating environment. It therefore needs to be flexible and up to date, able to address new threats and new situations with new methods and new technology.

At the same time, the national security intelligence capability must be able to operate strictly within the laws and acceptable parameters established by the very same democratic society it has been set up to protect.

Conscious of these conceptual legal requirements, ASIO in 2010–11 has focused on enhancing the national security intelligence capability in four key areas:

- enhanced and more flexible operational effectiveness across the Organisation;
- a rapid re-focusing of operational effort to address several significant new threat-related challenges;
- an internal strategic reform program to increase operating efficiency in the face of a tight budgetary environment; and
- enhanced cooperation with national and international intelligence partners.

Three stand-out examples from the reporting period highlight this focus. ASIO's Strategic Plan 2011–13 was released in December 2010. This plan identifies ASIO's four key strategic goals over the next three years: strengthen intelligence collection and analysis capability; enhance strategic impact; build and manage the workforce of the future; and improve business processes and practices. It provides an important strategic underpinning to ASIO's operational focus and current program of reform.

In January 2011, ASIO developed a security referral framework for irregular maritime arrivals (IMAs), which, when operational in March 2011, streamlined the security checking process for IMAs and allowed the Organisation to

focus on complex cases while finalising non-complex cases relatively quickly. The framework — which reflects an intelligence-led, risk-managed approach to security assessments — greatly improved ASIO's ability to assess IMAs for their relevance to security at roughly the same pace as they arrived at Christmas Island. Indeed, as at the time of writing, only nine per cent of IMAs currently in detention were awaiting security assessments by ASIO.

In July 2010, ASIO established the Cyber Espionage Branch to provide advice to government and business on the threat of cyber-espionage — one of the most concerning and damaging threats within the current security environment — as well as to investigate increasingly sophisticated and frequent cyber-intrusions into computer networks. This branch is now an important element of wider whole-of-government efforts to manage the cyber threat, and its value has been commented upon favourably by government and international partners.

In an increasingly interconnected world where transnational issues require transnational responses, the assistance of international security intelligence partners is vital to achieve outcomes. Australian security often benefits from the success of partner agencies overseas. The death of Usama bin Laden, the capture and arrest of Jemaah Islamiyah member Umar Patek and the sentencing and conviction of Abu Bakar Ba'asyir were all welcome developments in our collective efforts to counter terrorism.

Importantly, ASIO must continue to take opportunities to work more closely with Australian partner agencies, leveraging off their respective expertise, in pursuit of its security intelligence objectives.

Domestically, efforts to improve counter-terrorism coordination were enhanced by the work of the newly created Counter Terrorism Control Centre (CTCC). In its first year of operation, the CTCC filled a capability gap. The intelligence function, for example, is now prioritised and monitored more effectively, enabling the intelligence collectors to be tasked more precisely and the intelligence to be produced and acted upon in a more timely and accountable manner by the appropriate agencies.

ASIO's ability to do its job more collaboratively with intelligence community and law enforcement partners was also strengthened over the reporting period through amendments to the *Australian Security Intelligence Organisation Act 1979* by the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011*. As a result, ASIO is now able to assist its intelligence community and law enforcement partners in the performance of their respective functions, as well as to communicate a broader range of information and intelligence to these partners and other state and Commonwealth authorities.

It should be emphasised that recent, and future proposed, changes to ASIO's legislation do not and will not reduce oversight of ASIO or its accountability framework. In this respect, ASIO welcomed the appointment of Mr Bret Walker SC as the inaugural Independent National Security Legislation Monitor. In this capacity, Mr Walker will be responsible for providing advice to Government on the effectiveness of Australia's counter-terrorism legislation and also on whether the legislation contains appropriate safeguards to protect the rights of individuals.

As we reflect upon the tenth anniversary of the 11 September 2001 attacks in the United States, there is the danger of complacency in regard to the terrorist threat. Surveys conducted in Australia and the United States show terrorism is no longer seen as a significant issue by the majority of the population. This comes on top of ongoing complaints about the inconvenience and cost of counter-terrorism measures, and academic studies claiming the treatments put in place to manage terrorism are disproportionate to the threat — that governments are over-responding.

Despite counter-terrorism successes, including the death of Usama bin Laden and the thwarting of many planned terrorist attacks in Western countries over the past decade, the threat of a terrorist attack in Australia or against Australian interests in a number of countries overseas is real and will remain so into the future. ASIO's operational tempo in 2010–11 did not abate. ASIO continued to investigate Australians involved in or associated with activities of significant counter-terrorism interest both at home and abroad.

Turning to personnel, although ASIO was unable to meet its recruitment targets in the previous financial year, recruitment numbers over this reporting period place the Organisation in a good position to meet the number of 1,860 full-time staff — as recommended in the Review of ASIO Resourcing, conducted in 2005 by the late Mr Allan Taylor AM — by the 2012–13 budget cycle. Recruitment strategies and initiatives to attract new staff will remain a priority for ASIO. It is only because of ASIO's people that the Organisation can meet the considerable expectations rightfully placed on it by Government and the Australian community.

Looking ahead, ASIO will not be able to rely on current levels of funding to sustain its ongoing activities. Indeed, whilst the Organisation will receive funding towards the running costs of its new central office, it will provide net savings to Government over the next four years of \$69.2 million in addition to absorbing the costs of new tasks and capabilities. As a result, the Organisation's internal efficiency and modernisation program will be especially important in finding ways to absorb any financial cutbacks without having to reduce operational capability or coverage.

Events over the forthcoming year will pose many of the same challenges for ASIO as in the current reporting period. More than ever, and because of the significant advances and achievements made by the Organisation over the last twelve months, I am confident of ASIO's ability to meet these challenges and continue to provide the intelligence edge for a secure and safe Australia.

Guide to the Report

ASIO produces a classified and an unclassified annual report. Section 94 of the *Australian Security Intelligence Organisation Act 1979* requires the Director-General of Security, as soon as practicable after 30 June, to furnish to the Minister a report on the activities of ASIO. The Minister is required to table an unclassified version of this report in Parliament within 20 sitting days of receipt.

For reasons of national security, Part 3 of the *ASIO Annual Report* has been redacted in its entirety to produce the unclassified *Report to Parliament*. ASIO is the only Australian intelligence agency to produce an unclassified annual report.

ASIO's Role and Functions

'Successive Australian Governments have seen the role of ASIO, enshrined in the precise language of the ASIO Act, as being to protect against threats to our national life and the safety of the citizens of the sovereign nation of Australia.'

Director-General of Security's address to the University of Canberra Lecture Series on National Security
27 August 2010

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

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

ASIO's responsibility for security intelligence extends beyond Australia's borders and includes Australia's 'security' obligations to other countries. The ASIO Act also authorises ASIO to communicate and cooperate with relevant authorities of foreign countries.

In fulfilling its obligations to protect Australia, its people and its interests, ASIO:

- collects security intelligence through a wide range of means including human sources and technical operations, using the least intrusive means possible in accordance with the Attorney-General's Guidelines;
- assesses security intelligence and provides advice to Government on security matters;
- investigates and responds to threats to security;
- maintains a national counter-terrorism intelligence capability;
- provides protective security advice; and

- provides security assessments, including for visa entry checks and access to classified material and designated security-controlled areas.

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

ASIO works closely with state and federal law enforcement agencies, the AIC, foreign partners, other government departments and agencies and industry.

Organisational Structure

In order to meet its strategic goals, in 2009–10 ASIO developed a new structure to enable it to operate effectively within the changing security environment. On 1 July 2010, ASIO moved to a ten-division structure that aligned key elements of ASIO's functionality with its strategic framework. The new structure ensures resources are allocated efficiently and better aligns staff skills and work unit functions, contributing to an overall enhancement of ASIO's performance.

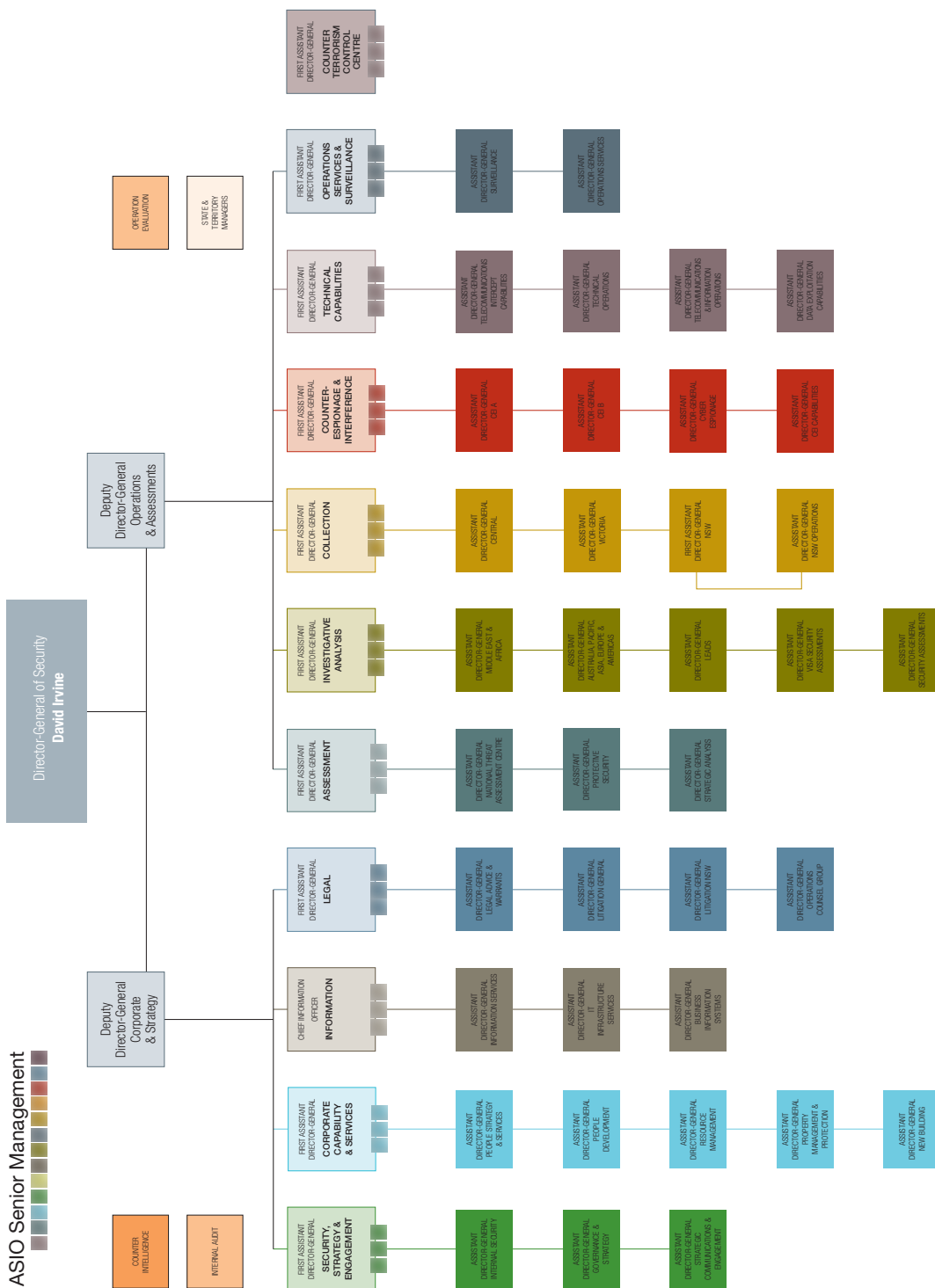


Figure 1. ASIO's organisational structure at 30 June 2011

An Outline of ASIO's Ten Divisions

Security, Strategy and Engagement Division provides high-level support to the offices of the Director-General and Deputy Directors-General; manages internal security policy and practices to ensure security is factored into the Organisation's decision making and culture; drives and implements the Organisation's corporate strategic agenda; coordinates corporate governance and high-level communication; delivers performance and corporate reporting; coordinates and enhances engagement with key government partners; and manages contact with the media.

Corporate Capability and Services Division is responsible for the finance, property, people, and learning and development activities within ASIO. Its remit covers matters such as recruitment; pay and conditions both in Australia and for ASIO's overseas posts; occupational health and safety; human resource policies, procedures and practices; the development, facilitation and evaluation of intelligence-related and corporate training; ASIO's accounting and budgeting responsibilities; and the maintenance of ASIO's buildings and property, including the New Building project.

Information Division is responsible for the delivery of classified and unclassified information systems across ASIO's international network in support of ASIO's collection, analysis, assessment and corporate functions. The division is the custodian of ASIO's corporate knowledge, including its archives.

Legal Division provides legal advice on operational, protective security, corporate and warrant-related matters. It also manages ASIO's involvement in litigation and provides legal and documentary support for the warrant process. Legal Division also assists in the identification of legal policy issues and legal reform issues affecting ASIO's ability to perform its functions.

Assessment Division is responsible for the alerting, analysis, production and dissemination of strategic, thematic and threat assessments and protective security advice in relation to threats to the security of Australians and Australian interests. It provides analytical and research capability for ASIO and the broader national security community and a focal point for assessment advice and engagement with government, international and private sector agencies. The division is also responsible for ASIO's international engagement and special events coordination.

Investigative Analysis Division manages, in partnership with the other divisions, ASIO's counter-terrorism and other politically motivated violence investigations. It provides analysis and synthesis of material from all sources in support of ASIO investigations and external agency and liaison requests. The division also has responsibility for ASIO's security assessment function.

Collection Division is responsible for the collection of information, primarily relating to counter-terrorism and other politically motivated violence. The division fulfils this role through human source intelligence collection; planning and conducting intelligence operations and investigations, including through the use of special powers; interviews with members of the public, including through community interview programs; engagement with state and federal law enforcement agencies; and partnerships with Australian Intelligence Community and foreign security and intelligence services.

Counter-Espionage and Interference Division investigates, analyses and provides advice to Government on espionage and foreign interference. The division conducts operations and investigations into efforts by foreign intelligence services to collect intelligence about the activities, capabilities and intentions of Australian government and strategic commercial interests. It investigates and reports on foreign interference against Australian interests. The division is also responsible for the collection of foreign intelligence in Australia, in collaboration with the Defence Signals Directorate and the Australian Secret Intelligence Service.

Technical Capabilities Division develops, delivers and maintains ASIO's technical collection and complex analysis capabilities. The division provides complex analytical services for all of ASIO to better inform existing intelligence and help discover new intelligence.

Operations Services and Surveillance Division provides national tactical intelligence collection capabilities to support operations conducted by all of ASIO's operational areas. It is responsible for operational cover, field inquiries, operational liaison and the planning of complex technical operations. It also delivers language services and physical surveillance capabilities.

ASIO's Funding, Outcome and Program Structure

In 2010–11, ASIO's total program expenses were \$385 million, a five per cent increase from a total of \$368 million in 2009–10. The estimated total cost for program expenses for 2011–12 is \$403 million. Government provided funding of \$345 million for cash expenditure only (following the introduction of Net Cash Funding) and an additional \$8 million was received from independent sources.

ASIO's program expenditure is allocated to the outcome 'security intelligence for Australia and its interests — locally and internationally — through intelligence collection and advice that counters politically motivated violence, espionage, foreign interference, communal violence, sabotage, and attacks on the defence system'. ASIO delivers and reports to the Australian Government against four program components of the outcome:

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

In 2010–11, ASIO received two equity injections: \$41 million towards the ASIO new building project and \$5 million for the ongoing replacement of assets. Two similar equity injections will be received in 2011–12: \$42 million towards the new ASIO building and \$19 million for asset replacement.

ASIO is in a consolidation phase following a period of budget growth since 2001 and will continue working on a number of strategic initiatives focused on the effective use of resources in support of the Government's fiscal strategy. Between 2009–10 and 2015–16, ASIO will provide \$193.7 million in funding offsets, additional savings and funding contributions to broader national security initiatives over and above the efficiency dividends required of agencies. As an annualised average, this funding represents around twelve per cent of ASIO's future annual revenue to 2015–16.

ASIO's Agency Resource Statement is at Appendix A. ASIO's Expenses and Resources Table is at Appendix B.

Executive Summary

The Security Environment

The fundamentals of the Australian security environment in 2010–11 remained largely unchanged from the previous period. This is despite some significant counter-terrorism successes and an increase in our understanding of the use of cyber-technologies by various sources of security threat. Espionage, foreign interference and terrorism present first-order threats to life, to the preservation of our freedoms, to political sovereignty and to economic prosperity.

Australia is, and will remain, a terrorist target for the foreseeable future. Jihadist terrorism remains the most immediate security threat. In addition to the threat posed by established groups such as al-Qa'ida and its affiliates, stand-alone jihadists or small groups — often with tenuous or no links to established groups — continue to emerge with increasing frequency.

Espionage is an enduring security threat to Australia. Espionage by cyber means — one aspect of the larger threat — is emerging as a serious and widespread concern that will continue to gain prominence given Australia's increasing reliance on technology in commercial, government and military business.

The security challenges for Australia represented by espionage, terrorism and foreign interference will not diminish in the near term. Partnerships, both across Australia's national security community and with like-minded international intelligence organisations, will remain critical to ensuring Australia remains equipped to deal with these challenges.

ASIO's Activities and Outcomes 2010–11

In 2010–11, ASIO's security intelligence analysis, assessment and advice provided insight to policymakers and partner agencies working at federal, state and international levels and provided context for intelligence officers on a range of strategic issues to support and inform their investigative activities. Key outcomes from the reporting period included:

- the production of 2,967 intelligence reports;
 - 575 threat-related products, including reports on the implications of the 'Arab spring' for the security of Australians in the Middle East, the G20 Summit in Korea, and the Commonwealth Games in New Delhi;
 - analytical reporting on the security implications for Australia of the death of Usama Bin Laden;

- the provision of intelligence-derived reporting to corporate security managers, enabling them to brief staff for their risk management and continuity planning;
- contribution to the whole-of-government cyber-security policy and coordination arrangements;
- the development of a security referral framework for irregular maritime arrivals (IMAs), which enabled ASIO to focus on complex IMA cases requiring intelligence investigation and to streamline the security process for non-complex cases; and
- ASIO's intelligence reporting distribution to 347 partners, both domestic and foreign.

In the reporting period, ASIO's protective security advice to both Government and the private sector assisted with the protection of classified information, premises and other assets. This included the provision of security advice for the Commonwealth Heads of Government Meeting to be held in late October 2011 in Perth and protective security and risk management training.

ASIO's investigative and operational activity in 2010–11 was directed at activities both within and outside Australia, including threats to Australian interests overseas and Australians engaged outside Australia in activities relevant to security. ASIO's counter-terrorism investigations and inquiries during the reporting period identified Australians seeking to travel overseas to engage in terrorism-related activities. Investigations into cyber-espionage were also a priority for ASIO. ASIO's Cyber Espionage Branch provided advice on foreign state-sponsored cyber-intrusions against Australia's interests.

In 2010–11, ASIO's contribution to whole-of-government efforts in the area of border integrity was focused sharply on onshore elements of international maritime people-smuggling networks and syndicates that facilitate IMAs' passage to Australia aboard suspected irregular entry vessels. ASIO investigations revealed several groups and individuals of security concern targeting Australia for irregular migration.

Throughout the reporting period, ASIO's international engagement and technical, surveillance and language capabilities supported both ASIO's work and that of ASIO's domestic and international partners. Key outcomes included:

- closer cooperation with key domestic and international partners to strengthen resource sharing and benchmarking of foreign language capabilities;
- contribution of ASIO's technical expertise to support whole-of-government telecommunications interception-related policy development;

- provision of support to national telecommunications interception agencies to develop and maintain their capabilities, through the National Interception Technical Assistance Centre pilot program; and
- development of a new analytical technique — using a novel application of data fusion and numeric quantitative techniques — to assist in identifying and assessing the possible implications of changes overseas for trends in violent extremism in Australia.

In 2010–11, ASIO pursued a multifaceted strategy of outreach and engagement to build mutual trust and confidence with partners and the public, to draw on external expertise and knowledge and to make as much information available as possible about ASIO and its work. Over the past twelve months, key activities and outcomes in this area included:

- the introduction of a new model for seeking feedback from partners on their satisfaction with ASIO’s engagement and performance which removes any potential for real or perceived bias of commentary;
- an increased focus on partnership forums for senior officers — participation was extended to representatives of state and territory police forces and the offices of premiers and chief ministers;
- adoption of a more coordinated and strategic approach to engagement with Australian educational and research institutions and think-tanks; and
- the official launch of the Counter Terrorism Control Centre on 21 October 2010.

In 2010–11, ASIO continued its program of organisational change and business modernisation to manage effectively the significant growth of the Organisation and respond to the rapidly changing threat and operating environment. ASIO also made significant progress towards building a highly competent, adaptable workforce, welcoming 96 new staff to the Organisation. Key corporate outcomes for the reporting period included:

- the launch of ASIO’s Strategic Plan 2011–13, which will ensure ASIO is better prepared to meet Australia’s security intelligence challenges now and into the future;
- the implementation of a roadmap of key initiatives to ensure a concentrated focus on progressing projects and proposals to attain strategic goals;
- the launch of a new anti-bullying and anti-harassment campaign; and
- the continued construction of ASIO’s new central office, which reached its peak period of construction during 2010–11 with over 500 contractors employed on site.



Part 1

Threats and the Security Environment 2010–11

The Security Environment 2010–11 and Outlook

'The security environment is more complex and challenging ... where terrorism threats are equally as likely to originate from home as they are from overseas.'

Director-General of Security's address to the Centre for Excellence in Policing and Security Conference
8 October 2010

ASIO's security intelligence responsibilities do not extend to all of the things that might harm Australia's national security interests.¹ They relate to certain deliberate activities that might be undertaken by foreign state or non-state entities and individuals, wherever those activities might occur. The activities in question are espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference or threats to Australia's territorial or border integrity. Thus our annual report on the security environment reflects the limitations of ASIO's remit and deals only with the activities for which ASIO has responsibility and the factors that drive or influence them.

That said, the environment ASIO deals with is wide-ranging. It comprises the activities that might harm our nation, its people and our interests; the people who undertake or facilitate those activities; the drivers and influences that motivate and shape them; the arrangements in place to prevent or respond to those activities; and the elements and aspects of our nation that we seek to protect. Australia's security environment is not limited geographically — the activities and people of concern are found in many places around the world. Consequently, ASIO's remit in respect of those activities is not limited by geography; ASIO is responsible for providing security intelligence and advice on them whether they are directed from, or committed in, Australia or not. So the security environment that will be described in this report is global. Indeed, it has always been the case that threats to Australia's national security have primarily had their origins overseas.

Australia's security environment is significantly influenced by major currents of global change. Some of these are new, some have their origins in the recent past, and others are continuations of trends that have been with us for some time. The use of pervasive modern technology by both foreign states and non-state actors, the communications revolution, the pervasive influence of the internet, cultural change, demographic developments, and the blurring of borders have all increased the complexity or difficulty of our intelligence work. Meanwhile, foreign conflicts — both longstanding and new — continue to act as drivers and motivation for extremism.

¹ The Australian Government's National Security Statement identifies a set of clear and enduring national security interests. These include maintaining Australia's territorial and border integrity; promoting Australia's political sovereignty; preserving Australia's cohesive and resilient society and the long-term strengths of our economy; protecting Australians and Australian interests both at home and abroad; and promoting an international environment, particularly in the Asia-Pacific region, that is stable, peaceful and prosperous, together with a global rules-based order which enhances Australia's national interests.

The conflict in Afghanistan, for example, continues to energise and fuel feelings of resentment toward the West, which risk finding manifestation in acts of terrorism. The longstanding conflict between the Palestinians and Israel also continues to provide a source of extremism which can be reflected outside the Middle East in Western countries.

More recently, the events of the 'Arab spring', which have seen a shift of political power and the growth of aspiration in some parts of the Levant, Africa and the Gulf, augur uncertainty and instability for the Middle East.

Similarly, the rapid increase in the world's reliance on information technology and the telecommunications sector has created a persuasive new vector through which state and non-state actors may conduct espionage or disruptive actions to damage national security.

These changes give rise to new security challenges in addition to the challenges that have been with us in the past.



Australia's Security Environment

Over the reporting period, the fundamentals of the Australian security environment remained largely unchanged from the previous period. Espionage, foreign interference and terrorism remained the first-order threats, and the sources and nature of the threats were fairly constant. This is despite some significant counter-terrorism successes and an increase in our understanding of the use of cyber-technologies by various sources of security threat. Espionage, foreign interference and terrorism present first-order

threats to life, to the preservation of our freedoms, to political sovereignty and to economic prosperity. Other activities currently pose a lower order threat, but nevertheless responding to them draws on ASIO's resources.

Jihadist terrorism remains the most immediate threat. Australia is a terrorist target. We have seen Australians and Australian interests deliberately targeted overseas and, in the past ten years, four mass casualty attacks within Australia have been disrupted only because of the work of intelligence and law enforcement agencies. The people involved have been inspired by an ideology imported from overseas — from the Middle-East and South Asia — but largely they are Australians. Three of these planned attacks would have been the work of groups with little or no contact with al-Qa'ida or its overseas affiliates. Of the nearly 40 individuals prosecuted for terrorism-related offences in Australia, 37 were Australian citizens and 34 were either born here or lived here since childhood.

**JIHADIST
TERRORISM
REMAINS
THE MOST
IMMEDIATE
THREAT.
AUSTRALIA IS
A TERRORIST
TARGET**

The terrorist threat to Australian interests overseas also comes from those who seek to undertake violent jihad. Al-Qa'ida and its affiliates, including al-Qa'ida in the Arabian Peninsula (AQAP), are one element of this, but other jihadist groups in South-East Asia, South Asia and the Middle East, such as Pakistan-based groups Lashkar-e-Tayyiba and Tehrik-e-Taliban, also are of concern. Similarly, Indonesian extremist groups are an ongoing concern.



AAP Images

(From left to right) Abu Bakar Ba'asyir, Usama bin Laden, Umar Patek.

