



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.