Over the past twelve months, we have seen some significant counter-terrorism successes, including the death of Usama bin Laden, a leading advocate of global violent jihad and the central figure around which al-Qa'ida was organised; the arrest of Umar Patek, a Jemaah Islamiyah member and one of the alleged masterminds of the 2002 Bali bombings; and the arrest and conviction of the Emir of Jamaah Ansharut Tauhid, Abu Bakar Ba'asyir. However, terrorist groups have demonstrated a capacity over the past decade to overcome setbacks, including the loss of their leaders.

In addition to the threat posed by established groups, stand-alone jihadists or small groups — often with tenuous or no links to established groups — are emerging with increasing frequency. Propagandists such as AQAP senior figure Anwar al-Aulaqi are specifically targeting an English-speaking audience and encouraging would-be jihadists in the West and elsewhere to take action using whatever means are at their disposal without seeking any further sanction. The target audience for this message is young and English-speaking, primarily in the West but also elsewhere English is understood (including in parts of South-East Asia, South Asia, the Middle East and Africa). The distribution of these propaganda messages via the internet and through means such as AQAP's online English-language magazine *Inspire* is of particular concern because it amplifies both the reach of those seeking to radicalise new jihadis globally and the immediacy of their message.

Some Australians continue to be drawn to the jihadist message. New extremist groups and individuals continue to emerge, and some seek to act in Australia or travel overseas to train or fight. The favoured destinations for those wishing to travel overseas include Yemen, Somalia and Afghanistan/Pakistan, although the opening of any new jihadist front could attract would-be combatants.

While jihadist terrorism remains the most immediate security threat, ASIO remains attuned to the terrorist threat posed both in Australia and abroad by other ideologies and motivations.² Many of the conditions that are conducive to the promotion of communal violence are present in Australia, including tensions arising from conflicts overseas and a small number who actively promote hate between segments of society. However, Australia has to date not been marred by such violence. The complexity of factors that drive terrorism — individual psychology, identity, socioeconomic circumstance, reaction to events and government policy, ideology and group dynamics — are also at play in respect of communal violence, but the threshold for action is likely to be lower and the violence more spontaneous.

Tensions arising from overseas conflicts — for example, events in Israel and the Palestinian territories — have given rise to some political protests but these have not been reflected in communal violence. Anti-Muslim rhetoric adopted by some nationalist or racist extremists and others clearly has some resonance, but there has been no translation of this into any systemic activity. Nevertheless, significant incidents such as a major terrorist attack in Australia attributed to jihadists might quickly and unexpectedly unlock the potential for violence latent in the underlying tensions. Communal violence can also be a displacement response to tensions and incidents not obviously or directly connected to the target of that violence.

² The attacks in Norway in July 2011 serve as a reminder that politically motivated violence is a broad and constantly evolving phenomenon.

There has been a persistent but small sub-culture of racist and nationalist extremists in Australia, forming groups, fragmenting, re-forming and often fighting amongst themselves. Over the past year, such extremists have been active in protesting against various Muslim interests. Local racist and nationalist extremists maintain links and draw inspiration from like-minded overseas extremists, and much of their rhetoric and activity is derivative, heavily influenced by developments overseas. At present, their main focus is propaganda and engendering support. However, there is always the possibility of a lone actor or autonomous group inspired by a nationalist or racist extremist ideology engaging in violence as a means of provoking a wider response. A recent development is the emergence of an 'anti-fascist' movement, led by self-styled anarchists, which aims to confront those it identifies as fascists, including some of the nationalist and racist extremist groups also of interest to ASIO. Where such confrontations have occurred, the 'anti-fascists' have outnumbered the nationalist and racist extremists and police intervention has been required.

**THERE HAS BEEN
A PERSISTENT
BUT SMALL
SUB-CULTURE
OF RACIST AND
NATIONALIST
EXTREMISTS IN
AUSTRALIA**

Australian issue-motivated groups in general use legitimate protest to publicise and further the cause they advocate. The *Australian Security Intelligence Organisation Act 1979* states that lawful advocacy, protest or dissent shall not be regarded as prejudicial to security, and ASIO's interest in protest is limited to that which is unlawful or violent. Unfortunately, while most issue-motivated groups act lawfully, there are some who do not. There is also a small minority who seek to use protests around a range of emotive issues to further their own (often unrelated) political agenda by provoking, inciting or engaging in violence. It is this fringe that is of concern to ASIO.

ASIO has seen violent and provocative tactics used deliberately by this fringe at a range of protests in recent years, although the frequency and intensity of such violence tends to wax and wane. Provocative tactics used include attacks on police managing protests using 'invisible' weapons such as fishing hooks flicked into faces or squirting dangerous or unpleasant liquids in order to provoke an apparently disproportionate police response. The aim is to gain public support and to escalate the anger of those protesting in order to cause widespread violence in an attempt to de-legitimise the government position and undermine the rule of law. Other unlawful tactics used include property damage and sabotage.

Espionage is an enduring security threat to Australia. It has been a constant feature of the security environment in the past, is occurring now and will continue as long as there are states willing to maintain an intelligence

capability and use it against us. Espionage is a less immediately obvious but potentially more insidious threat than terrorism. The harm from espionage is not necessarily immediate and its seriousness can be amplified by future developments. Activities that appear to have moderate consequences now can have extreme consequences in the future. The full harm caused by effective espionage may not be known for some time after it has occurred, if at all, and in some circumstances the consequences can be grave.

The traditional methods of espionage — suborning Australians and others to obtain information or provide support for foreign intelligence agencies and using technology to access communications or conversations — continue to be the backbone of the threat. But they have been joined by additional capabilities exploiting new technologies and by the new vulnerabilities that they bring with them.

Espionage through cyber means is one aspect of the larger threat. It has emerged as a serious and widespread concern that will continue to gain prominence with the increasing reliance on digital technology by the commercial, government and military sectors. ASIO is seeing increasingly both foreign state and non-state actors taking advantage of the access, relative anonymity and global reach of the internet. From the comfort of wherever their computer terminal may be, they probe Australian information systems and data holdings for vulnerabilities and mine for valuable commercial, diplomatic and military intelligence — sometimes with success.

Despite the rise of espionage through cyber means, ASIO has not seen any reduction in the intensity of other, more traditional forms of espionage — human spies are still being recruited and run and foreign intelligence agencies are still interfering covertly in the Australian community. Indeed, effective coordination between traditional, human-based espionage and computer network operations represents a potent threat to our most sensitive data and networks that are not connected to the internet.

Not all clandestine or deceptive activity by foreign agencies is for espionage. Foreign powers also seek to use clandestine, deceptive or otherwise unlawful means to build capabilities to use against Australia in times of conflict or to use against third countries or non-state targets. They also undertake activities to interfere in the lives of individuals and groups in Australia, including some who came here as refugees.

Outlook

The security challenges for Australia from espionage, terrorism and foreign interference will not diminish in the near term. The drivers and influences on foreign powers to engage in espionage and foreign interference are enduring. Foreign powers will continue to engage in these activities to seek to achieve their policy goals and extend their national influence and capabilities at Australia's expense. The terrorism challenge is driven by ideas and radicalisation processes which will continue to be attractive to some. It only requires relatively few individuals to carry out a mass casualty attack which would cause serious loss of life, economic harm or damage to our social cohesion.

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

Part 2

Program Performance 2010–11

2

Program Performance 2010–11

Security Intelligence Analysis and Advice

'If we are going to stop a terrorist attack, we need the information and analytical capability to be able to predict, evaluate and ultimately counter the threat.'

Director-General of Security's address at the official launch of the Counter Terrorism Control Centre
21 October 2010

Intelligence Analysis and Advice in ASIO

ASIO's intelligence analysis and assessment function serves a diverse range of customers. Internally, it is essential for understanding the security environment. It identifies trends and themes cutting across subject lines — for example, Australians travelling overseas for terrorism-related purposes. It includes scanning the horizon for potential sources of threat so ASIO and its partners can respond, and it provides context for intelligence officers on a range of strategic issues to support and inform their investigative activities.

Externally, ASIO's intelligence assessments provide unique insight to policymakers and partner agencies working at federal, state and international levels. ASIO's threat assessments are an integral part of the national protective security machinery and inform deployment decisions by law enforcement agencies and the work of the Department of Foreign Affairs and Trade (DFAT), particularly in relation to travel advice for Australians and the security of Australian missions abroad. In all of these settings, ASIO's assessment capabilities contribute to a suite of reporting and advice designed to meet the needs of ASIO's intelligence consumers.

ASIO provides a range of security advice to state and territory governments, including threat assessments, region-specific assessments of violent extremism (to enable more effective implementation of state-based programs countering violent extremism), protective security advice, advice on critical infrastructure protection and cyber-security advice.

Strategic Assessment and Advice

Much of ASIO's strategic analysis is focused on terrorism intelligence assessments — they provide context, insight and foresight into implications for the security environment. Key areas of work are focused on supporting national decision making and policy development — for example, the *Counter-Terrorism White Paper* and the National Security Statement — as well as supporting counter-terrorism professionals.



ASIO's intelligence assessments and advice have helped policymakers understand risk factors related to radicalisation and violent extremism. This intelligence advice plays a key role in developing appropriately focused strategies, particularly in relation to the use of the internet by terrorist or extremist groups as a tool for radicalisation. ASIO has also contributed to an understanding of how the internet affects stand-alone extremists who are unconnected to organisations but nevertheless support their goals.

In 2010–11, ASIO continued to contribute to the work of the Countering Violent Extremism Taskforce within the Attorney-General's Department (AGD), which is developing and coordinating the national approach to this issue. ASIO also produced a range of strategic and thematic assessments, including an analysis of the security implications for Australia of the death of Usama bin Laden.

Threat Assessment and Advice

Threat assessments prepared by the National Threat Assessment Centre (NTAC) are the principal way ASIO advises Commonwealth, state and territory governments, the private sector and international partner agencies on threats to Australia, Australians and Australian interests. They are a key input to Australia's coordinated protective security arrangements.

National Threat Assessment Centre

The National Threat Assessment Centre (NTAC) was established in 2004, bringing together Australian government agencies with a role in collecting, monitoring, collating and analysing all threat intelligence available to the Australian Government. It is located in ASIO and includes attached officers from the Australian Federal Police, the Australian Secret Intelligence Service, the Defence Signals Directorate, the Defence Intelligence Organisation, the Department of Foreign Affairs and Trade, the New South Wales Police, the Department of Infrastructure and Transport and the Office of National Assessments.

Attached officers have access to their own agency's communication systems and databases. This allows for connectivity and coordination between agencies and provides greater assurance that all relevant information available to the Australian Government is assessed and reflected in threat assessment advice. The NTAC now includes ASIO's 24/7 monitoring, alerting and assessment capability, which has enhanced ASIO's capacity to disseminate timely advice in response to developments in the security environment in Australia and internationally.

In 2010–11, ASIO produced 575 threat-related products. ASIO provided threat assessment advice specifically addressing significant shifts in the political and security landscape and other high profile international events. ASIO also produced a number of Commonwealth Heads of Government Meeting (CHOGM) related products, including threat assessments and country reports. ASIO anticipates producing over 100 CHOGM-related products in 2011.

**IN 2010–11
ASIO
PRODUCED
OVER 575
THREAT-
RELATED
PRODUCTS**

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

Business Liaison Unit

ASIO's Business Liaison Unit (BLU), established within ASIO in October 2005, provides a public interface between the private sector and the Australian Intelligence Community. Its principal objective is to raise awareness about national security within the private sector.

The BLU operates a secure website on a subscription basis that is free-of-charge. Reports on the BLU website cover security-related topics including the current security environment, terrorist incidents, threats to industry sectors, violence-prone issue motivated groups, security risk management (physical, personnel and information security), threats to high-profile world events, terrorist tactics and methodologies, and country security snapshots. At the close of the reporting period, there were more than 260 reports, covering domestic and international security perspectives, posted on the BLU website, providing information to 950 subscribers from corporations and government agencies. Industries represented include utilities, oil and gas, transport, and banking and finance.

ASIO's Register of Australian Interests is maintained by the BLU and helps to protect Australian assets and personnel by providing a record of where public and private sector interests are located around the world. The information contained in the register provides ASIO with an understanding of Australian business operations located overseas and enables the provision of more targeted security advice. In 2010–11, the register had around 145 participating companies, with over 1,270 facilities registered in 85 countries worldwide.

Critical Infrastructure Protection Advice

ASIO has a significant role in the Australian Government's national counter-terrorism planning for the protection of critical infrastructure. The Critical Infrastructure Protection Unit is responsible for providing assessments on the threat from terrorism to Australia's critical infrastructure sectors, as well as threats to specific individual assets categorised as nationally vital.

This process includes:

- identifying the nation's critical national infrastructure and interdependencies;
- determining the threats, vulnerabilities and potential consequences of disruption or failure;

- advising the Government of those consequences and vulnerabilities and providing briefings on threats to critical infrastructure to government and private sector stakeholders; and
- maintaining a national database of critical infrastructure assets on behalf of the National Counter-Terrorism Committee (NCTC).

These assessments are used to inform Commonwealth, state and territory governments and relevant industry stakeholders on the threat to nationally critical infrastructure sectors. In 2010–11, ASIO produced 27 critical infrastructure protection reports and undertook 41 briefing sessions, encompassing over 145 government and private sector stakeholders from a range of critical infrastructure sectors.

Cyber-Security Advice

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

In 2010–11, ASIO contributed to the whole-of-government cyber-security policy and crisis coordination arrangements. ASIO engaged with the Attorney-General's Department and other Commonwealth departments and agencies to develop policy that aims for a more secure and resilient cyber-environment for critical infrastructure and across the public and private sectors more broadly.

Advice on Chemical, Biological, Radiological, Nuclear and Explosive Weaponry

In 2010–11, ASIO provided advice to AGD on terrorist interest in, and any attempts to acquire, chemical agents or explosive precursor chemicals.

ASIO also provided regular threat briefings on chemical, biological, radiological, nuclear and explosive (CBRNE) weaponry to key stakeholders, including the National Counter-Terrorism CBRNE Security Sub-Committee and the National Government Advisory Group on Chemical Security.

In 2010–11, ASIO and the Australian Federal Police (AFP) commenced the publication of a series of bi-monthly assessments on the trends in weaponry. ASIO also published regular threat assessments on the threat to Australia's domestic security from radiological and nuclear terrorism. Unclassified CBRNE-related reports were posted on the BLU website, including an analysis of terrorist use of explosives in South and South-East Asia.



Advice for Special Events

In 2010–11, ASIO contributed to whole-of-government efforts to provide useful, timely and accurate advice to protect Australian people and businesses involved in high-profile events of international significance in Australia and overseas. Such events pose, to varying degrees, attractive targets for a range of terrorist groups and violence-prone issue motivated groups. ASIO's contribution included the provision of threat assessments and protective security advice; deployment of personnel to events to coordinate security intelligence information flow and advice; and support to international partners hosting major events.

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

- the Shanghai World Expo in China between May and October 2010;
- the Fédération Internationale de Football Association (FIFA) World Cup in South Africa in June 2010;

- the Commonwealth Games in India in October 2010;
- the G20 Summit in Korea in November 2010;
- the Asia-Pacific Economic Cooperation (APEC) forum in Japan in November 2010;
- the Cricket World Cup in India, Sri Lanka and Bangladesh between February and April 2011; and
- the annual ANZAC Day commemorations in Turkey and France in April 2011.

ASIO's support for the 2010 Commonwealth Games in India was the most significant commitment to date of organisational resources to support an overseas event. ASIO officers played a major role in the Australian intelligence cell which was established to provide local security intelligence support and coordination and operated on a 24/7 basis. ASIO officers also engaged with local and international authorities and provided a conduit of intelligence and threat information relevant to the security of Australian athletes, officials and spectators. The NTAC also provided all-source threat analysis and advice to the Australian Government in the lead-up to and during the Games.

CHOGM, which will be held between 28 and 30 October 2011, will be the biggest international event ever held in Perth. CHOGM will be opened by Her Majesty Queen Elizabeth II and is expected to attract up to 300 delegates from over 50 countries, as well as a large international and domestic media contingent. ASIO has contributed, and will continue to contribute, to the development of security plans for the event, including integrating security arrangements with the National Counter-Terrorism Plan; providing protective security advice, including physical security advice, to event organisers; conducting security checking of all persons requiring accreditation for access to CHOGM venues; providing security intelligence and threat advice for the event participants; and engaging with police and other relevant authorities.

ASIO is working with key foreign partners to support security planning for other future major events, including the Rugby World Cup in New Zealand in September–October 2011 and the 2012 London Olympic Games.

**ASIO'S SUPPORT
FOR THE 2010
COMMONWEALTH
GAMES IN INDIA
WAS THE MOST
SIGNIFICANT
COMMITMENT
TO DATE OF
ORGANISATIONAL
RESOURCES TO
SUPPORT AN
OVERSEAS EVENT**

Proscription-Related Advice

Proscription is an important component of Australia's counter-terrorism framework. The listing of an organisation as a terrorist organisation under the *Criminal Code Act 1995* (Criminal Code) sends a clear message to Australians, and others, that involvement with such organisations, either in Australia or overseas, is prohibited under Australian law. While proscription serves as a deterrent, it is also educative. The listing of an organisation also assists in creating a hostile operating environment for groups wanting to establish a presence in Australia for either operational or facilitation purposes.

ASIO's security advice is one element that informs the Attorney-General's consideration of whether a group should be proscribed in Australia as a terrorist organisation. ASIO provides a Statement of Reasons, which must address the legislative test outlined in the Criminal Code, advising that a group is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not a terrorist act has occurred or will occur); or advocates the doing of a terrorist act (whether or not a terrorist act has occurred or will occur).

When assessing groups for possible recommendation for proscription, ASIO considers a range of factors relevant to security — such as whether a group is engaged in supporting and/or facilitating terrorist attacks — as defined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). ASIO's Statement of Reasons is prepared in consultation with DFAT, AGD and the Australian Government Solicitor. ASIO's role is advisory only and has no decision-making powers in relation to proscription.

The expiration period of regulations proscribing a terrorist organisation under the Criminal Code was extended from two years to three years as part of the *National Security Legislation Amendment Bill 2010*, which was passed by the Commonwealth Parliament on 15 November 2010.

Groups proscribed, re-listed and delisted in Australia in 2010–11

In 2010–11, al-Qa'ida in the Arabian Peninsula (AQAP) was proscribed as a terrorist organisation. AQAP is a recognised affiliate of al-Qa'ida. It operates in Saudi Arabia and Yemen and has claimed responsibility for the attempted attack on Northwest Airlines Flight 253 on 25 December 2009. AQAP is led by a Yemeni extremist, Nasir al-Wahisi, who was once a close aide and bodyguard to Usama bin Laden.

There are currently 19 proscribed organisations in Australia. Those relisted since 1 July 2010 are: the Abu Sayyaf Group, al-Qa'ida, al-Qa'ida in the Lands of the Islamic Maghreb, al-Qa'ida in Iraq, Jamiat ul-Ansar and Jemaah Islamiyah.

While proscription is important in legal, deterrent and educative terms, it is not a threshold for investigation. The activities of groups and/or individuals who promote or use violence can fall within the definition of 'politically motivated violence' in the ASIO Act and, therefore, be of interest to ASIO. Indeed, a group does not need to be proscribed in Australia to be considered by ASIO, Australian courts or the international community as a terrorist organisation.

**A GROUP DOES NOT
NEED TO BE PROSCRIBED
IN AUSTRALIA TO BE
CONSIDERED BY ASIO,
AUSTRALIAN COURTS
OR THE INTERNATIONAL
COMMUNITY AS
A TERRORIST
ORGANISATION**

Investigative Analysis

Leads Development and Analysis

'... ASIO receives millions of pieces of information and secret intelligence every year — the relevance of which requires very careful assessment.'

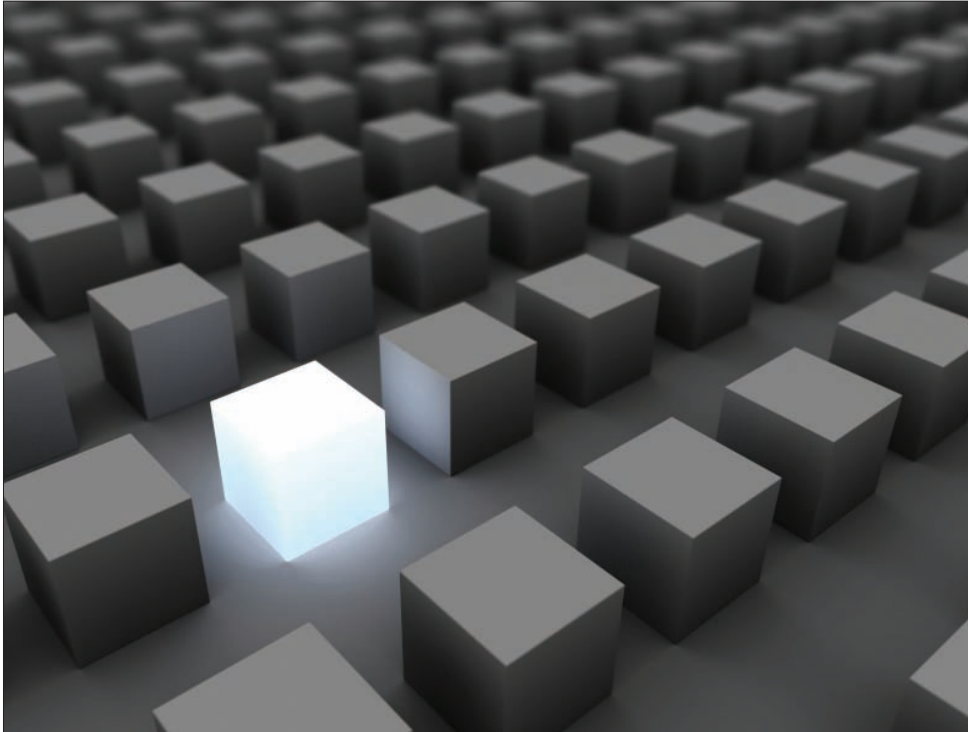
Director-General of Security's address at the official launch of the Counter Terrorism Control Centre
21 October 2010

ASIO relies on information passed to it by members of the public, the police, other government agencies and overseas liaison services. The AGD-managed National Security Hotline (NSH) is a single point of contact for the public to report possible signs of terrorism. Information submitted to the NSH is passed on to Australia's police and security agencies, including ASIO, for analysis and further investigation. In July 2010, the Australian National Audit Office (ANAO) completed an audit of the NSH. An objective of the audit was to determine whether the AFP and ASIO have effective procedures in place to deal with incoming referrals from the NSH. The ANAO found that ASIO's procedures for evaluating NSH referrals are sound and that the documenting of calls warranting further investigation is robust.

Lead intelligence is a vital source of information for ASIO about potential and previously unknown threats. Each lead is assessed to identify its relevance to security, as defined in the ASIO Act, and its relative significance in terms of priorities. ASIO has the discretion to refer matters to other agencies, including the police, if they relate to serious criminal offences. In some cases, lead intelligence has led to major investigations and resulted in ASIO uncovering cases of espionage and foreign interference, weapons proliferation and terrorism. Resolution of lead investigations often relies heavily on continued collaboration with state, territory and federal police services. The presence of secondees from the Australian Customs and Border Protection Service (ACBPS) and the AFP in ASIO's leads investigation area allows investigations

to benefit from secondees' contact with their home agencies and information holdings.

In 2010–11, ASIO officers met with overseas counterparts to benchmark and refine ASIO's leads assessment, evaluation and investigation methodology. The ASIO delegation provided briefings on leads methodology and lessons learned regarding structure, training, staffing and processes.



Intelligence Reporting

ASIO strives to provide security advice in a form that best meets customer demands and to actively support the aims and the principles of the *National Security Information Environment Roadmap: 2020 Vision* regarding enhanced information sharing across the national security community. Following a comprehensive review of intelligence reporting product lines and client needs, in July 2010 ASIO introduced a new, rationalised suite of easily identifiable reporting products covering investigative, analytical, threat, liaison and other categories.

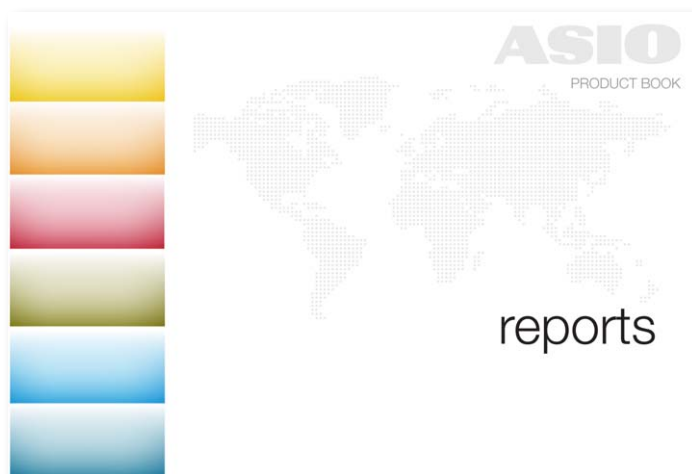
Throughout 2010–11, ASIO, through its Intelligence Reporting and Production Client Liaison Unit, conducted an extensive program of engagement with recipients of ASIO product to seek feedback on the new product range. The

feedback confirmed the rationalisation of product has enhanced information sharing and product quality. Key international partners described ASIO's product as 'leading edge' and are exploring options to better digest ASIO reporting — confirming the high value placed upon it. However, clients identified accessibility of ASIO reporting as an area for improvement. In response, ASIO is exploring a variety of ways to better reach partners, including through an upgrade to a secure web page. Internally, ASIO is exploiting a new information management system to make formal product dating back to 1993 more readily accessible to staff electronically.

**THE FEEDBACK
CONFIRMED THE
RATIONALISATION
OF PRODUCT
HAS ENHANCED
INFORMATION-
SHARING AND
PRODUCT QUALITY**

A key component of ASIO's strategic assessment and analysis product is visualisation, mapping and analytical frameworks. Incorporating dynamic visualisation images with traditional text, ASIO can explore and summarise information and convey key intelligence judgements and findings in more easily digestible ways for readers.

In 2010–11, ASIO produced 2,967 reports and shared product with 347 partners — both domestic and foreign. To ensure ASIO's products are useful and relevant, fill identified intelligence gaps and are driven by key client needs, ASIO's intelligence reporting, planning and production processes align closely with the National Intelligence Priorities (NIPs). In 2010–11, 91 per cent of product related to matters coming within the two highest tiers of the NIPs.



ASIO Product Book

To support the launch of ASIO's new product lines in July 2010, ASIO produced a brochure to explain the nature and purpose of each product type. The product booklet was well received by clients, who reported it assisted in raising awareness of the range and function of the various ASIO products as well as identifying which product might be of most relevance to their functions.

Security Assessment Advice

ASIO provides security assessment advice to appropriate areas of government concerning risks to security, including links to terrorism, espionage or foreign interference.

ASIO's security assessments are not just 'checks'. They are investigations, which can be complex and routinely involve subjective and predictive judgements about the harm to Australia's security that may arise from issuing a visa or granting access (for example, to dangerous goods or to the Australian Nuclear Science and Technology Organisation) to the individual in question. Complex investigations can take an extended period of time. Australia's national security considerations take precedence at all stages.

Passports

Australia has international legal obligations, as well as the moral obligations of good international citizenship, that require Australian authorities to act to prevent terrorist acts overseas, especially when Australian citizens are implicated. Under the *Australian Passports Act 2005*, ASIO may request the cancellation of an existing Australian passport, as well as the refusal of an application for a new Australian passport, on security grounds. Under the *Foreign Passports (Law Enforcement and Security) Act 2005*, an adverse ASIO security assessment can also be grounds for the Minister for Foreign Affairs to demand the surrender of a foreign travel document.

**WITHOLDING
PASSPORTS IS AN
IMPORTANT MEANS
OF PREVENTING
AUSTRALIANS
FROM TRAVELLING
OVERSEAS TO
TRAIN, SUPPORT
OR PARTICIPATE IN
TERRORISM**

Withholding passports is an important means of preventing Australians from travelling overseas to train, support or participate in terrorism. It may also be used to help prevent an Australian already overseas from participating (or further participating) in activities that are prejudicial to the security of Australia or another country. Consistent with its obligations, in 2010–11 ASIO issued adverse security assessments for the passports of seven individuals. This compares with eight in 2009–10.

A security assessment remains valid until it is replaced — it can be superseded by a new assessment, which would take account of the information available at the time. During the reporting period, three individuals who were previously the subject of an adverse assessment by ASIO — and consequently had their passports withdrawn or applications denied — were the subject of new security assessments. Such assessments are not a recanting of ASIO's previous assessment but rather a new assessment based on new information, circumstances and factors relevant to the issue of whether that particular individual poses a risk to Australia's or another country's security. New assessments can provide a basis for the return or renewal of a passport.

Visa Security Assessments

An equally important activity in protecting Australia from terrorism and maintaining Australia's security is preventing individuals who have been assessed as posing an unacceptable risk to security from entering Australia. ASIO also uses the visa security assessment process as part of its defensive response to foreign intelligence activity. The security checking undertaken by ASIO in respect of visa security assessments varies according to the purpose for which an assessment is being made — for example, whether an assessment is being made to determine suitability for community-based detention in Australia or to determine the suitability for an individual to reside permanently in Australia.

ASIO and the Department of Immigration and Citizenship (DIAC) have a longstanding arrangement for the referral of visa applicants to ASIO for security assessment purposes. These apply in respect of all visa streams, including irregular maritime arrivals (IMAs) and onshore protection visas. The criteria under which this referral occurs are determined by ASIO. The visa referral process is intelligence-led and risk-managed and involves close cooperation between ASIO and DIAC.

In its *2009–10 Report to Parliament*, ASIO highlighted the need to divert resources to undertaking security assessment of IMAs for DIAC. Prior to 2011, it was government policy that all IMAs be subject to the full ASIO investigative security assessment process. This proved difficult due to the complexity of the investigations and because of the numbers involved. In December 2010, the Government also decided that only those with refugee status would be referred to ASIO for the purpose of determining suitability — on national security grounds — to reside permanently in Australia. In January 2011, ASIO developed a referral framework, which commenced operation in March 2011. The new framework has enabled ASIO to focus on complex IMA cases requiring intelligence investigation and to streamline the security process for

non-complex cases in accordance with the risk to security they present.

ASIO completed 34,396 visa security assessments in 2010–11, as a result of which 45 visas were refused or revoked. ASIO issued 40 adverse assessments on counter-terrorism grounds, two on the grounds of involvement in people smuggling and three on the basis of counter-espionage or foreign interference concerns.

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

* 2,058 protection visas assessed under revised framework as of April 2011.

Table 1. Visa Security Assessments 2010–11

Frequently asked questions about ASIO's Role in Visa Security Assessments

Is ASIO responsible for all delays in the processing of irregular maritime arrivals?

An ASIO security assessment forms part of the Department of Immigration and Citizenship's (DIAC) overall consideration of whether to issue a permanent Australian visa. DIAC is responsible for determining the refugee status for all irregular maritime arrivals and checks an individual's identity and health prior to making a decision.

At 30 June 2011, there were 5,738 irregular maritime arrivals in immigration detention, of which 456 had been found to be refugees and were awaiting security assessment — this represented eight per cent of those in detention at that time.

Does ASIO require irregular maritime arrivals to remain in detention whilst it undertakes its security assessment?

It is not a requirement under the *Australian Security Intelligence Organisation Act 1979* that irregular maritime arrivals (IMAs) remain in detention during the security assessment process. The detention of IMAs is managed by the DIAC, in accordance with Australian Government policy.

ASIO is doing fewer assessments under the new referral framework. Does this mean ASIO is being less thorough in assessing whether IMAs pose a threat to national security?

In 2011, ASIO implemented changes to the security assessment process to ensure an intelligence-led and risk-managed approach to security assessments and to ensure ASIO resources are most appropriately utilised. Under the security referral framework, all IMAs continue to be the subject of intelligence-led and risk-managed security checking. The framework allows ASIO and the DIAC to work together to ensure only IMAs who have been found to be refugees are subject to a security assessment as part of considering their eligibility for a visa. As a result, ASIO has avoided much of the duplication experienced in the previous year, when it was required to assess all IMAs regardless of their eligibility for refugee status.

The framework, which enabled ASIO to focus on more complex cases during 2010–11, also resulted in some efficiency gains, including a decrease in the number of security assessments requiring the most extensive investigative processes. However, ASIO has not compromised on Australia's national security, and its security assessments continue to be thorough.

Does ASIO keep identification documents provided by IMAs?

ASIO does not request, take possession of or retain documents belonging to IMAs. On occasion, IMAs offer ASIO photocopies of documentation to assist with the security assessment process.

Does ASIO seek information from an IMAs country of origin to make its security assessment?

ASIO is mindful of obligations on the Commonwealth under international human rights and refugee law and works to ensure that its activities concerning irregular maritime arrivals are conducted in accordance with those obligations. During his appearance at the public hearing by the Parliamentary Joint Committee on Intelligence and Security into visa security assessments in June 2011, the Director-General of Security stated:

I can give you a categorical assurance that ASIO's policy, in accordance with government policy and with Australia's international obligations, does not refer the names of individuals who have sought asylum in Australia to the host government. We just do not do it. So our decisions are not, therefore, made on the basis of information provided about an individual from the host government.

Counter-Terrorism Security Assessments

ASIO undertakes counter-terrorism security assessments for a range of purposes including:

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

Type of Access	Number of Assessments Completed
ASIC	67,501
MSIC	30,421
Dangerous Goods (ammonium nitrate/explosives)	9,101
ANSTO	1,274
Special Events (CHOGM)	666
Flight Crew	203
Total	109,166

Table 2. Counter-Terrorism Security Assessments 2010–11

ASIO conducts counter-terrorism security assessments to determine whether an individual has any known links of relevance to security. These assessments are separate from criminal checks undertaken by other agencies.

In 2010–11, ASIO completed 109,166 counter-terrorism security assessments, 97,922 of which were ASIC and MSIC assessments. Overall, ASIO completed eleven per cent more counter-terrorism security assessments in 2010–11 than in 2009–10. In 2010–11, ASIO issued two adverse counter-terrorism security assessments; one was for access to dangerous goods and the other was for an ASIC — this is the first time ASIO has issued adverse security assessments for these purposes.

In 2011, ASIO undertook counter-terrorism security assessments for MSIC renewals for the first time. Over the forthcoming reporting period, ASIO anticipates a substantial increase in counter-terrorism security assessment workload as a result of MSIC renewal and CHOGM 2011 accreditation (onshore) counter-terrorism security assessment referrals.

Personnel Security Assessments

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

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

ASIO issued two qualified personnel security assessments in 2010–11.

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

Table 3. Personnel Security Assessments 2010–11

Involvement in Litigation

ASIO has continued to contribute actively to prosecutions in national security cases. Its officers and information are often required in evidence or in responding to requests or subpoenae from the prosecution or defence. It has also been involved directly in a number of civil matters arising from the

discharge of its statutory functions. Additionally, ASIO has become involved indirectly in other proceedings from time to time, where its information is relevant in cases involving third parties. Accordingly, ASIO takes seriously its obligations to the judicial process, mindful at the same time of the need to bring to the attention of courts and tribunals any issues which may imperil the effectiveness of future security efforts through the exposure of sensitive capabilities or other information.

In 2010–11, ASIO was involved in over 59 litigation matters. These ranged from criminal (including terrorism) prosecutions and civil proceedings to judicial and administrative reviews of security assessments. The diverse nature of these matters, combined with the increasing level of activity experienced since 2005, produced a significant workload.

During the reporting period, ASIO was involved directly in two legal matters initiated by Mr Mamdouh Habib:

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

In December 2010, the Prime Minister of Australia requested the Inspector-General of Intelligence and Security (IGIS) conduct an inquiry into the actions of relevant Australian agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005.

In May 2011, ASIO issued a non-adverse security assessment in respect of Mr Habib's March 2011 passport application. This was not a recanting of ASIO's previous assessments made in 2006 and 2010 but rather a new assessment based on new information, circumstances and factors relevant to any risk to Australia's security at the time of the new assessment. Mr Habib's AAT proceedings were dismissed on 30 June 2011.

During the reporting period, ASIO was also involved in challenges to a number of its security assessments. In December 2010, the AAT held that it did not have jurisdiction to hear three applications for merits review of IMA adverse security assessments. In a separate matter, in March 2011, the Federal Court dismissed two applicants' challenges to their adverse security assessments, noting there was insufficient evidence to support any of their grounds for appeal.

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

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



Protective Security Advice

ASIO's T4 Protective Security Directorate (T4) provides protective security advice to both the government and the private sector to assist with the protection of classified information, premises and other assets. This advice includes:

- protective security risk reviews for government departments, and critical infrastructure that is rated as nationally vital;
- certification of, and advice in relation to, all Top Secret facilities in Australia;
- evaluation of security equipment and service providers on behalf of the Government's Security Construction and Equipment Committee (SCEC);
- advice on ministerial office security arrangements;
- provision of construction advice in regard to the security of Australian

Government facilities;

- protective security and risk management training; and
- provision of security advice for special events such as CHOGM 2011.

T4 also provides a national technical surveillance countermeasures capability to contribute to the protection of sensitive discussions.

As part of ASIO, T4 is able to draw upon the security intelligence from ASIO intelligence sources — both domestic and international — and to benefit from sensitive technical partnerships with close foreign partners. Throughout 2010–11, T4 continued to work closely with ASIO's NTAC and Critical Infrastructure Protection Directorate, using threat assessments compiled in these areas to inform its protective security recommendations to government and private facilities. ASIO also continued to engage in international security forums, sharing information on protective security practices and technology and applying this in the context of the Australian security environment.



Example of an access control gate at a critical infrastructure facility.

Protective Security Risk Reviews

T4 provides protective security risk reviews and vulnerability assessments, assessing physical, information, administration and personnel security risks, for government and the private sector. As mandated by the Council of Australian Governments, T4 undertakes biennial protective security risk reviews on Australia's national vital critical infrastructure. These reviews provide functional recommendations directed towards achieving operational security objectives, consistent with the requirements of government policy and mitigating security vulnerabilities and risks.

Private industry security consultants, endorsed by the Security Construction and Equipment Committee as having the required technical skills and experience, are often used by clients to implement protective security solutions suggested by T4. In 2010–11, ASIO completed eight protective security risk reviews and/or vulnerability assessments, with efforts focused on critical infrastructure rated as 'vital'.

During the reporting period, T4 also worked with the CHOGM Task Force, the Western Australia Police and the Western Australia Department of the Premier and Cabinet to provide protective security advice on some of the venues being used for CHOGM 2011 in Perth.

Ministerial Office Security Reviews

At the recommendation of the IGIS, following a review of security in 2000, ASIO provides security advice to ministerial offices. ASIO's T4 undertakes these reviews of the security status of ministerial offices twice during the life of each Parliament. The review includes inspection of the office and consultation with office staff. Recommendations are provided to mitigate any risks to sensitive information and assets.

As part of its review of ministerial security in 2010–11, T4 conducted briefings for ministerial staff in partnership with the Defence Signals Directorate (DSD) and the Dignitary Protection Section of the Security Coordination Branch in AGD. In response to the elevated threats against information communication and technology (ICT) systems, DSD provided briefings on ICT security and risks associated with the use of laptop computers, mobile phones, portable electronic devices and external networks. Briefings conducted by the Dignitary Protection Section provided advice and information relating to the personal and physical safety and security of high office holders, including the security of electorate offices and residences and security during domestic and international travel.

During 2010–11 ASIO, in collaboration with DSD and AGD, completed ten ministerial office security reviews.



Top Secret Certifications

ASIO's T4 is the designated authority for the certification of Top Secret government sites. Using risk management principles, government agencies and those private sector agencies that directly support government functions at the Top Secret level are assessed for suitability. ASIO certified 28 sites in 2010–11.

Technical Surveillance Counter Measures Services

ASIO's T4 provides technical surveillance countermeasures (TSCM) assistance to Australian government departments and agencies to ensure that highly classified or sensitive discussions are not subject to compromise through technical means — for example, through covert listening devices.

An interagency TSCM working group was established in March 2011. This working group will provide a more coordinated approach to TSCM work across government. The working group has been established to improve training opportunities and information sharing on equipment and techniques and will provide a platform to develop standards and competency levels across the community.

Security Equipment Evaluations/Catalogue

ASIO's T4 undertakes an ongoing testing and evaluation program of physical security equipment and products. This testing ensures that the product is suitable for use in Australian government facilities and meets the claims made by the manufacturers and that specific applications and limitations are clearly identified. From this program, an extensive list of equipment is produced for use by government security managers and consultants. Linked to this, T4 also provides engineering advice to the Australian government on the appropriateness of a range of technologies. In order to meet changes in technology and the ever-evolving demands of Australia's

**ASIO
CONTINUED
TO ENGAGE
WITH SECURITY
SPECIALISTS
BOTH WITHIN
AUSTRALIA
AND OVERSEAS
TO ENSURE IT
REMAINS AT
THE FOREFRONT
OF EVALUATION
TECHNIQUES**

security environment, in 2010–11 ASIO continued to engage with security specialists both within Australia and overseas to ensure it remains at the forefront of evaluation techniques.

In 2011, the SCEC endorsed a new approach to the evaluation and publication of security products for use within the Australian government. A security equipment evaluated product list will replace the current security equipment catalogue. Similar to the catalogue, the security equipment evaluated product list will be developed for the benefit and assistance of Australian government agencies and will be limited to those products assessed as meeting the requirements for high, administrative or specialised protective security categories.

In 2010–11, ASIO completed 27 security equipment evaluations, 16 locksmith evaluations, six container maintenance evaluations and 13 classified waste service evaluations.

Training for Agency Personnel

ASIO's T4 provides a range of training courses in protective security including to Australian government agency security advisers and agency security personnel. This training equips participants with the skills and knowledge to manage the security responsibilities of their departments. In 2010–11, T4 delivered three agency security adviser courses (50 participants in total), and four training courses for AGD's Protective Security Training Centre (64 participants in total).

T4 also provides training for SCEC-endorsed security consultants, who assist with establishing appropriate physical security environments for the protection

of official information and assets. T4 delivered one course in 2010–11, with ten consultants gaining endorsement. At the expiry of endorsement, SCEC consultants are required to be re-certified under a refresher program.

T4 also trains locksmiths to work with SCEC-endorsed security containers and locks. In the reporting period, 16 locksmiths qualified to work as SCEC-endorsed locksmiths.

Protective Security Policy Framework

Following the launch of the Protective Security Policy Framework (PSPF) by the Attorney-General in June 2010, ASIO continued to make strong contributions to whole-of-government protective security policy development through the Protective Security Policy Committee and the Inter-Agency Security Forum. These contributions included assisting in the development of new PSPF physical, information and personnel security protocols and associated guidelines. Over the forthcoming reporting period, ASIO will focus on the implementation of and compliance with the PSPF, including the new national classification system.

Security Intelligence Investigations and Capabilities

Investigations and Operations

The objective of ASIO's investigative and operational activity is to collect and analyse intelligence about threats to Australia's national security, including from terrorism, and provide advice to mitigate them. ASIO's investigative function is defined by its role as the national security agency rather than by geography. While a significant proportion of ASIO investigations are directed at targets within Australia, ASIO also investigates and assesses activity outside Australia, including threats to Australian interests overseas, and Australian persons who are engaged outside Australia in activities relevant to security. ASIO is the only Australian intelligence agency with the legislative mandate to do so.

Counter-Terrorism

ASIO's investigation of politically motivated violence — terrorism — is the most high profile of ASIO's responsibilities, and the threat posed by Islamist extremist violence remains the most serious threat to the security of Australia

THE NUMBER OF ASIO COUNTER-TERRORISM INVESTIGATIONS AND INQUIRIES HAS GROWN CONSISTENTLY ON A YEAR-TO-YEAR BASIS

and Australians today. The number of ASIO counter-terrorism investigations and inquiries has grown consistently on a year-to-year basis — from just over 100 in 2005 to almost 300 in 2011.

ASIO's counter-terrorism-related investigations range from the investigation of Australians in contact with terrorists offshore to the investigation of potential threats to Australian interests from extremist activity, either in Australia or offshore. This includes Australians with the intent to travel abroad — or who are already abroad — for militant jihad; the attack-planning activities of militant jihadists overseas against Western and potentially Australian interests; and the activities of Australians onshore who are associated with international terrorist groups.



ASIO's counter-terrorism investigations during the reporting period continued to see Australians being drawn to the jihadist message. ASIO identified Australians seeking to travel overseas to engage in terrorism-related activities. To prevent the overseas travel of a number of these individuals, ASIO issued seven security assessments in respect of Australian passports or passport applications.

The conflict in Afghanistan is one factor that has motivated, and continues to motivate, Australians to engage in activities prejudicial to Australia's security interests. Australians have undertaken and continue to attempt to undertake terrorist training in Afghanistan or participate in violent jihad. Australia's alliance with the United States, our active involvement in countering jihadist terrorism and our status as a liberal, Western democracy have resulted in Australia and our interests being written into the jihadist narrative and legitimised as targets.

Counter Terrorism Control Centre

'I am confident CTCC staff and leadership are equipped and prepared to perform the important task of operationalising the control centre and further enhancing Australia's already highly regarded and effective counter-terrorism capability for the protection of all Australians.'

Prime Minister of Australia's address at the official launch of the Counter Terrorism Control Centre
21 October 2010

Announced in the Australian Government's *Counter-Terrorism White Paper 2010*, the Counter Terrorism Control Centre (CTCC) is an ASIO-led multi-agency unit which commenced operation in June 2010. Its role includes, inter alia, the setting and management of counter-terrorism priorities for Australia's counter-terrorism community, the evaluation of agency performance against those requirements and ensuring the process of collecting and distributing counter-terrorism information is fully harmonised and effective. The unit's staff of ten includes Senior Executive Service and/or senior officers from ASIO, the Australian Secret Intelligence Service, the Defence Signals Directorate, the Defence Imagery and Geospatial Organisation and the Australian Federal Police.

In its first year of operation, the CTCC's focus has been the establishment of revised priority-setting mechanisms for the counter-terrorism community. These are aimed at providing clearer direction regarding priorities and a higher level of shared situational awareness, both strategic and operational, within the community.

Separately, senior CTCC seconded staff are also members of both ASIO's Intelligence Coordination Committee and their parent agencies' counter-terrorism management committees. They provide a valuable link between agencies in ensuring coordination of effort and in resolving emerging issues in counter-terrorism cooperation.

Counter-Espionage and Foreign Interference

Espionage and foreign interference in and against Australia are a constant feature of the security environment. While these activities are less visible than terrorism, they pose an ongoing and pervasive threat to Australia's security. The consequences of espionage may not be immediately apparent and the seriousness of those consequences can be affected by future developments.

During 2010–11, ASIO worked closely with its national and international partners, leveraging partners' complementary capabilities, to investigate and respond to the threats representing the greatest potential harm to Australia. ASIO issued three adverse visa security assessments on espionage or foreign interference grounds during the reporting period.

Cyber-Espionage

'ASIO's close cooperation with CERT Australia and the CSOC seeks to identify developing threats and determine appropriate responses. For this reason, ASIO has also established a specialist cyber investigations unit to investigate and provide advice on state-sponsored cyber attack against, or involving, Australian interests.'

Attorney-General's address to the National Security College Senior Executive Development Course Dinner
10 March 2011

Investigations into cyber-espionage continued to be a significant priority for ASIO during 2010–11. In recognition of this challenge, and as part of ASIO's efforts to strengthen its counter-espionage capabilities, a dedicated Cyber Espionage Branch was established in July 2010 to investigate and provide advice on state-sponsored cyber-attack against Australia's interests.

ASIO's cyber-espionage investigations predate June 2010. However, the establishment of the Cyber Espionage Branch reflects the growing significance of this activity in regard to Australia's national security. Furthermore, the establishment of a dedicated branch within ASIO provides a point of focus for its relationships with Australian and international partners on this issue.



Contact Reporting Scheme

Throughout the reporting period, ASIO continued to investigate and analyse reporting from Australian Government employees on suspicious, unusual, persistent or ongoing contact with foreign nationals. During 2010–11, ASIO engaged on a regular basis with departments and agencies to promote awareness of the scheme and its role in protecting the interests of the Australian Government.

Violent Protest and Communal Violence

Lawful advocacy, protest and dissent are part of Australian society, and most Australian issue-motivated groups do not engage in activities that are prejudicial to security. However, a small number of protesters choose to engage in politically motivated violence and those with an agenda that includes violence will continue to exploit or subvert legitimate protest issues for their own ends.

ASIO has a responsibility to respond where individuals or groups promote or use violence to try to achieve a political objective or to influence the policy or acts of a government. In doing so, ASIO observes strictly the provisions of section 17A of the ASIO Act, which does not limit the right of persons to engage in lawful advocacy, protest or dissent.

ASIO OBSERVES STRICTLY THE PROVISIONS OF SECTION 17A OF THE ASIO ACT, WHICH DOES NOT LIMIT THE RIGHT OF PERSONS TO ENGAGE IN LAWFUL ADVOCACY, PROTEST OR DISSENT

Throughout 2010–11, protest activity in Australia remained largely non-violent.

Border Integrity

The ASIO Act was amended in June 2010 to provide ASIO with a new function to investigate serious threats to Australia's territorial and border integrity. ASIO is consequently able to use its capabilities to support the whole-of-government effort and an intelligence-led approach to combat people smuggling.

In 2010–11, ASIO's contribution to whole-of-government efforts was focused sharply on onshore elements of international maritime people-smuggling networks and syndicates that facilitate IMAs' passage to Australia aboard suspected irregular entry vessels. ASIO investigations revealed several groups and individuals of security concern targeting Australia for irregular migration. To minimise the risk to security, effective border control measures are necessary. The security assessment process is an effective means of identifying individuals of security concern and preventing these people from entering Australia.

During the reporting period, ASIO worked closely with partner agencies through a range of interdepartmental bodies such as the Border Protection Taskforce and ACBPS-led operationally focused groups, including the Joint Management Group and the People Smuggling Advisory Group, which bring a whole-of-government approach to intelligence and operational responses to people smuggling.

Counter-Proliferation

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

Capabilities

'In a volatile and unpredictable security environment, where threats can originate offshore and onshore, ASIO needs to work closely, indeed more closely than ever, with its security, intelligence and law enforcement counterparts, both nationally and internationally.'

Statement made by the Director-General of Security before the Senate Standing Committee on Legal and Constitutional Affairs
25 May 2011

ASIO relies heavily on a range of enabling capabilities to support its work in identifying emerging threats and in carrying out security investigations. ASIO's international engagement and technical, surveillance and language capabilities are increasingly supporting not only ASIO's work but also that of ASIO's domestic and international partners. ASIO engages closely with counterparts both in Australia and overseas to develop and share technical, analytical and investigative capability. ASIO partners with a number of agencies in the national security community to ensure that its capability and capacity are deployed effectively to deliver the best outcomes for Australia and its partners.

Investigative, Analytical and Operational Capability

ASIO collects information in support of investigations and to counter threats to security through a range of operational activity. ASIO's operational activity may take the form of interviews with members of the public, including through:

- the Community Contact Program;
- human source intelligence collection;
- intelligence operations, including the use of special powers;
- engagement with state and federal law enforcement agencies; and
- partnerships with the Australian Intelligence Community (AIC) and overseas security and intelligence services.

ASIO officers rely on the cooperation and goodwill of members of the public and may approach anyone in the community for assistance in the course of carrying out the security intelligence functions of the Organisation. With the exception of a questioning warrant, information is provided to ASIO on a voluntary basis. Information provided by members of the public may be of enormous intelligence value and such assistance is always appreciated. ASIO's Community Contact Program is a systematic approach towards ongoing engagement with individuals from a range of communities

represented in Australia and is an important strategy in identifying emerging issues or activities of potential security interest.

ASIO's own collection activity provides a significant proportion of the Organisation's investigative capability, with ASIO officers having the ability to task and receive information from ASIO human sources, surveillance and data collected through technical operations. The wider AIC also provides a significant human intelligence, signals intelligence and imagery intelligence input to ASIO's investigative function. ASIO works closely with other AIC agencies, as well as the AFP and state police services, to further the investigative role of these agencies.

International Engagement

ASIO's security mandate does not end with the geographic boundaries of Australia. Security threats against Australians emanate from many different locations worldwide. The transnational nature of security threats and ASIO's global remit make engagement with, and support from, international partners essential to ASIO's work and effectiveness. Indeed, international liaison relationships are a force multiplier for ASIO, enabling it to draw on the information, expertise and capability of overseas partners to pursue intelligence investigations that transcend national boundaries.

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

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

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

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

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

ASIO has a well-established and structured framework for its international engagement. As ASIO's investigations invariably touch on Australians, officers adhere to specific protocols regulating the exchange of information with overseas services. These include strict accountability measures, including auditing by the IGIS.

**OFFICERS
ADHERE TO
SPECIFIC
PROTOCOLS
REGULATING
EXCHANGE OF
INFORMATION
WITH
OVERSEAS
SERVICES**

Counter-Terrorism Intelligence Training Program — Capacity Building with International Partners

A particularly successful component of ASIO's international engagement agenda is its contribution to the Counter-Terrorism Intelligence Training Program (CTITP). The program, which was established in 2005, delivers counter-terrorism training and capacity building to partner agencies in South-East and South Asia, the Middle East, Africa and the Pacific. A further objective of the program is to enhance counter-terrorism cooperation with partner agencies for our mutual benefit.

CTITP courses conducted both in Australia and overseas cover a broad range of operational, analytical and strategic topics. In 2010–11, CTITP delivered 87 training programs to intelligence, security and law enforcement services of some 21 countries and involving over 1,000 participants. Particular highlights of the program in the reporting period included the annual International Counter-Terrorism seminar, which in 2011 included delegates from 25 agencies from 14 countries and discussed 'Countering Terrorism: Obstacles and Actions'. CTITP also conducted a regional counter-terrorism seminar for other partners in the Pacific, South and South-East Asia.

During the reporting period, CTITP conducted a comprehensive review of training methods and course content, and this led to better tailored programs to meet specific client needs. The program received very positive feedback, and requests for CTITP's training programs from overseas partners continued to increase.

Special Powers under Warrant

ASIO's warranted intelligence collection capabilities are referred to as 'special powers' in the ASIO Act. Like other investigative agencies, legislation grants ASIO powers to collect intelligence under warrant. The criteria for warrants are strictly prescribed and complemented by the Attorney-General's Guidelines. Warrants are available, for a limited duration, to use listening devices and tracking devices, access computers remotely, enter and search premises and examine postal articles. There are also questioning and detention warrants, subject to very stringent criteria, for use in serious counter-terrorism matters. 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 IGIS.

Technical Collection Capability

ASIO's technical collection capabilities make a vital contribution to every priority ASIO investigation and complement the Organisation's human intelligence collection activities. These capabilities must meet the challenges presented by the full spectrum of ASIO's targets, some of whom are particularly technically savvy.



Investment in technical capabilities remained a priority for ASIO in 2010–11. For ASIO, the reality and rate of technological change, the increasing complexity and diversification of the telecommunications landscape in Australia, the continued upward trend in volumes of data to be ingested, exploited, managed and eventually stored or discarded, and the increasing sophistication of ASIO's targets, together with the greater interconnectedness of the world in which ASIO operates, all require significant investment in technical capabilities. Sustained investment and research and development, combined with close cooperation with national and international partners, is necessary to keep pace with developments.

During the reporting period, ASIO contributed its technical expertise to support whole-of-government telecommunications interception-related policy development. ASIO also continued to support national telecommunications interception agencies to develop and maintain their capabilities through the National Interception Technical Assistance Centre (NiTAC) pilot program.

Telecommunications Interception

In 2010–11, telecommunications interception remained a cornerstone of ASIO's technical capabilities and made critical contributions to the Organisation's operational and investigative work.

The combination of increasingly sophisticated, diversified technology and outdated legislation, which has been outstripped by the technology and the way in which technology is now used for purposes that threaten security, means that both ASIO and law enforcement agencies are gradually 'going dark' in terms of their telecommunications interception capabilities. During the reporting period ASIO, as the lead agency within the Commonwealth for technical advice relating to telecommunications interception, worked closely with policy departments and other operational agencies to develop proposals to mitigate the impact on agencies' interception capabilities.

Increased collaboration, technical exchange and burden sharing between agencies are critical components of addressing the telecommunications interception challenge. The NiTAC, which was launched in ASIO on 1 July 2010 on a two-year pilot trial basis, made an important contribution in this area during its first year of operation by assisting a number of Commonwealth law enforcement agencies to develop their interception capabilities in line with the rapidly changing technological environment. The NiTAC will continue to work with interception agencies to ensure they understand the skills, capabilities and techniques required to maintain telecommunications interception as a valuable investigative tool.

ASIO WORKS CLOSELY WITH INDUSTRY PARTNERS ON THE DEVELOPMENT OF NEW CAPABILITIES

As another element of its 'lead house role' in telecommunications interception, ASIO continued its liaison with key participants in the telecommunications industry for the provision of interception capabilities. ASIO performs this function to meet its own needs and also to meet those of the 16 other intercepting agencies. Through this role, ASIO works closely with industry partners on the development of new capabilities and to ensure the functionality of existing ones is not impacted upon adversely by the many changes made to networks. The key relationships established through this role provide an important insight into changes within carriers' networks. This allowed ASIO to provide important protective security advice to some industry participants throughout the reporting period.

Data Exploitation

The complexity and risks associated with ASIO's intelligence roles require timely analysis of large amounts of information. ASIO maintains dedicated capabilities that draw insightful linkages, patterns and trends to identify information gaps and inconsistencies and determine proportionate assignment of investigative attention and resources. In 2010–11, ASIO developed a new analytical technique — using a novel application of data fusion and numeric quantitative techniques — to assist in identifying and assessing the possible implications of changes overseas for trends in violent extremism in Australia.

Research and Development

ASIO reviews regularly the strategic priorities for its research and development program and undertook a major reassessment during 2010–11. ASIO's Science Adviser continued to work closely with domestic and international partners on emerging and disruptive technologies and to coordinate and expand the outsourced research program. Close partnerships with the National Security Science and Technology Branch within the Department of the Prime Minister and Cabinet and with the Defence Science and Technology Organisation remain important links.

During 2010–11, ASIO continued to contribute to the implementation of the Australian Government's National Security Science and Innovation Strategy. Part of the strategy aims to communicate national security challenges — in appropriate terminology and detail — to encourage novel approaches and solutions. This augments the expanded direct outreach and engagement with Australian universities, the Commonwealth Scientific and Industrial Research Organisation and other research providers.

Commonwealth Technical Response Capability

The Commonwealth Technical Response Capability (CTRC) was introduced on 1 July 2010 and provides a framework for state and territory law enforcement agencies to draw on the technical capabilities of ASIO and the AFP at short notice in response to a major terrorist incident or in support of a significant event. During 2010–11, ASIO and the AFP worked closely to exercise and refine CTRC procedures and to strengthen interoperability with state and territory police forces.

Deployment of the CTRC was not sought by state and territory law enforcement agencies during the reporting period. However, the capability was drawn on by both ASIO and the AFP to support operational activities.

Physical Surveillance Capability

In 2010–11, ASIO's physical surveillance capability continued to provide critical support for intelligence collection operations. ASIO surveillance officers work in difficult and sometimes dangerous areas against targets who are undertaking activities that threaten Australia's security and who frequently attempt to conceal their activities from observation. Surveillance reporting provided unique perspectives that opened new lines of investigation, identified activities of potential security concern and enabled other operational activity to take place.



During the reporting period, ASIO worked closely at both the state and federal level, with surveillance teams operated by other Australian agencies, especially in support of counter-terrorism investigations and through joint training. ASIO also commenced implementation of a strategy to enhance the safety, security and effectiveness of surveillance operations. The strategy includes:

- additional recruitment;
- advanced training;
- leveraging Australian and international partnerships;
- acquisition of new technology;
- improved logistics capacity; and
- a risk management model to enhance the efficiency and effectiveness of surveillance resource allocation.

Language Capability

ASIO maintains foreign language capabilities to support the Organisation's

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

Information and Communication Technology Capability and Connectivity

Following a review of ASIO's ICT Strategic Plan in March 2010, in 2010–11 ASIO implemented a number of recommendations to enhance its ICT capability. ICT operates in a rapidly developing and dynamic security environment, and ASIO's role in meeting emerging threats to national security depends to a great extent on ensuring its ICT capability and competency are enhanced, modified and maintained to the highest level. Ensuring ASIO's ICT systems meet developing and changing organisational and operational needs was a key operating factor in the reporting period. ASIO worked with other AIC agencies and the broader national intelligence community to improve capability and connectivity in ICT.

Protecting Capabilities and Information

Those who would threaten the security of Australia or its allies may endeavour to monitor security intelligence activity in order to identify, create and exploit potential vulnerabilities. Protecting from unnecessary exposure ASIO's security intelligence, its sources and the relationships and capabilities which facilitate its collection and analysis is therefore central to ASIO's effectiveness. As part of its significant contribution to meeting the threats confronting Australia's security, ASIO gives careful attention to the ongoing protection of its own information and capabilities. Through 2010–11, ASIO continued to work in close partnership with external stakeholders, such as the Commonwealth Director of Public Prosecutions and the AFP, to ensure that it made a meaningful contribution to litigation within the requirements of the justice process while minimising the risk to ASIO's ongoing effectiveness.

Foreign Intelligence Collection

In addition to its security intelligence function, ASIO has the legislative authority to collect foreign intelligence on Australian matters relating to the defence of the Commonwealth or to the conduct of the Commonwealth's international affairs. In relation to telecommunications interception operations, these matters also extend to Australia's national security, Australia's foreign relations and Australia's national economic wellbeing.

ASIO's foreign intelligence collection work is substantial and in 2010–11 resulted in a substantial amount of valuable reporting to ASIS and DSD on issues designated as very high national priorities requiring intensive coverage.

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 collection agencies, ASIS and DSD.



Part 3

Outcomes & Highlights

3

Outcomes & Highlights

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

3

Outcomes & Highlights

Part 4

Accountability

4

Accountability

ASIO and Accountability

'Our law makers have ... [put] in place an extensive legislative, regulatory and oversight regime that works well in the Australian context, ensuring that intelligence agencies act with the appropriate levels of propriety, legality and respect for human rights that ordinary Australians would expect.'

Director-General of Security's speech to Monash University
15 April 2011

ASIO operates under a thorough oversight and accountability framework. This allows for scrutiny of ASIO's activities by a range of oversight bodies, including the Attorney-General, parliamentary committees, the Inspector-General of Intelligence and Security (IGIS) and the Australian National Audit Office. Because much of ASIO's work necessarily occurs outside of the public view, ASIO's oversight and accountability framework ensures the Organisation operates professionally and with propriety in respect of both the requirements of security and the individual rights of Australians.

Attorney-General

Attorney-General's Guidelines

Under section 8A(1)(a) of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), the Attorney-General may give the Director-General of Security written guidelines to be observed by ASIO in the performance of its functions. The guidelines:

- set out the Attorney-General's expectations of ASIO in the collection and handling of personal information;
- provide guidance on when information obtained in an investigation is relevant to security;
- clarify when ASIO can communicate information in its possession which, although not relevant to its security function, should nevertheless be communicated because there are public interest reasons for communicating the information;
- set out relevant principles that govern ASIO's work; and
- incorporate the current definition of politically motivated violence and provide additional guidance on the investigation of violent protest activities relating to threats to various specified persons.

The guidelines require investigations to be conducted with as little intrusion into privacy as possible, consistent with the national interest. ASIO's methods are determined by the gravity and immediacy of the threat to security

posed by the subject. Where the threat is assessed as serious, or where it emerges quickly, a greater degree of intrusion may be necessary. Strict warrant procedures govern the use of more intrusive powers, which are not employed unless the subject's activities are, or are reasonably suspected to be, prejudicial to security.



The Attorney-General, The Hon. Robert McClelland MP, at the official launch of the Counter Terrorism Control Centre in October 2010.

Proposals to collect intelligence are subject to rigorous internal consideration and approvals at a senior level. Documentation for warrants is reviewed by ASIO's Legal Division and the Attorney-General's Department (AGD) before the Director-General of Security agrees to request a warrant from the Attorney-General. Warrants are issued for limited periods. At the expiry of each warrant, ASIO must report to the Attorney-General on the extent to which the operation helped ASIO carry out its functions.

The IGIS has access to all warrant material and monitors the process regularly. The IGIS examines and audits all ASIO warrant documentation. The Director-General of Security may issue warrants for up to 48 hours in emergency situations. The Attorney-General must be advised of any such warrant.

Parliamentary Oversight

ASIO is subject to oversight by a number of Australian parliamentary committees. Throughout the year, ASIO attends hearings and provides classified and unclassified submissions, briefings and advice to the Parliament, including through its annual report. ASIO produces an unclassified Report to Parliament annually, which must be tabled by 31 October each year. It also produces a classified annual report, which has a limited circulation amongst senior government officials. ASIO is the only Australian intelligence agency to produce both a classified and an unclassified annual report.

National Security Committee of Cabinet

The National Security Committee (NSC) is a Cabinet committee chaired by the Prime Minister which considers and makes decisions in relation to security issues of strategic importance to Australia, Australia's response to developing situations (either domestic or international) and classified matters relating to aspects of operations and activities of the Australian Intelligence Community (AIC). The NSC also determines resourcing for Australia's intelligence agencies, sets national security priorities and monitors agencies' performance against those priorities throughout the year. The NSC is supported by the Secretaries Committee on National Security (SCNS). The Director-General of Security attends all NSC meetings and is also a member of SCNS.

Parliamentary Joint Committee on Intelligence and Security

Parliament first appointed the Parliamentary Committee on ASIO, the Australian Secret Intelligence Service (ASIS) and the Defence Signals Directorate (DSD) in March 2002. This committee was replaced by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on 2 December 2005 following recommendations in the report of the 2004 Flood Inquiry into Australian Intelligence Agencies. The PJCIS also includes the Defence Imagery and Geospatial Organisation (DIGO), the Defence Intelligence Organisation (DIO) and the Office of National Assessments (ONA) in its oversight role.

The PJCIS is appointed under section 28 of the *Intelligence Services Act 2001* (IS Act). Section 29 of the IS Act states that the functions of the committee are:

- to review the administration and expenditure of ASIO, ASIS, DIGO, DIO, DSD and ONA, including their annual financial statements;
- to review any matter in relation to ASIO, ASIS, DIGO, DIO, DSD and ONA referred to the committee by the responsible minister or a

resolution of either House of Parliament;

- to review, as soon as possible after the third anniversary of the day on which the *Security Legislation Amendment (Terrorism) Act 2002* received royal assent, the operation, effectiveness and implications of amendments made by that Act and the following Acts: the *Border Security Legislation Amendment Act 2002*, the *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002*; and the *Suppression of the Financing of Terrorism Act 2002*;
- to review, by 22 January 2016, the operation, effectiveness and implications of Division 3 of Part III of the ASIO Act ‘Special powers relating to terrorism offences’; and
- to report the committee’s comments and recommendations to each House of the Parliament and to the responsible minister.

In 2010–11, ASIO provided its annual, classified *Review of Administration and Expenditure (No. 9: 2009–10)* to the PJCIS. An unclassified version of the review was made available on the PJCIS website (www.apf.gov.au/house/committee/pjcis.reports.htm). ASIO also engaged with the PJCIS on several occasions throughout the reporting period. In March 2011, ASIO appeared before the PJCIS to respond to questions on its administration and expenditure. Later, in June 2011, ASIO appeared before the PJCIS in a public hearing to respond to questions on security assessments. The public hearing was also attended by several asylum seeker advocacy groups.

Senate Standing Committee on Legal and Constitutional Affairs

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

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

- security assessments;
- ASIO’s new central office;
- budget and staffing;
- cyber-espionage attacks on the Department of Parliamentary Services network;
- WikiLeaks;
- the Intelligence Services Legislation Bill 2011;

- the IGIS’s inquiry regarding Mr Mamdouh Habib;
- Mr Habib’s Commonwealth compensation claim and settlement;
- counter-terrorism laws; and
- personnel security assessments and vetting procedures for Australian Government employees.

ASIO also responded to 29 questions on notice during the reporting period.

Inspector-General of Intelligence and Security

THE OFFICE OF THE IGIS IS A CRITICAL COMPONENT OF ASIO'S EXTERNAL ACCOUNTABILITY FRAMEWORK

The Office of the IGIS is a critical, independent component of ASIO's external accountability framework. The IGIS provides assurance that ASIO — along with the other AIC agencies — acts legally, with propriety, in accordance with ministerial guidelines and directions and with due regard for human rights. Through the exercise of the IGIS's inspection and inquiry functions and through a wider program of engagement and consultation, the IGIS maintains comprehensive scrutiny of ASIO's activities and has visibility of ASIO policy development and strategic reform programs.

Inspections

To monitor ASIO's compliance with legislation, ministerial guidelines and internal policies and procedures, the IGIS maintains a rigorous schedule of routine inspections of ASIO's conduct of investigations, use of special powers, engagement with other Australian agencies and access to their information, and sharing of information on Australian people and companies with foreign agencies.

Additionally, the IGIS occasionally investigates agency-specific or cross-AIC practices or policy approaches to particular issues, with a view to making recommendations for improvements. In September 2010, the IGIS concluded a report on 'Policies, Procedures and Practices in the AIC for Exchange of Information with Foreign Liaison Organisations', in response to which ASIO refined its internal business processes.

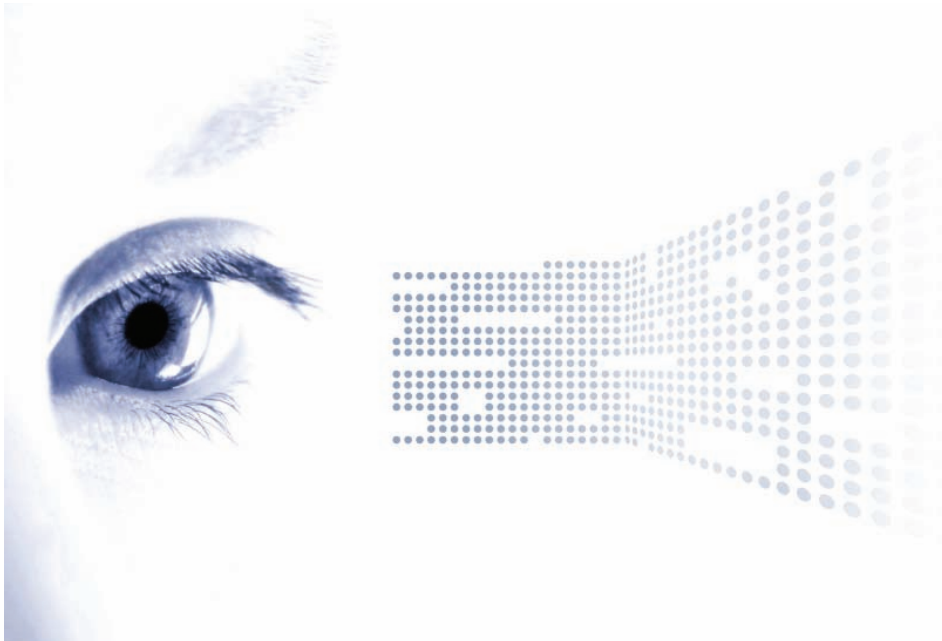
Inquiry

In December 2010, the Prime Minister of Australia requested that the IGIS conduct an inquiry into the actions of relevant Australian agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005. In respect of this inquiry, ASIO facilitated the IGIS's access to ASIO's information holdings and provided evidence through interviews, to disclose any relevant material or information which ASIO or its staff might possess on this matter. The Habib inquiry is an example of the exercise of the IGIS's formal inquiry power at the request of the Prime Minister. Additionally, the IGIS can conduct an inquiry in respect of ASIO at the request of the Attorney-General, in response to a public complaint or through the IGIS's own motion.

In 2010–11, as in recent years, the majority of investigations conducted by the IGIS relating to ASIO concerned complaints by visa applicants who believed delays in the processing of their applications were a result of an outstanding ASIO security assessment. The IGIS has noted that the increase in such complaints is driven in large part by the increase in the number of irregular maritime arrivals to Australia. ASIO continues to work closely with the IGIS (as well as other agencies) to introduce more effective processes for the management of security assessments.

Regular Engagement with ASIO's Senior Executive

ASIO values the important role the Office of the IGIS performs in instilling public and government confidence that the Organisation is acting within the law and with propriety. ASIO is both responsive to IGIS requests for advice and information and proactive in respect of identifying emerging issues of likely interest relating to ASIO's activities, organisational perspectives, policy development and strategic direction. Engagement on such matters occurs at regular monthly senior management meetings with the IGIS or through targeted briefings and presentations. ASIO's comprehensive reform of operational policy and procedure to deliver greater effectiveness and efficiency has been a particular area of interest to and constructive consultation with the IGIS.



©iStockphoto.com

Reviews

Independent Review of the Intelligence Community

In 2010, the Government agreed to conduct an independent review of the AIC in 2011, which produced the 2011 Independent Review into the Intelligence Community. The purpose of this review was to examine the AIC and make recommendations on its ability to meet the needs of Government now and into the future. The decision to conduct the review was in line with a recommendation from the 2004 report by Mr Philip Flood AO into Australia's intelligence agencies, which recommended the AIC be subject to reviews on a regular basis.

ASIO welcomed the review as an opportunity to showcase its capabilities and achievements and perspectives from a security intelligence standpoint. It was also an opportunity for ASIO to comment more broadly on the challenges facing the AIC today and to suggest ways to improve the ability of agencies to work together and meet the needs of Government into the future. To that end, ASIO worked closely with the review team. As well as seconding staff to support the review, along with other AIC agencies, the Organisation made three formal submissions to the review secretariat. ASIO also facilitated formal and informal briefings of review staff by ASIO officers from various parts of the Organisation and helped facilitate a number of other support requests made to the Organisation by the review secretary.

ASIO anticipates the review recommendations, to be provided to Government in July 2011, will assist to position the AIC for greater responsiveness, cohesiveness and effectiveness on national interest imperatives as the community moves into the future. ASIO looks forward to its recommendations.³

Internal Audits and Fraud Control

Audit

During 2010–11, ASIO's internal audit team became an independent functional unit operating under the Office of the Director-General and Deputy Directors-General and reporting to the Chair of the Audit and Evaluation Committee (AEC). This structural adjustment reinforces the independence of the internal audit role.

The AEC includes two external members, both senior executives from other agencies — the Australian National Audit Office Signing Officer also attends as an observer. It facilitates internal auditing of ASIO in accordance with the Internal Audit Mandate. The AEC, under its charter, approves the annual audit work program, prioritised according to risk, and supports fraud control and evaluation planning. The effectiveness of the AEC was enhanced during the reporting period through the training of members by the Institute of Internal Auditors in governance, roles and procedures.

2010–11 saw a broadening of compliance audit requirements to take into account changes to assumed identity legislation and strict compliance requirements incorporated into agreements for ASIO access to other agencies' data. Seventeen internal audits were completed in the period and three management-requested reviews were completed, along with the facilitation of an evaluation. The audit activity has focused on improving performance beyond basic compliance to gain efficiencies in effective service delivery.

An expanded internal audit capacity enabled broader performance audit activity covering a range of ASIO's administrative and operational practices. Performance audits conducted in 2010–11 included ASIO's processes for planning and approving capital projects and ASIO's stakeholder engagement as well as audits leading to improved support mechanisms for operational activity.

3

The Independent Review of the Intelligence Community presented its report to Government on 29 July 2011.



ASIO also seeks to undertake broader system evaluations to assist in the assessment of service delivery as well as the efficiency and effectiveness of the Organisation. Two major reviews were undertaken in 2010–11, relating to ASIO’s engagement with another Commonwealth department and the integration of a risk management framework in organisational processes for priority setting in respect of counter-terrorism investigations and assessments.

Fraud Control

AGD released the revised version of the Fraud Control Guidelines (2011) in March 2011. As a result, ASIO updated both the ASIO Fraud Risk Assessment and the ASIO Fraud Control Plan (2011–13). A new requirement of the 2011 Fraud Control Guidelines is the establishment of a fraud policy statement which has been endorsed by the Director-General of Security. ASIO is committed to minimising the incidence of fraud through the development and implementation of a range of fraud prevention and detection strategies.

Fraud and ethics training is a core component of the fraud prevention strategy and is mandatory for all new staff and contractors. Refresher ethics training is mandatory for all staff every three years. ASIO also provides ongoing training via an e-Learning solution.

ASIO has a robust fraud control and detection strategy in place. Central to

this is the commitment of all staff to report any suspected instances of fraud. The Fraud Control Plan articulates clearly the responsibilities of staff and the decision-making authorities. During 2010–11, seven incidents of alleged fraud were reported within ASIO, with one found to be actual fraud. All of these incidents have been dealt with in accordance with the ASIO Fraud Control Plan.

ASIO also responded to the Australian Institute of Criminology's annual fraud survey in September 2010.

Audit of Assumed Identities

Cover and Assumed Identities

Assumed identities and commercial cover arrangements are used to assist in the protection of ASIO officer identities and the prevention of compromise of ASIO activities. All use of assumed identities in ASIO is authorised under Part IAC of the *Crimes Act 1914* (Cth). A small number of assumed identities are also maintained in accordance with the *New South Wales Law Enforcement and National Security (Assumed Identities) Act 2010* where appropriate.

Amendments to both Commonwealth and New South Wales legislation in 2010 mandated periodic review of all assumed identities. Audits of ASIO assumed identities were conducted in January and July 2011 and found no discrepancies or instances of fraud.

AUDITS OF ASIO
ASSUMED IDENTITIES
WERE CONDUCTED IN
JANUARY AND JULY
2011 AND FOUND NO
DISCREPANCIES OR
INSTANCES OF FRAUD

Security in ASIO

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

Security Policy, Awareness and Audit

ASIO has a comprehensive suite of internal security policies to guide and support staff to uphold the highest standards of security practice. In the

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



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

Regular audits are conducted of staff compliance with security policy. Statistics on breaches are reported to ASIO's Corporate Executive Committee on a quarterly basis to monitor trends in security lapses potentially requiring remedial action.

Personnel security

All staff working in ASIO are required to hold a security clearance at the Top Secret Positive Vetting level, and ASIO's policy for re-evaluation of staff clearances exceeds minimum standards required by the Australian Government Protective Security Policy Framework. The rapid growth of the Organisation over the past five years has put enormous pressure on ASIO's personnel vetting and revalidation areas. In 2010–11, ASIO introduced a considered, risk-managed approach to facilitate more timely recruitment and re-evaluation of 'low-risk' applicants and employees while still meeting minimum government requirements. The result was a significant reduction in outstanding clearances and re-evaluations, within an appropriate risk management framework.

ASIO offers a free and confidential counselling service through its Employee Assistance Program to assist staff affected by personal or job-related problems and to promote staff wellbeing. This program is an important means of countering the development of personal security vulnerabilities, which might be exploited or otherwise impact on personnel security in ASIO.

Information Technology Security

ASIO's information technology (IT) security program provides assurance that ASIO's information and communications systems are being used in an authorised, secure and appropriate manner, through auditing, investigation of IT security incidents and IT security policy and advice.

In the reporting period, protection of ASIO externally connected IT systems from attempted cyber (malicious email) attacks was a particular focus of security attention. The implementation of an information-sharing security model to protect the security of ASIO information as the Organisation moves to a single information environment was another important body of work undertaken in the reporting period.

**PROTECTION OF
ASIO EXTERNALLY
CONNECTED IT SYSTEMS
FROM ATTEMPTED
CYBER (MALICIOUS
EMAIL) ATTACKS WAS A
PARTICULAR FOCUS OF
SECURITY ATTENTION**

Security Coordination

The effective coordination and delivery of the many facets of ASIO's security program are assisted by the Security Committee, which reviews and addresses key issues relevant to the security of ASIO people, property and information technology systems and provides a consultative forum to develop

security policies and practices. The Security Committee provides detailed reporting on key security issues, trends and vulnerabilities to the senior leadership group.

Outreach and Engagement

Reaching out to partners — traditional and new, business and industry, academia and the wider community — has become increasingly important for ASIO. As a security intelligence organisation, much of ASIO’s work is necessarily conducted in secret, which can lead to erroneous speculation and commentary about ASIO’s activities. ASIO is dependent on the support and cooperation of its partners and the Australian community; without this support ASIO cannot protect the security and safety of Australians effectively. ASIO therefore pursues a multifaceted strategy of outreach and engagement to build mutual trust and confidence with partners and the public, to draw on external expertise and knowledge and to make as much information available as is possible about ASIO and its work. ASIO does this through its website, speeches by the Director-General of Security to various forums and engagement with the media and through documents such as its unclassified annual report.



Another key element of ASIO’s engagement strategy is to actively seek, and respond to, external feedback on the Organisation’s performance.

ASIO Website

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

Stakeholder Satisfaction Survey

In 2011, ASIO introduced a new model for seeking feedback from stakeholders on their satisfaction with ASIO's engagement and performance. The new approach involves independently administered interviews of high-office holders in those agencies with whom ASIO most closely engages. Feedback was sought on partners' levels of satisfaction with their engagement with ASIO, their views on ASIO's collaboration, stakeholder focus, capabilities and people and their evaluation of the quality, timeliness and accessibility of ASIO information and advice.

Consistent with previous years, stakeholders reported high levels of satisfaction with their engagement with ASIO. ASIO was rated highly as an effective collaborator, particularly through its contributions to whole-of-government outcomes and its sharing of capabilities. Partners considered their ASIO counterparts as professional and capable interlocutors. ASIO's advice, assessments and intelligence were considered mostly relevant and useful, although there may be scope in some instances for ASIO to provide more unique perspectives in its product. Some issues of timeliness of advice in regard to ASIO security assessments were noted by some partners.

The survey indicated collaboration with AIC partners has continued to improve over the past twelve months, and most noted a desire for even greater integration and cooperation in the future. Many identified an interest in expanding opportunities for secondments, exchanges and collaborative work, as well as increasing the regularity of personal engagement at working and senior executive levels. ASIO welcomes this feedback and will work with stakeholders to further enhance relationships.

Federal, state and territory police services commented on the high quality of their partnerships and strong engagement with ASIO. Information sharing

between ASIO and law enforcement partners was seen as effective. ASIO reporting was well regarded, and some services expressed interest in receiving even more product. The Counter Terrorism Control Centre was widely regarded as an exemplar of successful whole-of-government collaboration which has helped clarify respective agency roles and functions and delivered coherence to the counter-terrorism community.

ASIO will work with its partner agencies to exploit ideas proffered through the survey to enhance its engagement with stakeholders and achieve even higher value outcomes for Government.

The other key component of the new survey framework is a complementary online survey which will canvass a range of views and perspectives of stakeholders, at varying levels, in Commonwealth and state and territory governments as well as in private industry. Feedback received through the online survey will enable ASIO to further improve the quality of its engagement and security intelligence advice. The online survey will be conducted in October 2011 and outcomes will be reported in the 2011–12 annual report.

Partnership Forum

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

Public Statements and Media



The Director-General of Security, Mr David Irvine AO, at the official launch of the Counter Terrorism Control Centre in October 2011.

Throughout 2010–11, ASIO continued to engage publicly through speeches and appearances by the Director-General of Security. The Director-General spoke on numerous occasions throughout the year, including to universities, research and private industry groups and at official government functions. The speeches covered a variety of topics, including the current security environment and cyber-security.

Transcripts of public speeches by the Director-General of Security can be found on the ASIO website, www.asio.gov.au.

Official Launch of the Counter Terrorism Control Centre

On 21 October 2010, the Prime Minister of Australia, the Attorney-General and the Director-General of Security officially launched the Counter Terrorism Control Centre (CTCC) in ASIO. A number of journalists accredited to the Parliament House Press Gallery attended the launch, which provided an opportunity for journalists to enter ASIO headquarters and meet ASIO staff. The launch was also attended by representatives from within Australia's intelligence community and wider government.



(From left to right) The Attorney-General, the Hon. Robert McClelland MP, the Prime Minister, the Hon. Julia Gillard MP and the Director-General of Security, Mr David Irvine AO, at the official launch of the Counter Terrorism Control Centre.

The launch received coverage across a wide range of print and broadcast media, reaching a potential audience of nearly two million people.

ASIO's engagement with the media is an important part of the Organisation's commitment to building mutual trust and confidence with the Australian public. Events such as the launch of the CTCC also provide an insight into how ASIO and the Australian Intelligence Community work together to ensure the security of Australia, its people and its interests.

Academia

In 2010–11, ASIO adopted a more coordinated and strategic approach to its engagement with Australian educational and research institutions and think-tanks. The new strategy supports planning for collaboration and the commitment of funding for research initiatives to ensure ASIO maximises the benefit of investment.

University Outreach Program

ASIO has developed a network of research contacts within Australian universities and research institutions and is exploring technical collaboration to enhance existing capability and develop new capabilities. This outreach allows ASIO to keep abreast of a broad spectrum of relevant technologies and expert knowledge and is supported by research contracts with Australian universities and the sponsorship of PhD and master's students.

Lowy Institute

As part of the strategy to enhance outreach with academia, in 2010 ASIO became a corporate member of the Lowy Institute for International Policy — a think-tank generating new ideas and dialogue on international economic, political and strategic developments and Australia's role in the world. The Executive Director of the Lowy Institute visited ASIO to present on the implications for Australia of changes in the international security environment, including the impact on the intelligence community of the shifting shape of global politics and the new architecture of interconnectivity. ASIO's membership of the Lowy Institute enables its staff to attend Lowy seminars and reflects the Organisation's acknowledgement that access to external expertise and knowledge is vital to ensuring ASIO's strategic thinking is progressive.

4 Accountability



Part 5

Corporate Management

People

'The reputation of the Organisation in Government and in the level of trust it enjoys in the Australian community hinges on the capabilities, quality and mettle of its people'.

Director-General of Security's address to Monash University
15 April 2011

In 2000, ASIO employed 584 staff and was focused primarily on potential terrorist threats and communal violence in respect of the Sydney Olympic Games. Over the past decade, the Organisation has become larger and more flexible, diverse and professional in response to a changing international and domestic security environment.

ASIO has made significant changes to its business model and culture, moving from a strict policy of 'need to know' towards a culture of 'responsibility to provide'. During 2010–11, ASIO continued to increase its collaboration with the broader national security community to achieve a common goal of protecting Australia, and Australian interests, from threats to security.

ASIO's people operate in a complex, rapidly changing environment and must continually scan the horizon — not just for existing threats but also for new and emerging threats and challenges.



ASIO needs to ensure that it is positioned to protect Australia's national security both as the nation's security service and as a crucial component of Australia's overall national security community. The work involved in contributing to securing Australia's future is diverse and rewarding, and ASIO officers share a strong culture of commitment to the Organisation, its mission and values.

Human Capital Framework

ASIO's Human Capital Framework is a key output of the independent review of ASIO's people strategy, frameworks and processes. The framework guides a detailed and strategically-oriented approach to workforce planning which includes better integrating ASIO's people management activities, aligning its people processes to deliver outcomes which support business requirements, and strengthening its recruitment and vetting pipeline. The framework is underpinned by guiding principles which drive behaviour in the development and execution of people activities, and continuous improvement across people programs. These principles are focused on outcomes, owned by the executive and unified across divisions. They are agile, progressive, pragmatic and efficient.

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

In 2011, ASIO engaged an independent consultant to review its progress in the implementation of the Human Capital Framework. The review identified that the framework represented best practice in the public and private sectors and identified a number of strengths within the framework which had not been seen outside the Organisation.

**THE REVIEW
IDENTIFIED
THAT THE
FRAMEWORK
REPRESENTED
BEST PRACTICE
IN THE PUBLIC
AND PRIVATE
SECTORS**



The elements of the Human Capital Framework

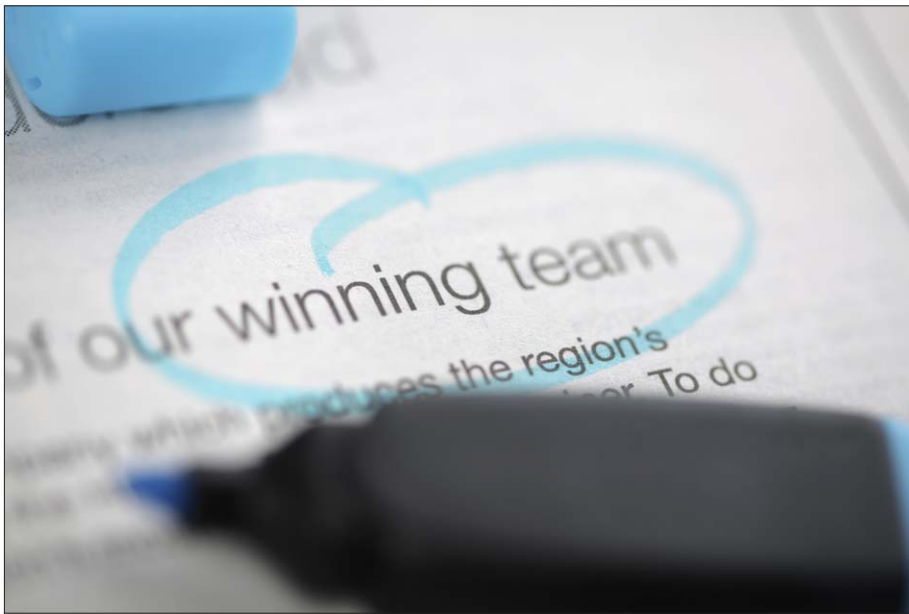
Recruiting ASIO's People

ASIO's strength is in the people it employs, and recruiting the right staff with the relevant skills, temperament and experience is critical to positioning ASIO for tomorrow's challenges in the national security sphere.

During 2010–11, ASIO continued to work towards its substantial workforce growth program, as recommended by the Review of ASIO Resourcing conducted by the late Mr Allan Taylor AM in 2005 (Taylor Review). In previous years, ASIO experienced difficulty meeting these growth targets. While employment market conditions have created a significant barrier, ASIO has achieved its end-point capability growth in a number of areas, such as corporate services. The skill sets ASIO now needs are less readily available in the employment market or require intense in-house development, including in intelligence analysis and collection and technical specialist areas. ASIO undertakes necessarily stringent security vetting for all potential employees. This lengthy, labour-intensive process remains a significant challenge and does not increase ASIO's attractiveness as an employer in a tight labour market.

ASIO is currently implementing the recommendations of a commissioned, independent review of recruitment and vetting. These measures have both a

short and long-term focus and will improve selection and vetting processes, better manage resources and improve return on investment at each stage of the process. Areas of improvement include increasing ASIO's vetting capacity and implementing different, more targeted marketing approaches to reach specialised professions and skill sets. These changes will not compromise ASIO's necessarily high standards.



ASIO is currently on track to reach the Taylor Review target of 1,860 staff during the 2012–13 budget cycle. ASIO welcomed 196 new staff to the Organisation in 2010–11, with 74 per cent engaged on an ongoing basis. As at 30 June 2011, ASIO employed a total of 1,769 staff, representing 1,684 full-time equivalents. In previous years, ASIO's separation rate was influenced positively by the significant workforce growth recommended by the Taylor Review. ASIO experienced a slight increase in its separation rate during the reporting period, from 5 per cent in 2009–10 to 5.8 per cent in 2010–11.

Talent Acquisition

Cognisant of the growing online market, in 2010–11 ASIO continued to utilise the internet to engage with prospective employees. ASIO placed recruitment advertising across a range of online media, including social networking sites, and it continued to attract prospective applicants via its own website, which was updated throughout the year with vacancies and information about positions available within the Organisation. ASIO's expenditure on recruitment advertising decreased from \$1.25 million in 2009–10 to \$1.06 million in 2010–11.

Developing ASIO's People

ASIO People Capability Framework

ASIO launched its People Capability Framework in October 2010. The framework allows ASIO to more accurately describe the capabilities and behaviours required of its workforce to deliver broader and more complex outcomes to the Australian Government. The People Capability Framework was developed using the Australian Public Service (APS) Integrated Leadership System as a foundation. It is future focused, supports ASIO's strategic intent, reflects ASIO's unique role and frames the workforce required to achieve excellence.

The framework will be used to support and guide thinking in relation to workforce management and strategic workforce planning; recruitment, promotion and mobility; induction and orientation; performance management; learning and development; and individual career planning.

Staff Placements

In 2010–11, ASIO's Staff Placements Committee continued to work in accordance with ASIO's strategically focused internal framework to ensure staff were deployed effectively according to organisational requirements and priorities. The committee takes into account an officer's career growth and diversity when considering placements. These considerations allow ASIO to manage individual talents, support staff retention rates and enhance the Organisation's ability to adapt to the changing security environment.

ASIO values and encourages staff exchanges with its Australian and international partners. These exchanges improve ASIO's cooperation and interoperability with a range of other agencies and encourage the sharing of skills, capability, knowledge and information, enhancing national security outcomes. They also provide excellent opportunities for the personal and professional development of ASIO staff.

During the reporting period, ASIO continued to build on its outreach and engagement strategy with regard to staff placements. In 2010–11, there were attachments to and/or from:

- the Attorney-General's Department;
- the Australian Customs and Border Protection Service;
- the Australian Federal Police;
- the Australian Government Solicitor;

- the Australian Secret Intelligence Service;
- the Defence Imagery and Geospatial Organisation;
- the Defence Intelligence Organisation;
- the Defence Security Authority;
- the Defence Signals Directorate;
- the Department of Defence;
- the Department of Foreign Affairs and Trade;
- the Office of Transport Security within the Department of Infrastructure and Transport;
- the Department of the Prime Minister and Cabinet;
- the New South Wales Police;
- the Office of National Assessments; and
- the Western Australia Police.

ASIO staff may also participate in exchanges with ASIO's foreign partners.

Training and Professional Development

ASIO invests in the professional development of its staff as one of three pillars of its strategic program. Internal professional development and leadership development programs are complemented by programs drawing on skills and experience from other parts of government and non-government sectors. Increasingly, ASIO is drawing on the resources of academia and elsewhere to provide programs that meet the particular needs of the Organisation in areas such as strategic analysis, risk management and cultural awareness.



ASIO has a strong learning culture and aims to cultivate professionalism, including through support for external study. ASIO officers may access study assistance, which is designed to encourage continuing education and competency development relevant to the Organisation's work. Study assistance may include additional leave to attend classes and examinations and financial assistance, dependent on the type and relevance of the study undertaken. During 2010–11, ASIO's Study Assistance Program continued to be a key component of the Organisation's people retention, rewards and recognition strategy. ASIO provided assistance to 214 officers enrolled in external study programs across a range of disciplines, such as international studies, law and education. ASIO also fully, or partly, funded the language development training of 17 officers during the reporting period.

In addition to ASIO's Study Assistance Program, in 2011 the Director-General of Security awarded a number of study bursaries to officers who achieved excellence in their academic performance while continuing to make a valued contribution to ASIO's work.

Leadership and Management Skills

ASIO officers have access to a range of leadership programs designed to build skills required for both ASIO and the wider APS. ASIO's programs seek to develop its leaders as individuals with the resilience and dexterity to

ASIO OFFICERS HAVE ACCESS TO A RANGE OF LEADERSHIP PROGRAMS DESIGNED TO BUILD SKILLS REQUIRED FOR BOTH ASIO AND THE WIDER APS

manage and lead. In 2010–11, ASIO continued to implement the leadership strategy it established in 2010. The program is on track to have all leaders in ASIO participate by 2013.

ASIO's seminar series also continued throughout the reporting period. The series allows ASIO officers to engage with presenters from government and academia and seeks to assist ASIO to contextualise its work with broader government priorities. During the reporting period, speakers to the series included representatives from the Lowy Institute, the Australian National University and ASIO's domestic and international partner agencies.

e-Learning

In 2010–11, ASIO continued to utilise e-Learning, a computer-based training method which provides staff with increased access to various training packages to encourage professional development. ASIO developed and implemented 28 new e-Learning modules during the year, with a focus on corporate and systems-based training.



© ThinkStock.com

Intelligence Training

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

ASIO continued to support a whole-of-government approach to intelligence training and partnerships during the reporting period. This included providing presenters and participants for the Australian Intelligence Community (AIC) induction and senior officer development programs and allocating places in ASIO development programs for participants from other agencies.

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

Supporting and Retaining ASIO Staff

Strategic Workforce Planning

ASIO completed the first phase of its Strategic Workforce Plan in 2010–11. The plan forms a key component of ASIO's Human Capital Framework and will ensure that ASIO's workforce has the capability to meet the Organisation's current and future strategic and operational goals. The plan outlines the strategies and actions required to engage, develop and retain the workforce essential to meet ASIO's capability requirements to 2015 and beyond.

For staff, the plan clarifies individual career planning and development options and provides for the design and implementation of programs to enhance engagement and retention of staff. Phase 1 of the plan was completed on 30 June 2011.

ASIO's strategic workforce planning is detailed and strategically focused to enable discussion and agreement around workforce priorities. To manage ASIO's workforce effectively, the Strategic Workforce Plan looks to:

- consider and analyse the capability requirements needed to build and sustain capabilities and deliver agreed outcomes to Government;
- monitor internal demand for capabilities — those which are critical now and those which may become critical in the future;
- determine and plan for the optimal balance of capability within ASIO's workforce;
- scan the environment to determine how labour market forces are impacting upon the supply of skills and capabilities, and how ASIO can best compete for and access the skills it needs; and
- analyse and engage with national security community partners to determine the capabilities ASIO might borrow, share or collectively build.

Performance Management Framework

ASIO employs a highly competent and committed workforce and recognises the importance of harnessing its talent and continuing to foster and develop the capability of its people. Following the introduction of ASIO's Human Capital Framework, ASIO undertook to redesign its performance management framework. The new framework 'Enhancing Performance' is a modern approach to manage, build and deliver capability within ASIO's workforce. It is interconnected with ASIO's mission and objectives and provides opportunities to improve employee engagement across the Organisation.

The framework and associated activities are supported by a range of interactive processes and tools. These aim to cultivate leadership skills and practices, assist managers to focus on managing for performance, support effective performance conversations and plan for individual and professional growth.

The Enhancing Performance framework will be implemented within ASIO from July 2011. It is anticipated it will better align staff efforts with strategic goals and build ASIO's people capability more effectively, now and for the future.



© iStockphoto.com

Diversity, Harassment and Discrimination

ASIO is an equal opportunity employer and employs people from diverse backgrounds. During 2010–11, ASIO implemented recruitment and people management strategies designed to create an inclusive working environment that recognises and utilises the diversity in the workforce, seeking to recruit a range of people that reflect the Australian community.

In February 2011, the Director-General of Security launched ASIO's new anti-bullying and anti-harassment campaign, 'Silence Hurts'. The campaign aligns with ASIO's values and Code of Conduct and is designed to prevent and stop bullying and harassment in the workplace and encourage staff to 'speak up' when they experience or witness inappropriate behaviour. The campaign also helps to foster ASIO's values and to create a workplace culture free of inappropriate behaviour, where, if there is such behaviour, it is addressed actively. The Organisation-wide campaign included the launch of a bullying and harassment hotline, which provides information to staff members and managers on what to do if they experience or witness inappropriate behaviour, and/or support if they have experienced bullying or harassment.

**IN FEBRUARY
2011, THE
DIRECTOR-GENERAL
OF SECURITY
LAUNCHED ASIO'S NEW
ANTI-BULLYING
AND ANTI-
HARASSMENT
CAMPAIGN**



Following the launch of the ‘Silence Hurts’ campaign in February 2011, eleven requests for support or information were raised in the reporting period. The matters ranged from equity and diversity concerns to experiencing or witnessing inappropriate behaviour in the workplace. The increase in reporting in 2010–11, compared with the three cases reported in 2009–10, demonstrates the success of the ‘Silence Hurts’ campaign in promoting greater awareness and improving communication channels.

ASIO Code of Conduct

ASIO staff maintain high professional and personal standards and behaviours that align with the ASIO Code of Conduct. The ASIO Code of Conduct, along with the Organisation’s values, shape the work requirements and behaviour of staff to ensure they conduct themselves in a professional, responsible and effective manner.

The Code of Conduct is available on the ASIO website, www.asio.gov.au.

Occupational Health and Safety

ASIO is committed to ensuring the health and safety of its staff. During 2010–11, time off work as a result of workplace injuries decreased by over 50 per cent compared to the previous year. This is a continuing trend from

2008–09 and 2007–08, when the reductions were 54 per cent and 43 per cent respectively.

In 2010–11, no notifications were made to Comcare under section 68 of the *Occupational Health and Safety Act 1991*. No investigations were conducted under section 41 or any notices issued under sections 29, 46 or 27 of the Act.

ASIO continues to support its staff and is committed to a robust safety culture through health and safety initiatives and workplace risk assessments. ASIO's annual Health Week commenced in September 2010, with a number of activities organised for staff at ASIO's offices nationwide. A large proportion of staff participated in events throughout the week, including health appraisals, consultations with registered dietitians, fitness classes and presentations on enhancing health and wellbeing both in and out of the workplace.

Staff and Family Liaison Office

ASIO's Staff and Family Liaison Office (SFLO) began service in November 2009. Its purpose is to provide an integrated model of wellbeing services that meets the needs of staff and families whilst supporting the Organisation's requirements. During 2010–11, the SFLO provided support to many ASIO staff members who were affected by the Queensland flood crisis. The SFLO also provided guidance to staff regarding available government and community assistance and additional support provisions.

ASIO Ombudsman

ASIO employs an external ombudsman to assist in resolving issues raised by staff who judge they have been treated unfairly or unreasonably by the Organisation, after internal complaints mechanisms have been exhausted. The ombudsman ensures concerns are considered impartially, informally and expediently, and the independent nature of the post provides an additional assurance of transparency and objectivity to the process. The ombudsman reports on a biannual basis on the general nature of his activities to ASIO's Corporate Executive Committee and more explicitly to the Director-General of Security as particular cases require.

In 2010–11, the ombudsman considered a small number of specific staff complaints and provided advice and support in response to informal staff or workplace inquiries. The Director-General of Security also requested that the ombudsman undertake three formal investigations into workplace behaviour and interactions. The ombudsman reported that no issues suggesting systemic personnel problems within the Organisation were encountered.

Employment Framework

ASIO's eighth enterprise bargaining agreement commenced on 1 January 2010, with a nominal expiry date of 30 June 2011. During the reporting period, ASIO staff voted on a new enterprise bargaining agreement which commenced on 21 June 2011, with a nominal expiry date of 30 June 2014. The ninth agreement complies with wider APS parameters and aligns with public sector enterprise bargaining rules. The ninth agreement received 70 per cent acceptance from the ASIO staff who voted. Key outcomes of the ninth agreement included the introduction of top-of-increment payments for staff at the top of their salary band classification, provisions for staff to access annual leave payments at half pay, and a green initiative reimbursement that recognises staff taking steps to reduce their carbon footprint when travelling to and from the workplace.

Senior Executive Service Performance Pay

Sixty-three Senior Executive Service (SES) members were awarded a performance bonus in 2010–11. Seventeen staff members acting in an SES capacity for a period greater than three months received a pro-rata amount. The individual range of performance pay was \$291 to \$16,268, with an average payment of \$7,898. The total amount of performance pay awarded to ASIO's SES officers during the reporting period was \$623,946.

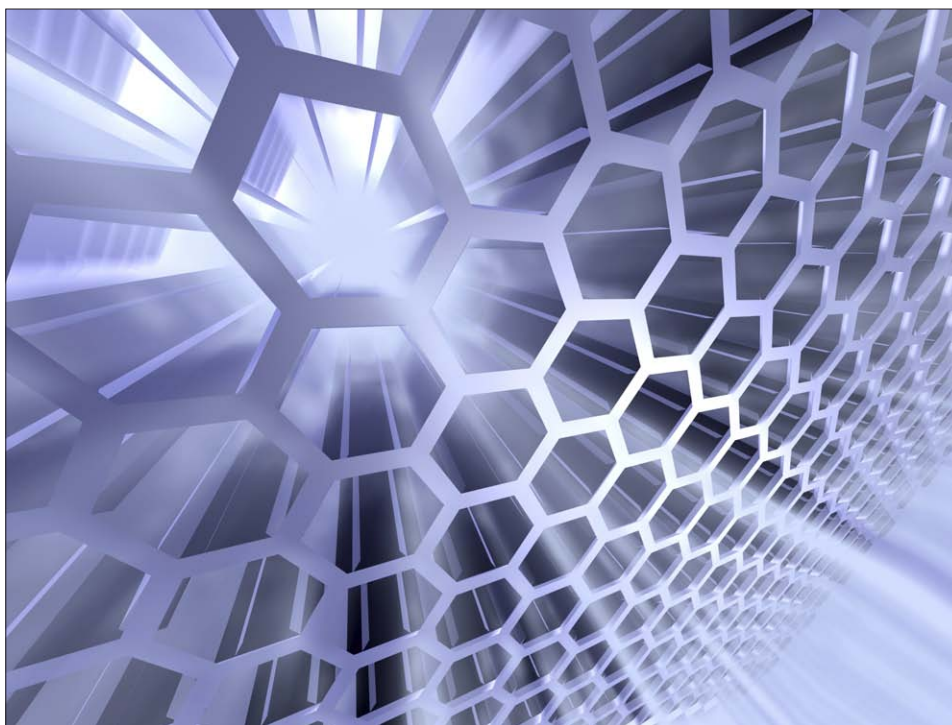
Corporate Capabilities

In 2010–11, ASIO continued its program to realign corporate services. ASIO's change management team worked with ASIO staff to ensure the Organisation is prepared for the relocation to ASIO's new central office in 2012. Workshops were held to identify issues, assess the impact of any changes on work processes and propose strategies to assist staff to reduce any impact on their work during the transition. The change management initiative will continue through the period after ASIO occupies the new building, to ensure staff receive assistance when dealing with the new processes.

Corporate Strategy and Governance

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

ASIO introduced a uniform approach to business planning across the Organisation to ensure it is organising its resources in the best way to achieve results, identify opportunities for continuous improvement to meet emerging challenges, optimise potential opportunities and identify and address potential risks. Business plans align activity at divisional and branch levels closely with ASIO's strategic goals, as articulated in the Strategic Plan 2011–13, and provide a sound basis for governance and performance evaluation. They also provide staff with a shared understanding of the role, direction, work and priorities of the particular areas in which they work and will be linked closely with staff performance agreement processes.



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

ASIO is currently examining its corporate governance structure. A modified framework of high-level decision-making bodies and supporting corporate committees is expected to be introduced early in 2011–12. Currently, the structure has at its core two senior leadership committees — the

Director-General’s Meeting (DGM), which considers the day-to-day tactical business of the Organisation, makes decisions on urgent or emerging issues and monitors progress against ASIO’s strategic agenda; and the Corporate Executive (CE), which is the principal forum for managing strategic corporate priorities, risks, organisational performance and budget and resource issues. The DGM and CE are supported by nine corporate committees, which focus on particular issues or streams of work which are integral to the effective functioning of the Organisation. In 2010–11, the Strategic Workforce Design Committee was established to provide greater focus on workforce management and development issues, in line with ASIO’s strategic agenda.

It is anticipated the improved corporate governance framework will further promote effective resource and risk management in ASIO, enhance accountability and ensure ASIO is preparing for the future by driving activity to meet agreed strategic objectives.



Figure 2. Corporate governance chart

ASIO Strategic Plan 2011–13

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

The plan highlights ASIO’s strategic direction and sets out four key strategic goals to achieve by 2013. These goals will guide ASIO to meet the expectations of the Government, domestic and international partners and the Australian public. The four goals are to strengthen intelligence collection and analysis capability; enhance strategic impact; build and manage the workforce of the future; and improve business processes and practices.

The plan guides business and project planning in ASIO, including performance and development agreements. It also provides a sound basis for the evaluation of organisational performance both internally and through feedback sought from key stakeholders through the annual stakeholder satisfaction survey. The Strategic Plan 2011–13 can be found at the ASIO website, www.asio.gov.au.



ASIO Strategic Plan 2011–13

Roadmap of Key Initiatives

In 2010–11, ASIO continued to pursue its program of organisational change and business modernisation to manage the significant growth of the Organisation effectively and respond to the rapidly changing security and operating environment. The program aims to position ASIO to be flexible and adaptable to further changes in the environment and to utilise resources more efficiently, including by working more effectively and cooperatively with partners in the national security community.

During the period, ASIO implemented a Roadmap of Key Initiatives and a rigorous governance framework to ensure a concentrated focus on progressing projects and proposals to attain strategic goals identified in the program. Initiatives include improving business processes, procedures and systems; enhancing information management and accessibility; increasing the empowerment of people; improving partnerships with domestic and international stakeholders; enabling a focused management of risk; and building and supporting a stronger and more capable workforce.

Notable achievements in 2010–11 included:

- the rollout of an enhanced corporate electronic document and record management system that allows staff to store, access, manage, share and collaborate on corporate documents, records and files through a common user interface. This rollout incorporates a new information sharing business model to better ensure information is accessible to those who need it, when they need it;
- further enhancement of ASIO's operational and analytical capabilities through a comprehensive mapping and review of intelligence business processes, resulting in improved efficiencies and a significant reduction in unnecessary administration. New operational analyst and operational support roles have been created and embedded in operational teams, and ASIO's intelligence prioritisation processes have been re-engineered to better manage collection and analytical risk;
- significant progress towards improving intelligence analysis capability and the timely identification and management of operational risk by better exploiting available or potentially available data. Further development is underway to achieve an enterprise-wide analytical environment that will comprise desktop analytics and complementary complex analytical capabilities. This will involve changed business practices and processes, enhanced staff capabilities and new software suites; and

- the completion of detailed, business-driven scoping to define the specific functionality required for ASIO's electronic case management system. These specifications will now be used to finalise the development of the system for rollout by June 2012.

The roadmap also outlines the importance of building a highly competent workforce with the flexibility and agility to anticipate and adapt to the challenges in Australia's dynamic security environment. ASIO made significant progress towards this throughout 2010–11.

ASIO's strategic agenda and associated work program will continue to evolve and become the primary means to transform ASIO's strategic plan into workplace practices, processes, systems and opportunities which make a real and significant difference both to staff and to the contribution ASIO makes to national security.

Risk Management

ASIO necessarily operates in an environment of risk. A challenge for ASIO, in dealing with threats to the security of Australian people and interests, is to identify the risks, determine the level of acceptable risk and, when risks are near or exceed tolerable levels, develop comprehensive strategies to mitigate them. ASIO's Strategic Risk Management Framework, introduced in 2010, allows ASIO to identify and assess risks to the Organisation and the effective conduct of its functions and to implement risk treatment plans where risks are not considered acceptable.



© Thinkstock.com

In 2010–11, ASIO enhanced its approach to risk management by integrating processes for managing risk into the Organisation’s overall governance, business planning and project management frameworks and performance reporting processes. Further work is underway to develop tools to standardise risk assessment and management in operational planning and to further embed it in ASIO’s culture.

ASIO Internal Performance Reporting

ASIO’s senior leadership group rigorously assesses its performance against specific benchmarks on a quarterly basis, utilising a ‘traffic light’ evaluation system. Underperformance against particular outputs or goals can impact on decisions and resourcing, changes to operational or corporate priorities, and whether specific strategies need to be implemented to address the situation. In 2010–11, ASIO undertook mapping of the relationship between strategic risks identified in the Strategic Risk Management Framework and performance reporting benchmarks to assess the extent to which performance reporting informs ASIO’s management of strategic risks. The project has produced greater alignment between these two critical governance mechanisms.

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

Enterprise Resilience

Through its Enterprise Resilience Program, ASIO seeks to develop an integrated, coordinated and consistent approach to protecting critical business functions and physical and information resources and ensuring their continuity. ASIO established the Enterprise Resilience Coordination Working Group in 2010–11, drawing from staff in a number of resilience disciplines. At the close of the reporting period, the working group was reviewing business continuity arrangements across the Organisation and coordinating the development of specific business impact assessments. The focus of enterprise resilience during the period, and likely to be continued in 2011–12, is business continuity planning in readiness for ASIO's move to its new central office.

Legislation

ASIO works collaboratively with other Commonwealth departments and agencies to ensure that Australia's legislative framework continues to support ASIO's functions and capabilities. During 2010–11, ASIO contributed to several proposed legislative amendments and policy developments. Legislative initiatives of relevance to ASIO which were progressed during the reporting period are detailed below.

Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011

The Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011 commenced in March 2011. The amendments enhance cooperation, assistance and information sharing between Australia's security, intelligence and law enforcement agencies in support of key national security priorities.

For ASIO, the legislation provides greater flexibility to share intelligence and information with the broader national security community, within strict guidelines, and enables it to cooperate with and provide assistance to law enforcement agencies in relation to telecommunications interception and other areas of expertise such as technical support, logistics and analytical advice.

Intelligence Services Legislation Amendment Bill 2011

The Intelligence Services Legislation Amendment Bill 2011 was introduced into Parliament in March 2011. The Bill will enhance interoperability within the AIC, and is expected to be passed during the 2011–12 financial year.⁴

The Bill included measures to:

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

⁴ The Intelligence Services Legislation Amendment Bill 2011 was passed on 4 July 2011.

Telecommunications Legislation Amendment (Cybercrime Convention) Bill 2011

The Telecommunications Legislation Amendment (Cybercrime Convention) Bill 2011 was introduced into the House of Representatives on 22 June 2011. At the end of the reporting period, this Bill remained under consideration by the Australian Parliament. The Bill proposes a regime to allow interception agencies to request the preservation of telecommunications until a warrant can be sought to authorise the agency's access to the content of those communications.

Information Services

Release of ASIO Records

ASIO is an exempt agency under the *Freedom of Information Act 1982*, but it is subject to the release of its records under the *Archives Act 1983*, which was amended in May 2010 to allow public access to all Commonwealth records over 20 years old. Transition arrangements were implemented in January 2011, with two years of records becoming available each year for the next ten years, resulting in full implementation of the change by 2020. It is anticipated there will be a significant increase in workload for ASIO as more records are released during, and following, the transition period. However, it is likely a greater percentage of material will be partially or totally exempted due to the increasing sensitivity of the material.

Requests to access ASIO records that are in the 'open period' and not released publicly can be made to the National Archives of Australia (NAA). Subject to the request meeting eligibility criteria, the NAA passes the application to ASIO, where relevant records are located and assessed. ASIO determines whether any information should be exempt from public release on national security grounds, balancing public access and the need to protect sensitive information. In most cases, the information is released and is available for public access.



During 2010–11, ASIO received 409 applications for access to records, a decrease from 583 in 2009–10. A total of 374 requests were completed during the reporting period, including some requests carried over from previous years. ASIO assessed a total of 48,096 pages during 2010–11, representing a decrease from 65,952 folios assessed in 2009–10. This decrease reflects the complexity of a number of requests and the ongoing processing of requests from the previous year.

ASIO GIVES GREATER PRIORITY TO REQUESTS FROM THOSE SEEKING RECORDS ON THEMSELVES OR FAMILY MEMBERS

ASIO gives greater priority to requests from those seeking records on themselves or family members. ASIO completed 187 such requests in 2010–11 compared with 153 in 2009–10. 91 per cent were completed within the benchmark of 90 days.

In 2010–11, ASIO completed 86 per cent of all Freedom of Information requests within 90 days, the same percentage as the previous year. This reflects the ongoing impact of assessing very large and complex requests and the need to prioritise where multiple requests are lodged by one applicant. Resources were also allocated to an Administrative Appeals Tribunal (AAT) application and the History of ASIO Project during the reporting period.

Applicants dissatisfied with exemptions by ASIO can request a reconsideration of the decision. Sixteen reconsiderations were conducted in 2010–11, with the majority lodged by a major researcher and a documentary maker. In all cases, the NAA upheld the ASIO exemptions. Applicants may also lodge an appeal with the AAT regarding the exemption, or if their request is not completed within 90 days. No appeals were lodged with the AAT in 2010–11. One outstanding appeal, carried over from the previous year, was resolved in July 2010, with the AAT ruling in favour of ASIO with no additional information released.

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. In 2010–11, ASIO resolved satisfactorily one complaint concerning the appropriate storage of cinefilm and video footage, with a number of still-classified records transferred to the NAA in Sydney for storage.

Subject of Assessment	2009–10	2010–11
Percentage of folio released without exemption	61%	57%
Percentage of folios released with partial exemptions	37%	41%
Percentage of folio claimed as totally exempt	2%	2%
Percentage of folios completed within the 90 days	86%	86%
Total folio assessed	65,952	48,096

Table 4. Folios released 2009–11

All requests for ASIO archival records should be directed to the NAA. Further information is available on the NAA website, www.naa.gov.au.

Official History of ASIO

Work continued on the two-volume unclassified History of ASIO Project during 2010–11. The official historian is Professor David Horner AM of the Strategic and Defence Studies Centre, Australian National University. The project focuses on the significant internal and external influences on ASIO's formation and development as a security intelligence organisation. In 2011, the timeline for the project was extended from the original end-date of 1979 to the end of the Cold War in 1989. It is anticipated extending the end-date

will enhance the integrity of the project and provide a more logical conclusion to the second volume. An advisory committee, with both internal and external representatives, meets every six months to monitor progress of the project.

Property

New Central Office

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

CONSTRUCTION WAS PROGRESSING ON SCHEDULE FOR THE BUILDING TO BE HANDED OVER TO ASIO IN MID-2012

During 2010–11, construction of ASIO's new central office continued. The project reached its peak period of construction during the reporting period, with over 500 contractors employed on site. Progress included the erection of the glass facade and continuation of the interior fit-out. At the close of the reporting period, construction was progressing on schedule for the building to be handed over to ASIO in mid-2012, with the

main relocation of ASIO staff to commence from late 2012.

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



State and Territory Offices

In 2006, ASIO commenced a program to accommodate growth within its state and territory offices. The program was completed in 2011 and has enabled ASIO to enhance its operational capability through the establishment of flexible, multifunctional accommodation. In all cases, the accommodation projects were delivered on time and within budget.

Environmental Performance

ASIO's current premises utilise a number of energy-saving and environmentally friendly measures, including recycling of paper, cardboard, glass, toner cartridges, fluorescent light tubes, batteries and waste. During the reporting period, ASIO replaced inefficient air-cooled chillers with highly efficient water-cooled chillers — saving approximately 45 per cent in power consumption — and installed energy-efficient lighting with after-hours controls for all 24/7 areas. ASIO also utilises energy monitoring, trending and progressive finetuning to ensure that its energy use is monitored actively for peak performance.

Through its energy efficiency program, ASIO achieved savings in electrical energy of 209,237 kilowatts and \$29,021 during the reporting period — despite an increase in staff and office floor space and higher electricity supply costs, which rose an average of 10.9 per cent in 2011. ASIO also participated in the fourth consecutive annual Earth Hour event on 26 March 2011.

ASIO's new central office building is being designed to achieve a 5-star NABERS (energy) and 4.5-star (water) rating for the base building. This involves the inclusion in the design of a range of renewable energy sources and a variety of energy-efficient fittings and finishes, including:

- a gas-fired cogeneration plant, which will reduce ASIO's reliance on the electricity grid. It also produces heat as a by-product, which will be used to help heat the building;
- photovoltaic cells (solar panels) on the roof, which will reduce ASIO's reliance on mains power;
- stormwater from the roof, which will be harvested in tanks and used for landscaping irrigation;
- air conditioning designed to provide 100 per cent fresh air at floor level for a healthier work environment;
- a building frontage designed to provide optimal climate control. The western dual-glass facade has an active ventilation system with roof-level cavity venting. This vented cavity will remain open in summer to allow the heat to escape and will be closed in winter to trap the heat, providing insulation to the building; and
- glass frontage with automated external sun shades, which reduce heat gain to the work areas.

Estate and Asset Management

ASIO adheres to planned maintenance schedules to ensure its properties, plant and equipment operate at an optimal level. Following the move to the new central office, it will be some time before any of ASIO's properties are scheduled for significant refurbishment.

Asset replacement is an ongoing task and allows ASIO to ensure that assets such as furniture and fittings are replaced when they are no longer useful or economical. ASIO's relocation to the new central office in 2012 presents an opportunity for ASIO to maximise the re-use of its furniture and equipment, where possible. Current assets, including furniture and information technology assets, have been identified for relocation.

Financial Services

Purchasing

In 2010–11, ASIO continued to adhere to the Australian Government's core procurement policy framework, utilising quality procurement advice, documentation and training to ensure that value for money was achieved through competitive procurement processes where practicable.

ASIO's procurement framework underwent a review in the reporting period, with new procedures and toolkits developed to better facilitate ASIO's procurement activities, in line with the Director-General's Finance Instructions and the Commonwealth Procurement Guidelines, subject to authorised exemptions for the protection of national security.

In 2010–11, ASIO continued to invest in capability, focusing its procurement objectives on ASIO's key business areas, including technical capabilities, enhancements to information technology infrastructure and protective security.

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 2010–11, ASIO entered 13 consultancy contracts, a decrease from 16 in 2009–10. The total expenditure during the year on consultancy contracts valued at \$10,000 or more (including contracts entered into during the previous year) totalled \$2.175 million.

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 two open tenders during 2010–11. Other approaches to market were not advertised publicly for reasons of national security.

Corrections to ASIO Annual Report 2009–10

The following statements in the 2009–10 *Report to Parliament* were identified as incorrect:

- On page 137 of *ASIO's 2009–10 Report to Parliament*, in Table 6: Composition of workforce for 2005–06 to 2009–10, the figures reported for ongoing fulltime staff and non-ongoing fulltime staff are incorrect. The table below provides the correct information:

	2009–10
Ongoing full-time (excl DG)	1,460
Non-ongoing full -time ¹	40
Ongoing part-time	134
Non-ongoing part-time	18
Non-ongoing Casual	39
Total	1,691

Table 7. Composition of workforce 2005–06 to 2010–11

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



Part 6

Financial Statements

6 Financial Statements

Statement by the Director-General of Security

In my opinion, the attached financial statements for the year ended 30 June 2011 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.

A handwritten signature in blue ink that reads "David Irvine".

David Irvine
Director-General of Security

14 September 2011

6 Financial Statements



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 2011, 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; Schedule of Asset Additions; and Notes comprising a Summary of Significant Accounting Policies.

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, except where disclosures of information in the notes to, and forming part of the financial statements would or could reasonably be expected to be operationally sensitive. The Director-General of Security is also responsible for such internal control as the Director-General of Security determines is necessary, to enable the preparation of the financial statements that 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 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

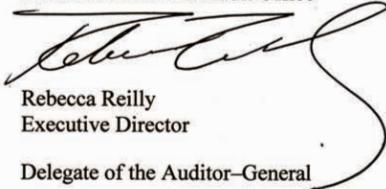
In conducting my audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

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 2011 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
14 September 2011

STATEMENT OF COMPREHENSIVE INCOME

for the period ended 30 June 2011

	Notes	2011 \$ '000	2010 \$ '000
EXPENSES			
Employee benefits	3A	186,529	178,361
Suppliers	3B	159,528	138,632
Depreciation and amortisation	3C	39,035	53,544
Finance costs	3D	328	369
Write-down and impairment of assets	3E	550	4,776
Foreign exchange losses	3F	1	2
Total Expenses		385,971	375,684
Less:			
OWN-SOURCE INCOME			
Own-source revenue			
Sale of goods and rendering of services	4A	6,044	5,913
Total Own-Source Revenue		6,044	5,913
Gains			
Net gain from sale of assets	4B	24	(131)
Other gains	4C	2,147	3,813
Total Gains		2,171	3,682
Total Own-Source Income		8,215	9,595
Net Cost of Services		377,756	366,089
Revenue from Government	4D	344,883	405,518
Surplus (deficit) attributable to the Australian Government		(32,873)	39,429
OTHER COMPREHENSIVE INCOME			
Changes in asset revaluation reserves		-	(792)
Total Comprehensive Income (loss) attributable to the Australian Government		(32,873)	38,637

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

BALANCE SHEET

as at 30 June 2011

	Notes	2011 \$ '000	2010 \$ '000
ASSETS			
Financial Assets			
Cash and cash equivalents		18,885	17,525
Trade and other receivables	5A	304,240	311,221
Other financial assets	5B	594	874
Total financial assets		323,719	329,620
Non-Financial Assets			
Land and buildings	6A,D	111,966	95,422
Infrastructure, plant and equipment	6B,D	81,466	82,338
Intangibles	6C,E	6,884	10,559
Other non-financial assets	6F	14,144	12,289
Total non-financial assets		214,460	200,609
Total Assets		538,179	530,229
LIABILITIES			
Payables			
Suppliers	7A	9,499	10,151
Other payables	7B	7,256	4,321
Total payables		16,755	14,471
Lease Liabilities			
Lease incentives	8	3,312	3,869
Total lease liabilities		3,312	3,869
Provisions			
Employee provisions	9A	45,472	41,898
Other provisions	9B	10,111	9,447
Total provisions		55,583	51,345
Total Liabilities		75,650	69,685
Net Assets		462,529	460,544
EQUITY			
Parent Equity Interest			
Contributed equity		427,045	392,187
Reserves		8,102	8,102
Retained surplus		27,382	60,255
Total Equity		462,529	460,544

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

STATEMENT OF CHANGES IN EQUITY

for the period ended 30 June 2011

	Retained Earnings		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2011	2010	2011	2010	2011	2010	2011	2010
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
Opening Balance	60,255	20,826	8,102	8,894	392,187	424,780	460,544	454,500
Comprehensive Income								
Changes in Asset Revaluation Reserves								
Asset revaluations	-	-	-	(989)	-	-	-	(989)
Restoration obligations revaluations	-	-	-	197	-	-	-	197
Surplus for the period	(32,873)	39,429	-	-	-	-	(32,873)	39,429
Total comprehensive income	(32,873)	39,429	-	(792)	-	-	(32,873)	38,637
Transactions with Owners								
Distributions to Owners								
Return of appropriation	-	-	-	-	(31,020)	(49,050)	(31,020)	(49,050)
Total distributions to owners	-	-	-	-	(31,020)	(49,050)	(31,020)	(49,050)
Contributions by Owners								
Equity injection — appropriation	-	-	-	-	61,186	16,457	61,186	16,457
Departmental capital budget	-	-	-	-	4,692	-	4,692	-
Total contributions by owners	-	-	-	-	65,878	16,457	65,878	16,457
Closing Balance attributable to the Australian Government	27,382	60,255	8,102	8,102	427,045	392,187	462,529	460,544

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

CASH FLOW STATEMENT

for the period ended 30 June 2011

	Notes	2011 \$ '000	2010 \$ '000
OPERATING ACTIVITIES			
Cash received			
Appropriations		351,409	341,406
Goods and services		7,287	5,987
Net GST received		13,196	13,112
Other cash received		5,013	4,966
Total cash received		376,905	365,472
Cash used			
Employees		180,786	171,312
Suppliers		179,073	155,724
Section 31 receipts transferred to OPA		3,606	-
Total cash used		363,465	327,037
Net cash from or (used by) operating activities	10	13,440	38,435
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		634	506
Total cash received		634	506
Cash used			
Purchase of property, plant and equipment		48,960	35,023
Purchase of intangibles		3,228	661
Total cash used		52,188	35,684
Net cash from or (used by) investing activities		(51,554)	(35,178)
FINANCING ACTIVITIES			
Cash received			
Appropriations — contributed equity		39,474	4,022
Total cash received		39,474	4,022
Net cash from or (used by) financing activities		39,474	4,022
Net increase or (decrease) in cash held		1,360	7,279
Cash and cash equivalents at the beginning of the reporting period		17,525	10,246
Cash and cash equivalents at the end of the reporting period		18,885	17,525

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

SCHEDULE OF COMMITMENTS

as at 30 June 2011

	Notes	2011 \$ '000	2010 \$ '000
BY TYPE			
Commitments receivable			
Sublease rental income		589	5,628
Net GST recoverable on commitments		11,787	11,010
Total commitments receivable		12,377	16,638
Commitments payable			
Capital commitments			
Land and buildings		130,529	158,897
Infrastructure, plant and equipment	A	2,250	638
Intangibles		-	12
Total capital commitments		132,780	159,547
Other commitments			
Operating leases	B	101,300	115,893
Other commitments		31,693	11,701
Total other commitments		132,994	127,594
Net commitments by type		253,397	270,504

Commitments are GST inclusive where relevant.

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

- A. Plant and equipment commitments are primarily contracts for purchases of 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.

Notes	2011 \$ '000	2010 \$ '000
BY MATURITY		
Commitments receivable		
Sublease rental income		
One year or less	589	1,697
From one to five years	-	3,931
Total operating lease income	589	5,628
Other commitments receivable		
One year or less	4,238	2,573
From one to five years	5,851	5,491
Over five years	1,697	2,945
Total other commitments receivable	11,787	11,010
Commitments payable		
Capital commitments		
One year or less	132,475	98,391
From one to five years	305	61,156
Total capital commitments	132,780	159,547
Operating lease commitments		
One year or less	23,174	21,025
From one to five years	59,449	62,463
Over five years	18,677	32,405
Total operating lease commitments	101,300	115,893
Other commitments		
One year or less	24,933	8,657
From one to five years	6,760	3,044
Total other commitments	31,693	11,701
Net commitments by maturity	253,397	270,504

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

SCHEDULE OF CONTINGENCIES

as at 30 June 2011

	Claims for damages or costs	
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 11: Contingent Liabilities and Assets.

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

SCHEDULE OF ASSET ADDITIONS

for the period ended 30 June 2011

Non-financial non-current assets added in 2010–11

Additions funded in the current year

By purchase — appropriation equity	-	27,782	3,787	688	32,257
By purchase — appropriation ordinary annual service	-	-	12,730	2,457	15,187
By purchase — departmental capital budget	-	182	4,429	82	4,692

Total additions funded in the current year

	-	27,964	20,946	3,227	52,136
--	---	--------	--------	-------	--------

Additions recognised in 2010–11 to be funded in future years

Restoration obligations

	-	49	-	-	49
--	---	----	---	---	----

Total additions funded in future years

	-	49	-	-	49
--	---	----	---	---	----

Total asset additions

	-	28,013	20,946	3,227	52,185
--	---	--------	--------	-------	--------

Non-financial non-current assets added in 2009–10

Additions funded in the current year

By purchase — appropriation equity	175	17,975	16,712	1,833	36,694
------------------------------------	-----	--------	--------	-------	--------

Total additions funded in the current year

	175	17,975	16,712	1,833	36,694
--	-----	--------	--------	-------	--------

Additions recognised in 2009-10 to be funded in future years

Restoration obligations

	-	175	-	-	175
--	---	-----	---	---	-----

Total additions funded in future years

	-	175	-	-	175
--	---	-----	---	---	-----

Total asset additions

	175	18,150	16,712	1,833	36,869
--	-----	--------	--------	-------	--------

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

for the year ended 30 June 2011

Note 1: Summary of Significant Accounting Policies

Note 2: Events after the Balance Sheet Date

Note 3: Expenses

Note 4: Income

Note 5: Financial Assets

Note 6: Non-Financial Assets

Note 7: Payables

Note 8: Leases

Note 9: Provisions

Note 10: Cash Flow Reconciliation

Note 11: Contingent Liabilities and Assets

Note 12: Remuneration of Auditors

Note 13: Senior Executive Remuneration

Note 14: Financial Instruments

Note 15: Appropriations

Note 16: Compensation and Debt Relief

Note 17: Reporting of Outcomes

Note 18: Restructuring

Note 19: Comprehensive Income Attributable to ASIO

Note 1: Summary of Significant Accounting Policies

1.1 Objective of ASIO

ASIO is an Australian Government-controlled 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: *Security for Australia and its interests — locally and internationally — through intelligence collection and advice that counters politically motivated violence, espionage, foreign interference, communal violence, sabotage, and attacks on the defence system.*

ASIO 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 and notes are required by section 49 of Schedule 1 of the Financial Management and Accountability Act 1997 and are general purpose financial statements. The financial statements have been prepared in accordance with the agreement between the Finance Minister and the Attorney-General. This agreement states that ASIO's financial statements must be prepared in accordance with the Finance Minister's Orders (FMOs) for reporting periods ending on or after 1 July 2010, except where the disclosure of information in the notes to the financial statements would be, or could reasonably be expected to be, operationally sensitive. Subject to the requirements of the agreement, the financial statements are prepared in accordance with:

- Finance Minister's Orders for reporting periods ending on or after 1 July 2010; 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 and 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 Judgments and Estimates

In the process of applying the accounting policies listed in this note, ASIO has made the following judgments 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 accounting period.

1.4 Changes in 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 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.

Other Types of 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 end of reporting period. Allowances are made when collectability of the debt is no longer probable.

ASIO offset amounts received under the Parental Leave Payments Scheme (for payment to employees) by amounts paid to employees under that scheme, because these transactions are only incidental to the main revenue-generating activities of ASIO.

The amount received by ASIO not yet paid to employees would be presented as cash and a liability (payable). The total amount received under this scheme is disclosed as a footnote to Note 4D Revenue from Government.

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) are recognised directly in Contributed Equity in that year.

Net Cash Appropriation Arrangements (2010)

'Net Cash Appropriation Arrangements' is a component of the Department of Finance and Deregulation's 'Operation Sunlight'.

Capital funding under Operation Sunlight involves development of Departmental Capital Budgets based on annual cash requirements for asset replacement. Cash reserves used by ASIO to fund capital requirements were returned to consolidated revenue as required.

Distributions to Owners

In 2010-11 ASIO relinquished control of appropriation funding of \$31.020m (2009-10: \$49.050m). A Finance Minister determination to reduce Departmental Appropriations is in progress.

1.8 Employee Benefits

Liabilities for 'short-term employee benefits' (as defined in AASB 119 Employee Benefits) and termination benefits due within twelve months of 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.

All 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.

The liability for long service leave has been determined by reference to the work of an actuary as at 30 June 2010. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

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 is a defined contribution scheme.

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 as an administered item.

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

The liability for superannuation recognised 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 Borrowing Costs

All borrowing costs are expensed as incurred.

1.11 Cash

Cash and cash equivalents means notes and coins held and any 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. Cash is recognised at its nominal amount.

1.12 Financial Assets

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

The classification depends on the nature and purpose of the financial assets and is determined at the time of initial recognition.

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.

Income is recognised on an effective interest rate basis except for financial assets at fair value through profit or loss.

Loans and Receivables

Trade receivables, loans 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 amortised cost — if there is objective evidence that an impairment loss has been incurred for loans and receivables or held to maturity investments held at amortised cost, the amount of the loss is measured as the difference between the asset's carrying amount and the present value of estimated future cash flows discounted at the asset's original effective interest rate. The carrying amount is reduced by way of an allowance account. The loss is recognised in the Statement of Comprehensive Income.

Financial assets held at cost - if there is objective evidence that an impairment loss has been incurred, the amount of the impairment loss is the difference between the carrying amount of the asset and the present value of the estimated future cash flows discounted at the current market rate for similar assets.

1.13 Financial Liabilities

ASIO classifies its financial liabilities 'at fair value through profit or loss' or other financial liabilities.

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

Financial Liabilities at Fair Value through Profit or Loss

Financial liabilities at fair value through profit or loss are initially measured at fair value. Subsequent fair value adjustments are recognised in profit or loss. The net gain or loss recognised in profit or loss incorporates any interest paid on the financial liability.

Other Financial Liabilities

Other financial liabilities, including borrowings, 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).

1.14 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.

1.15 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.

1.16 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 'makegood' 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 'makegood' recognised.

Revaluations

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

<i>Asset Class</i>	<i>Fair value measured at:</i>
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:

	2011	2010
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 2011. 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.

1.17 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 (2009–10: 4–5 years).

All software assets were assessed for indications of impairment as at 30 June 2011.

1.18 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

There were no events occurring after reporting date which had an effect on the 2011 financial statements (2010: Nil).

	2011 \$ '000	2010 \$ '000
Note 3: Expenses		
Note 3A: Employee Benefits		
Wages and salaries	143,365	137,269
Superannuation:		
Defined contribution plans	10,001	8,819
Defined benefit plans	17,574	18,165
Leave and other entitlements	14,552	11,889
Separation and redundancies	1,037	2,219
Total employee benefits	186,529	178,361

Note 3B: Suppliers

Provision of goods — related entities	1,160	1,038
Provision of goods — external entities	7,833	8,439
Rendering of services — related entities	31,372	28,094
Rendering of services — external entities	95,412	78,964
Operating lease rentals — related entities:		
minimum lease payments	3,468	3,626
Operating lease rentals — external entities:		
minimum lease payments	18,540	16,913
Workers' compensation premiums	1,743	1,558
Total supplier expenses	159,528	138,632

	2011 \$ '000	2010 \$ '000
Note 3C: Depreciation and amortisation		
Depreciation		
Infrastructure, plant and equipment	21,124	30,549
Buildings	11,071	11,737
Total depreciation	32,195	42,286
Amortisation — Intangibles — computer software	6,840	11,258
Total depreciation and amortisation	39,035	53,544

Note 3D: Finance costs

Unwinding of discount — restoration obligations	328	369
---	------------	-----

Note 3E: Write-down and impairment of assets

Asset write-downs from:

Impairment of receivables	4	2
Write-down of land and buildings	325	184
Write-down of property, plant and equipment	158	4,469
Write-down of intangible assets	63	121
Total write-down and impairment of assets	550	4,776

Note 3F: Foreign Exchange Losses

Non-speculative	1	2
-----------------	----------	---

Note 4: Income**Own-Source Revenue****Note 4A: Sale of Goods and Rendering of Services**

Provision of goods — related entities	15	31
Provision of goods — external entities	145	35
Rendering of services — related entities	5,653	3,704
Rendering of services — external entities	230	2,142
Total sale of goods and rendering of services	6,044	5,913

	2011 \$ '000	2010 \$ '000
Note 4B: Net Gain from Asset Sales		
Infrastructure, plant and equipment		
Proceeds from sale	634	506
Carrying value of assets sold	(610)	(667)
Intangibles		
Proceeds from sale	-	30
Total gain from asset sales	24	(131)

Note 4C: Gains

Resources received free of charge	110	100
Rent	1,570	1,515
Other	467	2,198
Total gains	2,147	3,813

Note 4D: Revenue from Government

Appropriation — Departmental appropriations	344,883	405,518
---	---------	---------

ASIO received \$18,240 (2010: Nil) under the Paid Parental Leave Scheme. These amounts were offset against the amounts paid to employees in the Statement of Comprehensive Income.

Note 5: Financial Assets

Note 5A: Trade and other Receivables

Goods and services		
Related entities	2,908	2,927
External entities	115	138
Total receivables for goods and services	3,023	3,065
Appropriations Receivable for existing programs	298,738	306,273
GST receivable from the Australian Taxation Office	2,479	1,882
Total trade and other receivables (gross)	304,240	311,220
Less impairment allowance account:	-	-
Total trade and other receivables (net)	304,240	311,220

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

	2011 \$ '000	2010 \$ '000
Receivables are aged as follows:		
Not overdue	303,911	310,801
Overdue by:		
less than 30 days	150	180
30 to 60 days	102	90
61 to 90 days	9	29
more than 90 days	68	120
Total receivables (gross)	304,240	311,220

	Goods & Services	Goods & Services
Reconciliation of the Impairment Allowance Account		
Opening balance	-	1
amounts written off	-	(1)
Closing balance	-	-

Note 5B: Other financial assets

Accrued Revenue	594	874
-----------------	------------	-----

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	7,653	7,653
accumulated depreciation	(530)	(105)
Total buildings on freehold land	7,123	7,548
Leasehold improvements		
work in progress	40,472	17,562
fair value	75,910	71,267
accumulated depreciation	(13,054)	(2,470)
Total leasehold improvements	103,328	86,359
Total land and buildings (non-current)	111,966	95,422

No indicators of impairment were found for land and buildings.

No land or buildings are expected to be sold or disposed of within the next 12 months.

	2011	2010
	\$ '000	\$ '000
Note 6B: Infrastructure, Plant and Equipment		
Infrastructure, plant and equipment		
work in progress	96	756
fair value	106,917	87,137
accumulated depreciation	(25,547)	(5,555)
Total Infrastructure, plant and equipment (non-current)	81,466	82,338

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

Amounts charged to the asset revaluation reserve in the equity section of the balance sheet:

Infrastructure, plant and equipment	-	(989)
-------------------------------------	---	-------

Note 6C: Intangibles

Computer software		
purchased — at cost	13,602	17,884
internally developed — in progress	165	194
internally developed — in use	14,799	20,807
accumulated amortisation	(20,557)	(27,202)
accumulated impairment	(1,125)	(1,125)
Total computer software	6,884	10,559
Total intangibles (non-current)	6,884	10,559

No indicators of impairment were found for intangibles.

No intangibles are expected to be sold or disposed of in the next 12 months.

Note 6D: Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment (2010–11)

	Land \$'000	Buildings \$'000	Buildings— Leasehold Improvement \$'000	Infrastructure, Plant & Equipment \$'000	Total \$'000
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	7,124	103,328	81,465	193,431
Net book value as at 30 June 2011 represented					
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

* Disaggregated additions information is disclosed in the Schedule of Asset Additions.

Reconciliation of the Opening and Closing Balances of Property, Plant and Equipment (2009–10)

	Land \$'000	Buildings \$'000	Buildings– Leasehold Improvement \$'000	Infrastructure Plant & Equipment \$'000	Total \$'000
As at 1 July 2009					
Gross book value	1,385	8,593	99,613	151,157	260,748
Accumulated depreciation and impairment	-	(676)	(19,897)	(48,840)	(69,413)
Net book value 1 July 2009	1,385	7,917	79,717	102,317	191,335
Additions by purchase*	-	175	18,149	16,712	35,036
Reclassifications	130	(61)	(69)	(989)	(989)
Depreciation expense	-	(483)	(11,254)	(30,549)	(42,287)
Disposals	-	-	(184)	(5,151)	(5,336)
Net book value 30 June 2010	1,515	7,548	86,359	82,338	177,760
Net book value as at 30 June 2010 represented					
Gross book value	1,515	7,653	88,828	87,893	185,889
Accumulated depreciation and impairment	-	(105)	(2,470)	(5,555)	(8,130)
	1,515	7,548	86,359	82,338	177,760

* Disaggregated additions information is disclosed in the Schedule of Asset Additions.

Note 6E: Reconciliation of the Opening and Closing Balances of Intangibles (2010–11)

	Computer software		Total \$'000
	Internally developed \$'000	Purchased \$'000	
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	3,226
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

Reconciliation of the Opening and Closing Balances of Intangibles (2009–10)

	Computer software		Total \$'000
	Internally developed \$'000	Purchased \$'000	
As at 1 July 2009			
Gross book value	24,095	14,961	39,056
Accumulated amortisation and impairment	(11,778)	(6,032)	(17,809)
Net book value 1 July 2009	12,317	8,929	21,247
Adjustment to Gross book value ¹	(542)	542	-
Adjusted Net book value 1 July 2009	11,775	9,471	21,247
Additions by purchase or internally developed	-	849	849
Reclassification	985	-	985
Amortisation expense	(6,417)	(4,841)	(11,258)
Disposals - Other	(1,157)	(106)	(1,263)
Net book value 30 June 2010	5,186	5,373	10,559
Net book value as at 30 June 2010 represented by:			
Gross book value	21,002	17,884	38,886
Accumulated amortisation and impairment	(15,816)	(12,511)	(28,327)
	5,186	5,373	10,559

1. The opening balance classification between internally developed and purchased software was revised based on a review of intangibles undertaken in 2009–10.

	2011 \$ '000	2010 \$ '000
Note 6F: Other non-financial assets		
Prepayments	12,585	12,289
Other debtors	1,559	-
Total Other non-financial assets	14,144	12,289

Total other non-financial assets are expected to be recovered in:

No more than 12 months	13,908	12,289
More than 12 months	236	-
	14,144	12,289

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

Note 7: Payables

Note 7A: Suppliers

Trade creditors and accruals	9,499	10,151
------------------------------	-------	--------

Supplier payables expected to be settled within 12 months:

Related entities	141	1,398
External entities	9,358	8,753
	9,499	10,151

Settlement is usually made within 30 days.

Note 7B: Other payables

Salaries and wages	3,955	3,172
Superannuation	1,845	459
Unearned income	791	8
Fringe Benefits Tax	665	682
Total other payables	7,256	4,321

All other payables are expected to be settled in no more than 12 months.

Note 8: Leases

Lease incentives	3,312	3,869
------------------	-------	-------

Lease incentives are expected to be settled in:

No more than 12 months	577	535
More than 12 months	2,735	3,334
	3,312	3,869

	2011	2010
Note 9: Provisions	\$ '000	\$ '000

Note 9A: Employee provisions

Leave	44,360	39,683
Redundancies	-	963
Superannuation	1,112	1,252
Total employee provisions	45,472	41,898

Employee provisions are expected to be settled in:

No more than 12 months	30,522	27,138
More than 12 months	14,950	14,760
	45,472	41,898

Note 9B: Other provisions

Restoration obligations	7,105	6,797
Rent payable	3,006	2,345
Reorganisation costs	-	305
Total other provisions	10,111	9,447

Other provisions are expected to be settled in:

No more than 12 months	3,023	2,345
More than 12 months	7,088	7,102
	10,111	9,447

	Restoration Obligations	Rent Payable	Total
	\$'000	\$'000	\$'000
Carrying amount 1 July 2010	6,797	2,345	9,142
Additional provisions made	49	661	710
Lease expiry	(69)	-	(69)
Unwinding of discount or change in discount rate	328	-	328
Closing balance	7,105	3,006	10,111

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.

	2011	2010
	\$ '000	\$ '000

Note 10: Cash Flow Reconciliation

Reconciliation of cash and cash equivalents per Balance Sheet to Cash Flow

Report cash and cash equivalents as per:

Cash Flow Statement	18,885	17,525
Balance Sheet	18,885	17,525

Reconciliation of net cost of services to net cash from operating activities:

Net cost of services	(377,756)	(366,089)
Add revenue from government	344,883	405,518

Adjustments for non-cash items

Depreciation/amortisation	39,035	53,544
Net write-down of non-financial assets	546	4,774
Net write-down of other provisions	-	197
Net gain on disposal of assets	(24)	131

Changes in assets/liabilities

(Increase)/decrease in receivables	2,368	(64,548)
(Increase)/decrease in accrued revenue	280	187
(Increase)/decrease in prepayments	(1,855)	(35)
Increase/(decrease) in employee provisions	3,574	6,313
Increase/(decrease) in other provisions	664	1,683
Increase/(decrease) in lease incentives	(557)	(120)
Increase/(decrease) in supplier payables	(653)	(3,522)
Increase/(decrease) in accrued expenses	2,935	403

Net cash from/(used by) operating activities	13,440	38,435
---	---------------	---------------

Note 11: Contingent Liabilities and Assets

Quantifiable contingencies

The Schedule of Contingencies reports no contingent liabilities in respect of claims for damages/costs. (2010: Nil)

Unquantifiable contingencies

At 30 June 2011, 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. (2010: Nil)

Remote contingencies

ASIO does not have any remote contingencies.

Note 12: 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.

	2011	2010
Fair value	110,000	100,000

Note 13: Senior Executive Remuneration

Note 13A: Senior Executive Expense for the Reporting Period 2011 2010

Short-term employee benefits:

Salary	9,075,386	9,005,188
Annual leave accrued	740,328	779,715
Performance bonuses	452,267	484,144
Motor vehicle and other allowances	869,316	775,342
Total short-term employee benefits	11,137,297	11,044,389

Post-employment benefits

Superannuation	1,891,179	2,118,351
Total post-employment benefits	1,891,179	2,118,351

Other long-term benefits

Long-service leave accrued	241,378	254,220
Total other long-term benefits	241,378	254,220

Termination benefits

	1,206,447	329,636
Total	14,476,301	13,746,596

Note 13A excludes acting arrangements and part-year services where remuneration expensed is less than \$150,000.

Note 13B: Average Annual Remuneration Packages and Bonuses for Substantive Senior Executives as at the end of the Reporting Period

Fixed Elements and Bonus	Senior Executives No.	as at 30 June 2011			Bonus paid \$
		Fixed elements			
		Salary \$	Allowances \$	Total \$	
Total remuneration:					
\$150 000 to \$179 999	38	162,462	12,185	174,647	7,747
\$180 000 to \$209 999	2	170,331	12,775	183,106	11,345
\$210 000 to \$239 999	13	202,283	15,171	217,454	14,091
\$240 000 to \$269 999	1	245,852	18,439	264,291	4,827
\$360 000 to \$389 999	-	-	-	-	-
\$390 000 to \$419 999	1	386,220	-	386,220	-
Total	55				

This table reports substantive senior executives who were employed by ASIO at the end of the reporting period. Fixed elements were based on the employment agreement of each individual. Each row represents an average annual figure (based on headcount) for the individuals in that remuneration package band. 'Bonus paid' represents average actual bonuses earned for the reporting period in that remuneration package band. Bonuses were paid after year end, however are shown in the year they relate to so remuneration for that year is represented accurately. Performance bonuses have been abolished from 1 July 2011. The 'Bonus paid' was excluded from the 'Total' calculation for the purpose of determining remuneration package bands.

as at 30 June 2010

Fixed Elements and Bonus	Senior Executives No.	Fixed elements			Bonus paid \$
		Salary \$	Allowances \$	Total \$	
Total remuneration:					
\$150 000 to \$179 999	38	147,693	7,385	155,078	8,628
\$180 000 to \$209 999	13	180,752	9,038	189,790	10,845
\$210 000 to \$239 999	2	201,175	10,059	211,234	12,071
\$240 000 to \$269 999	-	-	-	-	-
\$360 000 to \$389 999	1	360,678	-	360,678	-
\$390 000 to \$419 999	-	-	-	-	-
Total	54				

Variable elements

With the exception of bonuses, variable elements are not included in the 'Fixed Elements and Bonus Paid' table above. The following variable elements were available as part of the senior executives' remuneration package:

- Bonuses which are based on the performance rating of each individual. The maximum bonus an individual could receive is 9% (2010: 6%) of base salary.
- Senior executives were entitled to the following leave entitlements per year in 2010 and 2011 (pro-rata for part-time):
 - Annual Leave — 20 days
 - Personal Leave — 20 days
 - Long Service Leave — in accordance with the Long Service Leave (Commonwealth Employees) Act 1976
- Senior executives were members of one of the following superannuation funds:
 - Commonwealth Superannuation Scheme (CSS): this scheme is closed to new members and employer contributions were 26.1% (2010: 24.8%), including productivity component.
 - Public Sector Superannuation Scheme (PSS): this scheme is closed to new members and employer contributions were 19.1% (2010: 16.5%), including productivity component.
 - Public Sector Superannuation Accumulation Plan (PSSap): the fund has been in operation since July 2005 and contributions were 15.4% (2010: 15.4%).
 - Australian Government Employee Superannuation Trust (AGEST): employer contributions were 15.4% (2010: 15.4%).
 - Other: some senior executives have their own superannuation arrangements. Employer contributions were 15.4% (2010: 15.4%).
- Senior executives are provided with a fully maintained and fuelled vehicle (including parking at the workplace and applicable fringe benefits tax).
- Senior executives are paid a rental allowance when based outside Canberra.
- Salary-sacrifice arrangements are available to senior executives, including superannuation and motor vehicle fringe benefits.

Note 13C: Other highly paid staff

During the reporting period there were 4 employees (2010: 3 employees) whose salary plus higher duties and associated allowances was \$150,000 or more.

	2011	2010
Note 14: Financial Instruments	\$'000	\$'000

Note 14A: Categories of Financial Instruments**Financial Assets**

Loans and receivables		
Cash and cash equivalents	18,885	17,525
Trade receivables	3,023	3,065
Accrued revenue	594	874
Carrying amount of financial assets	22,502	21,465

Financial Liabilities

At amortised cost		
Trade creditors and accruals	9,499	10,151
Carrying amount of financial liabilities	9,499	10,151

Note 14B: 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 2011 (2010: Nil). The total expense from financial assets through the profit and loss for the period ending 30 June 2011 was \$4,246 (2010: \$2,315).

Note 14C: 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 2011 (2010: Nil).

Note 14D: Fair Value of Financial Instruments

	2011 \$'000	2011 \$'000	2010 \$'000	2010 \$'000
	Carrying amount	Fair value	Carrying amount	Fair value
Financial Assets				
Loans and Receivables				
Cash and cash equivalents	18,885	18,885	17,525	17,525
Trade receivables (net)	3,023	3,023	3,065	3,065
Accrued revenue	594	594	874	874
Total	22,502	22,502	21,464	21,465
Financial Liabilities				
At amortised cost				
Trade creditors and accruals	9,499	9,499	10,151	10,151

Note 14E: 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.

	2011 \$'000	2010 \$'000
Financial Assets		
Loans and receivables		
Cash and cash equivalents	18,885	17,525
Trade receivables	3,023	3,065
Accrued revenue	594	874
Total Financial Assets	22,502	21,465

Financial Liabilities

At amortised cost

Trade creditors and accruals	9,499	10,151
------------------------------	-------	--------

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

	2011 \$'000	2010 \$'000	2011 \$'000	2010 \$'000
	Not past due nor impaired		Past due or impaired	
Loans and receivables				
Cash and cash equivalents ¹	18,885	17,525	-	-
Trade receivables ²	2,694	2,646	329	419
Accrued revenue ³	594	874	-	-
Total Loans and Receivables	22,173	21,045	329	419

¹ Cash and cash equivalents are 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 for 2011

	0 to 30 days \$'000	31 to 60 days \$'000	61 to 90 days \$'000	90+ days \$'000	Total \$'000
Loans and receivables					
Trade and other receivables	150	102	9	68	329

Ageing of financial assets that are past due but not impaired for 2010

	0 to 30 days \$'000	31 to 60 days \$'000	61 to 90 days \$'000	90+ days \$'000	Total \$'000
Loans and receivables					
Trade and other receivables	180	90	29	120	419

Note 14F: 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 2009–10.

The following table illustrates the maturities for financial liabilities.

	2011 \$'000	2011 \$'000	2011 \$'000	2011 \$'000	2011 \$'000
	On demand	within 1 year	1 to 5 years	> 5 years	Total
At amortised cost					
Trade creditors and accruals	-	9,499	-	-	9,499
	2010 \$'000	2010 \$'000	2010 \$'000	2010 \$'000	2010 \$'000
	On demand	within 1 year	1 to 5 years	> 5 years	Total
At amortised cost					
Trade creditors and accruals	-	10,151	-	-	10,151

Note 14G: 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 2009–10. ASIO is not exposed to 'Currency risk', 'Other price risk' or 'Interest rate risk'.

Note 15: Appropriations

Note 15A: Annual Appropriations

	Appropriation Act		FMA Act			Total Appropriation applied \$ '000	Variance \$ '000
	Annual Appropriation \$ '000	Appropriations reduced \$ '000	Section 30 \$ '000	Section 31 (GST excl.) \$ '000	Section 32 \$ '000		
2011							
Departmental							
Ordinary annual services	373,447	(23,552) ¹	2,756	12,934	(320) ²	365,265	(18,097)
Other services							
Equity	61,186		-	-	-	61,186	28,947
Total Departmental	434,633	(23,552)	2,756	12,934	(320)	426,451	10,850
2010							
Departmental							
Ordinary annual services	408,518		1,253	11,459	-	421,230	45,144
Return of appropriation	-	(49,050) ³	-	-	-	(49,050)	
Other services							
Equity	16,457		-	-	-	16,457	(20,237)
Total Departmental	424,975	(49,050)	1,253	11,459	-	388,637	24,907

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

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

3. Net Cash arrangements

Note 15B: Unspent Departmental Annual Appropriations

	2011	2010
	\$ '000	\$ '000
Appropriation Act (No.1) 2010–11	268,924	-
Appropriation Act (No.2) 2010–11	48,699	-
Appropriation Act (No.1) 2009–10 *	-	295,743
Appropriation Act (No.2) 2009–10 *	-	16,035
Appropriation Act (No.2) 2008–09	-	12,020
Total	317,623	323,798

* Includes \$31.020m appropriations returned to Government.

Note 15C: Disclosure by Agent in relation to Annual Appropriations

	2011		2010	
	DoFD	DFAT	DoFD	DFAT
	\$ '000	\$ '000	\$ '000	\$ '000
Total payments	28,782	11,065	4,413	10,708

Note 16: Compensation and Debt Relief

No payments were made during the reporting period under the 'Defective Administration Scheme' (2010: NIL).

Note 17: Reporting of Outcomes

	2011	2010
	\$ '000	\$ '000
Expenses		
Departmental	385,971	375,815
Income from non-government sector		
Departmental		
Activities subject to cost recovery	(376)	(2,177)
Other	(491)	(2,198)
	(867)	(4,375)
Other own-source income		
Departmental	(7,348)	(5,350)
Net cost of outcome delivery	377,757	366,090

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

Note 18: 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 19: Comprehensive Income Attributable to ASIO	2011 \$ '000	2010 \$ '000
Total comprehensive income (loss)*	(32,873)	38,637
Non-appropriated expenses		
Depreciation and amortisation	39,035	53,544
<i>Total comprehensive income attributable to ASIO</i>	6,162	92,181

* as per the Statement of Comprehensive Income

6 Financial Statements



Part 7

Appendices & Indices

Appendix A: Agency Resource Statement 2010–11

	Actual Available Appropriations for 2010–11 \$'000	Payments Made 2010–11 \$'000	Balance Remaining \$'000
Ordinary Annual Services			
Departmental appropriation			
Prior year departmental appropriation	278,218	278,218	0
Departmental appropriation	344,883	94,844	250,039
S.31 Relevant agency receipts	3,400	6,044	-2,644
Total	626,501	379,106	247,395
Departmental non-operating			
Prior year equity injections	28,055	28,055	0
Equity Injections	61,186	12,487	48,699
Departmental Capital Budget	4,692	10,022	-5,330
Total	93,933	50,564	43,369
Total Resourcing and Payments	720,434	429,670	290,764

Appendix B: Expenses and Resources Table 2010–11

Outcome 1: Security for Australia and its interests — locally and internationally — through intelligence collection and advice that counters politically motivated violence, espionage, foreign interference, communal violence, sabotage, and attacks on the defence system.

	Budget 2010–11 \$'000	Actual Expenses 2010–11 \$'000	Variation 2010–11 \$'000
Program 1.1: Security Intelligence			
Departmental expenses			
Ordinary annual services (Appropriation Bill No.1)	344,883	346,321	-1,438
Revenues from independent sources (Section 31)	3,400	6,044	-2,644
Expenses not requiring appropriation in the Budget year	64,213	39,145	25,068
Total expenses for Outcome 1	412,496	391,510	20,986
	2009–10	2010–11	
Average staffing levels (number)	1,692	1,769	77

Appendix C: List of Proscribed Terrorist Organisations (30 June 2011)

Group	Initial listing	Date last relisted
Al-Shabaab	22 Aug 2009	
Al-Qa'ida	21 Oct 2002	19 Jul 2010
Jemaah Islamiyah	27 Oct 2002	19 Jul 2010
Abu Sayyaf Group (ASG)	14 Nov 2002	28 Oct 2010
Jamiat ul-Ansar (JuA)	14 Nov 2002	28 Oct 2010
Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) formerly known as the Salafist Group for Call and Combat (GSPC)	14 Nov 2002	19 Jul 2010
Ansar al-Islam (formerly known as Ansar al-Sunna)	27 Mar 2003	17 Mar 2009
Asbat al-Ansar (AAA)	11 Apr 2003	17 Mar 2009
Islamic Army of Aden (IAA)	11 Apr 2003	17 Mar 2009
Islamic Movement of Uzbekistan (IMU)	11 Apr 2003	17 Mar 2009
Jaish-e-Mohammed (JeM)	11 Apr 2003	17 Mar 2009
Lashkar-e Jhangvi (LeJ)	11 Apr 2003	17 Mar 2009
Hizballah's External Security Organisation (ESO)	5 Jun 2003	15 May 2009
Lashkar-e-Tayyiba (LeT)	9 Nov 2003	8 Sep 2009
Hamas' Izz al-Din al-Qassam Brigades	9 Nov 2003	8 Sep 2009
Palestinian Islamic Jihad (PIJ)	3 May 2004	8 Sep 2009
Al-Qa'ida in Iraq (AQI)	2 Mar 2005	28 Oct 2010
Kurdistan Workers Party (PKK)	17 Dec 2005	8 Sep 2009
Al-Qa'ida in the Arabian Peninsula (AQAP)	19 Jul 2010	

Appendix D: Mandatory Reporting Requirements 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

Table 5. Mandatory reporting requirements under section 94 of the *Australian Security Intelligence Organisation Act 1979*

Appendix E: Workforce Statistics

	2005–06	2006–07	2007–08	2008–09	2009–10	2010–11
Ongoing full-time (excl. DG)	800	1,125	1,263	1,452	1,460	1,512
Non-ongoing full-time ¹	178	55	52	49	40*	50
Ongoing part-time	50	94	108	116	134	148
Non-ongoing part-time	27	18	12	19	18	16
Non-ongoing casual	55	64	57	54	39	43
	1,110	1,356	1,492	1,690	1,691	1,769

Table 6. Composition of workforce 2005–06 to 2010–11

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

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

Table 7. SES equivalent classification and gender 2006-07 to 2010-11 (does not include the Director-General of Security)

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

Table 8. Representation of designated groups within ASIO at 30 June 2011

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

Group	2005–06	2006–07	2007–08	2008–09	2009–10	2010–11
Women ¹	45.9	45.5	45.4	44.6	44.3	44.3
Non-English Speaking Background	4.5	5.6	4.4	5.6	6.9	6.0
Aboriginal and Torres Strait Islander	0.4	0.3	0.3	0.2	0.2	0.3
People with a Disability	1.4	1.2	1.4	1.4	1.2	1.2

Table 9. Percentage of representation of designated groups in ASIO 2005–06 to 2010–11

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

ASIO Managers			
SES Band 3	\$201,175		minimum point
SES Band 2	\$159,009		minimum point
SES Band 1	\$133,365		minimum point
AE03	\$115,881		
AE02	\$105,126	to	\$115,881
AE01	\$92,697	to	\$105,126
Intelligence Officers			
IO	\$70,782	to	\$80,736
ASIO Officers			
ASIO Officer 5	\$70,782	to	\$80,736
ASIO Officer 4	\$58,377	to	\$65,616
ASIO Officer 3	\$50,908	to	\$56,236
ASIO Officer 2	\$44,830	to	\$49,590
ASIO Officer 1	\$39,736	to	\$43,802
ASIO ITOs			
SITOA	\$115,881		\$115,881
SITOB	\$105,126	to	\$115,881
SITOC	\$92,697	to	\$100,059
ITO2	\$70,782	to	\$80,736
ITO1	\$54,854	to	\$63,724
ASIO Engineers			
SIO(E)5	\$117,721		
SIO(E)4	\$105,126	to	\$115,881
SIO(E)3	\$92,697	to	\$100,059
SIO(E)2	\$70,782	to	\$80,736
SIO(E)1	\$54,854	to	\$63,724

Table 10. ASIO Salary Classification at 30 June 2011

Compliance Index

Part of Report	Description	Requirement	Page
	Letter of transmittal	Mandatory	III
	Table of contents	Mandatory	v
	Index	Mandatory	171
	Glossary	Mandatory	169
	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	XII–XXI
	Overview of department's performance and financial results	Suggested	XII–XXI
	Outlook for following year	Suggested	3
	Significant issues and developments – portfolio	Portfolio departments - suggested	Not applicable
Departmental overview			
	Role and functions	Mandatory	XII
	Organisational structure	Mandatory	XIV
	Outcome and program structure	Mandatory	XVII
	Where outcome and program structures differ from PBS/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	Mandatory for portfolio departments	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 PBS/PAES or other portfolio statements	Mandatory	Part 2	
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	
Performance of purchaser/provider arrangements	If applicable, suggested	Not applicable	
Significant changes in nature of principal functions/services	Suggested	Not applicable	
Factors, events or trends influencing departmental performance	Suggested	Part 1	
Contribution of risk management in achieving objectives	Suggested	99	
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	64, 93	
Discussion and analysis of the department's financial performance	Mandatory	XVII	
Discussion of any significant changes from the prior year or from budget	Suggested	Not applicable	
Agency resource statement and summary resource tables by outcomes	Mandatory	XVII, 155	
Developments since the end of the financial year that have affected or may significantly affect the department's operations or financial results in future	If applicable, mandatory	Not applicable	

Management Accountability			
Corporate Governance			
Agency heads are required to certify that their agency complies with the Commonwealth Fraud Control Guidelines	Mandatory	III	
Statement of the main corporate governance practices in place	Mandatory	94–96	
Names of the senior executive and their responsibilities	Suggested	–	
Senior management committees and their roles	Suggested	94–96	
Corporate and operational planning and associated performance reporting and review	Suggested	100	
Approach adopted to identifying areas of significant financial or operational risk	Suggested	98	
Policy and practices on the establishment and maintenance of appropriate ethical standards	Suggested	69–70	
How nature and amount of remuneration for SES officers is determined	Suggested	94	
External Scrutiny			
Significant developments in external scrutiny	Mandatory	61–65	
Judicial decisions and decisions of administrative tribunals	Mandatory	30–32, 104–105	
Reports by the Auditor-General, a Parliamentary Committee or the Commonwealth Ombudsman	Mandatory	Not applicable	
Management of Human Resources			
Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	Mandatory	82–89	

Workforce planning, staff turnover and retention	Suggested	89–90
Impact and features of enterprise of collective agreements, individual flexibility arrangements (IFAs), determinations, common law contracts and AWAs	Suggested	94
Training and development undertaken and its impact	Suggested	86–89
Occupational health and safety performance	Suggested	92–93
Productivity gains	Suggested	-
Statistics on staffing	Mandatory	Appendix E
Enterprise or collective agreements, IFAs, determinations, common law contracts and AWAs	Mandatory	94
Performance pay	Mandatory	94
Assessment of effectiveness of assets management	If applicable, mandatory	109
Assessment of purchasing against core policies and principles	Mandatory	109
The annual report must include a summary statement detailing the number of new consultancy services contracts let during the year; the total actual expenditure (inclusive of GST); the number of going 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	109–110
Absence of provisions in contracts allowing access by the Auditor-General	Mandatory	Not applicable
Contracts exempt from the AusTender	Mandatory	110
Financial statements	Mandatory	Part 6

Other Mandatory Information		
Occupational health and safety (section 7a of the Occupational Health and Safety Act 1991)	Mandatory	92–93
Freedom of information for the period 1 July 2010 to 30 April 2011 inclusive	Mandatory	103–105
Advertising and market research (Section 311A of the Commonwealth Electoral Act 1918) and statement on advertising campaigns	Mandatory	84
Ecologically sustainable development and environmental performance (Section 516A of the Environment Protection and Biodiversity Conservation Act 1999)	Mandatory	108
Grant programs	Mandatory	Not applicable
Disability reporting - explicit and transparent reference to agency-level information available through other reporting mechanisms	Mandatory	161, 162
Correction of material errors in previous annual report	If applicable, mandatory	110
List of Requirements	Mandatory	164-168

Glossary

AAT	Administrative Appeals Tribunal
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
AIC	Australian Intelligence Community
ANAO	Australian National Audit Office
ANSTO	Australian Nuclear Science and Technology Organisation
APEC	Asia Pacific Economic Forum
AQAP	Al-Qa'ida in the Arabian Peninsula
APS	Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASIC	Aviation Security Identification Card
ASIS	Australian Secret Intelligence Service
AGD	Attorney-General's Department
AUSTRAC	Australian Transaction Reports and Analysis Centre
BLU	Business Liaison Unit
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive (weaponry)
CDPP	Commonwealth Director of Public Prosecutions
CHOGM	Commonwealth Heads of Government Meeting
CTCC	Counter Terrorism Control Centre
CTRC	Commonwealth Technical Response Capability
CTITP	Counter-Terrorism Intelligence Training Program

DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DSD	Defence Signals Directorate
FTE	Full-Time Equivalent
IGIS	Inspector-General of Intelligence and Security
IMA	Irregular Maritime Arrival
JCTT	Joint Counter-Terrorism Team
MSIC	Maritime Security Identification Card
NAA	National Archives of Australia
NCTC	National Counter-Terrorism Committee
NIPs	National Intelligence Priorities
NiTAC	National Interception Technical Assistance Centre
NSC	National Security Committee of Cabinet
NSH	National Security Hotline
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
SCNS	Secretaries Committee on National Security
SES	Senior Executive Service
SFLO	Staff and Family Liaison Office
T4	ASIO's T4 Protective Security Directorate

Index

A

academia 72, 77, 86, 88
accommodation 107, 121
accountability XIX, XIII, 57-78, 96
Administrative Appeals Tribunal (AAT)
31, 104, 169
advertising 84, 168
Afghanistan 4, 6, 39
Africa XIV, 4, 6, 18, 46, 169
al-Aulaqi, Anwar 6
al-Qa'ida XIII, 5, 20, 157
al-Qa'ida in the Arabian Peninsula
(AQAP) 157, 169,
al-Shabaab 157
ammonium nitrate 29
analysis XV, XVII, 13
 complex technical and tactical XVI
 intelligence XVII, 13, 83, 98
 investigative XIV, XVI, 21
 strategic XIV, 13, 86
Ansar al-Islam 157
ASIO Act
 see legislation
ASIO website 73, 75, 92, 97
Assessments
 see also Threat Assessments
 see also Security Assessments
asset management 109
assumed identities 69
Attorney-General III, 20, 37, 40, 44, 59, 60,
64, 76, 125
Attorney-General's Department 14, 17, 85,
169
Attorney-General's Guidelines XII, 46, 59,
60
audit XIV, 21, 45, 59-60, 67, 69-71, 96, 124,
143, 166, 169
Australian Crime Commission (ACC) 169
Australian Customs and Border Protection
Service (ACBPS) 21, 85, 169
Australian Federal Police (AFP) 15, 18, 39,

85, 169

see also police

Australian Government Solicitor 20, 85
Australian National Audit Office (ANAO) 21,
67, 96, 115-116, 143, 169,
Australian Nuclear Science and Technology
Organisation (ANSTO) 24, 29, 169
Australian Secret Intelligence Service
(ASIS) XVI, 15, 39, 61, 86, 169
*Australian Security Intelligence
Organisation Act 1979*
 see legislation
Aviation Security Identification Cards
(ASICs) 29
 see also Security Assessments

B

Ba'asyir, Abu Bakar XII, 5
Bin Laden, Usama VII-XI, XIX, 5, 14, 20
border integrity XII, XIX, 3, 42
Business Liaison Unit (BLU) 15, 16, 169

C

Central office (ASIO) IX, XXI, 62, 94,
101, 106, 108-109
 see also accommodation
CERT Australia 17, 40
Chemical, Biological, Radiological, Nuclear
and Explosive (CBRNE) weaponry 17, 169
China 18
client survey
 see stakeholder satisfaction survey
Code of Conduct (ASIO) 91, 92
Comcare 93
Commonwealth Director of Public
Prosecutions (CDPP) 51, 169
Commonwealth Games XVII, 19
communal violence XII, XVII, 3, 6, 41, 81
Community Contact Program 43
community engagement
 see also Community Contact
 Program
complaints IX, 65, 93, 165

Consultants 34, 36, 109
 Contact Reporting Scheme 41
 corporate governance XIV, XV, XVII, 67, 94-96, 166
 Counter Terrorism Control Centre VII, XIV, XX, 13, 21, 39, 60, 74, 75, 76, 169
 Counter Terrorism White Paper 13, 39
 counter-espionage XVI, 26, 40, 44, 51
 see also espionage
 counter-proliferation 42, 44
 see also proliferation
 counter-terrorism VII, IX, XII, XVI, XVIII, XIX, 4, 13
 capability 39
 Commonwealth Technical Response Capability 49, 169
 investigations XIX, 38
 Joint Counter-Terrorism Team 169
Crimes Act 1914 69
 see legislation
Criminal Code Act 1995 20
 see legislation
 critical infrastructure 13, 16, 17, 32-34
 culture (ASIO) XV, 69-70, 81, 87, 91, 93
 customers
 see stakeholder satisfaction survey
 cyber espionage XIV, XIX
 Cyber Espionage Branch VIII, XIV, XIX, 40, 62
 Department of Parliamentary Services, compromise of 62
 see also cyber security
 cyber security XIX, 13, 17, 75
 Cyber Security Operations Centre 17

D

Defence Imagery and Geospatial Organisation (DIGO) 39, 61, 86, 170
 Defence Intelligence Organisation (DIO) 15, 61, 86, 170
 Defence Security Authority (DSA) 86
 Defence Signals Directorate (DSD) XVI, 15, 34, 39, 61, 86, 170

Department of Defence 86
 Department of Finance and Deregulation 106, 127, 129
 Department of Foreign Affairs and Trade (DFAT) 13, 15, 86, 170
 Department of Immigration and Citizenship (DIAC) 25, 27, 170
 Department of the Prime Minister and Cabinet 49, 86, 151, 170
 Deputy Director-General (Mr David Fricker) XIV, 62, 96
 Director-General of Security (Mr David Irvine AO) VII-X, XI, XIV, 3, 13, 15, 21, 28, 43, 59-62, 68, 72, 75, 76, 81, 87
 disability, people with 161-162
 diversity 85, 91
 see workplace diversity

E

East Africa 46
 e-Learning 68, 70, 88
 Enterprise Bargaining Agreement 94
 environmental performance 108, 168
 see also accommodation
 E-security
 see also cyber security
 espionage XII, XIV, XVI, XVII, XVIII, 3, 4, 7-9, 15, 24, 26, 40, 44, 51, 62, 125, 156
 see also cyber security
 see also counter-espionage
 exchanges 44, 73, 85-86
 extremism XX, 3, 4, 13-14, 49

F

foreign interference XII, XVI-XVIII, 3-4, 9, 21, 24, 26, 40, 51, 125, 156
 foreign liaison 64
 foreign partners XIII, 19, 33, 86
 fraud III, 67-69, 166
 Fricker, Mr David
 see Deputy Director-General
 funding IX, XVII, 127, 151

G

governance
see corporate governance

H

Habib, Mamdouh 31, 63-64
 Hamas Izz al-Din al-Qassam Brigades (HAMAS) 157
 History of ASIO Project 104-105
 human resources 161, 166
 human source intelligence collection/capability XVI, 43

I

ICT Strategic Plan 51
 India 19
see Commonwealth Games
 Indonesia 5
 Information Services 98, 103-105
 information technology 4, 71, 109, 161
 Inspector-General of Intelligence and Security (IGIS) XIII, 31, 59, 64, 105, 170
 Inspire magazine 6
 international liaison
see foreign liaison
 international partners
see foreign partners
 internet 3, 6-8, 14, 84, 164
 Irregular Maritime Arrivals (IMAs) VII, XIX, 25-28, 65
see also Security Assessments
 Irvine, Mr David AO
see Director-General of Security

J

Jamaah Ansharut Tauhid (JAT) 5
 Jemaah Islamiyah (JI) VII, 5, 20, 157

K

Kurdistan Workers Party (PKK) 157

L

Lashkar-e-Tayyiba (LeT) 5, 157
 law enforcement VIII, XIII, XVI, 5, 13, 24, 43, 46, 48, 49, 69, 74, 89, 102
see police
 legal proceedings
see litigation
 legislation VIII, 102
Archives Act 1983 103
Australian Passports Act 2005 24
Australian Security Intelligence Organisation Act 1979 VII, XI, XII, 7, 20, 27, 171
Crimes Act 1914 69
Criminal Code Act 1995 20
Freedom of Information Act 1982 103, 111
Law Enforcement and National Security (Assumed Identities) Act 2010 69
Occupational Health and Safety Act 1991 93, 168
Telecommunications (Interception and Access) Act 1979 102
 legislative amendments, proposed 102
 listening devices 35, 46
 litigation XVI, XV, 30, 31, 51

M

Maritime Security Identification Cards (MSICs) 29
see also Security Assessments
 Middle East XIV, XVIII, 4-6, 45-46
 Minister for Defence 52
 Minister for Foreign Affairs 24, 52

N

National Archives of Australia 103, 177
 National Government Advisory Group on Chemical Security 17
 National interception Technical Assistance Centre (NiTAC) XX, 47, 170
 National Security College 40, 89

National Security Committee of Cabinet (NSC) 61, 170
 national security community XV, XVIII, 22, 43, 81, 90, 98, 102, 106
 National Security Hotline (NSH) 21, 170
 National Security Science and Innovation Strategy 49
 National Security Statement (2008) 3, 13
 National Threat Assessment Centre (NTAC) XVI, 14-15, 170
 new building
 see Central office (ASIO)
 New Delhi 2010 Commonwealth Games
 see Commonwealth Games
 New South Wales Police 15, 86
 see also law enforcement,

O

Office of National Assessments (ONA) 15, 61, 86, 170
 Office of Transport Security (OTS) 86
 Operation Neath 32
 see litigation
 organisational structure XIII-XIV, 164
 outreach XX, 49, 72, 74, 77, 85
 oversight IX, XIII, 59, 61
 see accountability

P

Pakistan 5, 6
 Parliamentary Joint Committee on Intelligence and Security (PJCIS) 28, 61, 109-110, 170
 Partnership Forums XX, 74
 Patek, Umar VIII, 5
 people development XIV
 people smuggling XIX, 26, 42, 44
 see also border integrity
 People's Republic of China (PRC)
 see China
 performance management 85, 90
 performance pay 94, 167

performance reporting 100, 166
 police
 see also law enforcement,
 Australian Federal Police, New
 South Wales Police, Victoria Police,
 Western Australia Police
 politically motivated violence XII, XVI,
 XVII, 3, 6, 21, 37, 41, 59, 125, 156
 private sector XIX, 14, 16-17, 32-33, 35,
 82
 proliferation 21, 42, 44
 proscription 20
 advice 20-21
 List of proscribed terrorist
 organisations 20, 157
 prosecutions 30-31, 51
 protective security XII, XV, XVII, XIX, 13-
 18, 32, 37, 48, 109
 Protective Security Policy Framework
 (PSPF) 37, 71, 170
 Protective Security Risk Reviews (PSRRs)
 32-33
 protest activity 41
 purchasing 109, 167

Q

questioning and detention 46,

R

Radicalisation 9, 14
 records management
 see Information Services
 recruitment IX, XV, 50, 71, 82-85, 91
 research and development 47, 49, 96
 Reviews
 Independent Review of the
 Intelligence Community 66
 Review of ASIO Resourcing
 (Taylor Review), IX, 83, 84
 risk management XIX, 15-16, 33-35,
 50, 68, 71, 86, 94, 96, 99-100, 165

S

Sabotage XII, XVII, 3, 7, 125, 156

Science Adviser 49
 Secretaries Committee on National Security (SCNS) 61, 170
 Security Assessments VIII, XIV, 24, 25
 Adverse 24, 29, 31
 Counter-terrorism 29-30
 Access to dangerous goods 29
 access to the Australian Nuclear Science and Technology Organisation facility at Lucas Heights, Sydney 29
 Personnel 30, 63
 Visa 25-28, 40
 security environment 33, 36-37, 40, 43, 45, 51, 75, 77, 81, 85, 99, 106
 security equipment evaluations 36
 Senate Standing Committee on Legal and Constitutional Affairs 43, 62
 Somalia 6
 South Asia 5, 6, 46
 see also Afghanistan, India and Pakistan
 special powers XVI, 43, 46, 62, 64
 Staff and Family Liaison Office (SFLO)
 stakeholder satisfaction survey 73-74, 97
 Strategic Plan 2011–13 VII, XX, 95, 97,
 Roadmap of Key Initiatives XX, 98
 Strategic Workforce Plan 85, 89-90
 surveillance XIV, XVI, XIX, 33, 35, 43-44, 50
 capability 43

T

T4 (Protective Security) 32, 37, 117, 170
 see also protective security
 Taylor Review of ASIO Resourcing
 see Reviews
 technical capabilities XIV, XVI, 47-49, 96, 109
 technical collection 47-49
 technical operations XII, XIV, XVI, 44
 technical surveillance counter measures 35

Telecommunications (Interception and

Access) Act 1979 VII
 see legislation
 telecommunications interception XX, 47-48, 52
 tendering 110
 Threat Assessments XV, 13-15, 18, 33
 threat environment
 see security environment
 tracking devices 46
 training and development 22, 36, 70, 89, 167

V

Vetting 30, 63, 71, 82-84, 169
 see Security Assessments
 Australian Government Security Vetting Agency (AGSVA) 30, 169
 Victoria Police
 see also police
 violent protest 41, 59
 visa security assessments XIV, 25-28, 40
 see Security Assessments – Visa

W

warrants XIV, 46, 60, 102, 1588
 weapons of mass destruction 42
 weapons proliferation 21
 website
 see ASIO website
 Western Australia Police 34, 86
 see also police
 Workplace Agreement
 see Enterprise Bargaining Agreement
 Workplace diversity
 Anti-bullying and harassment campaign 91, 92

Y

Yemen 6, 20
 see also Africa

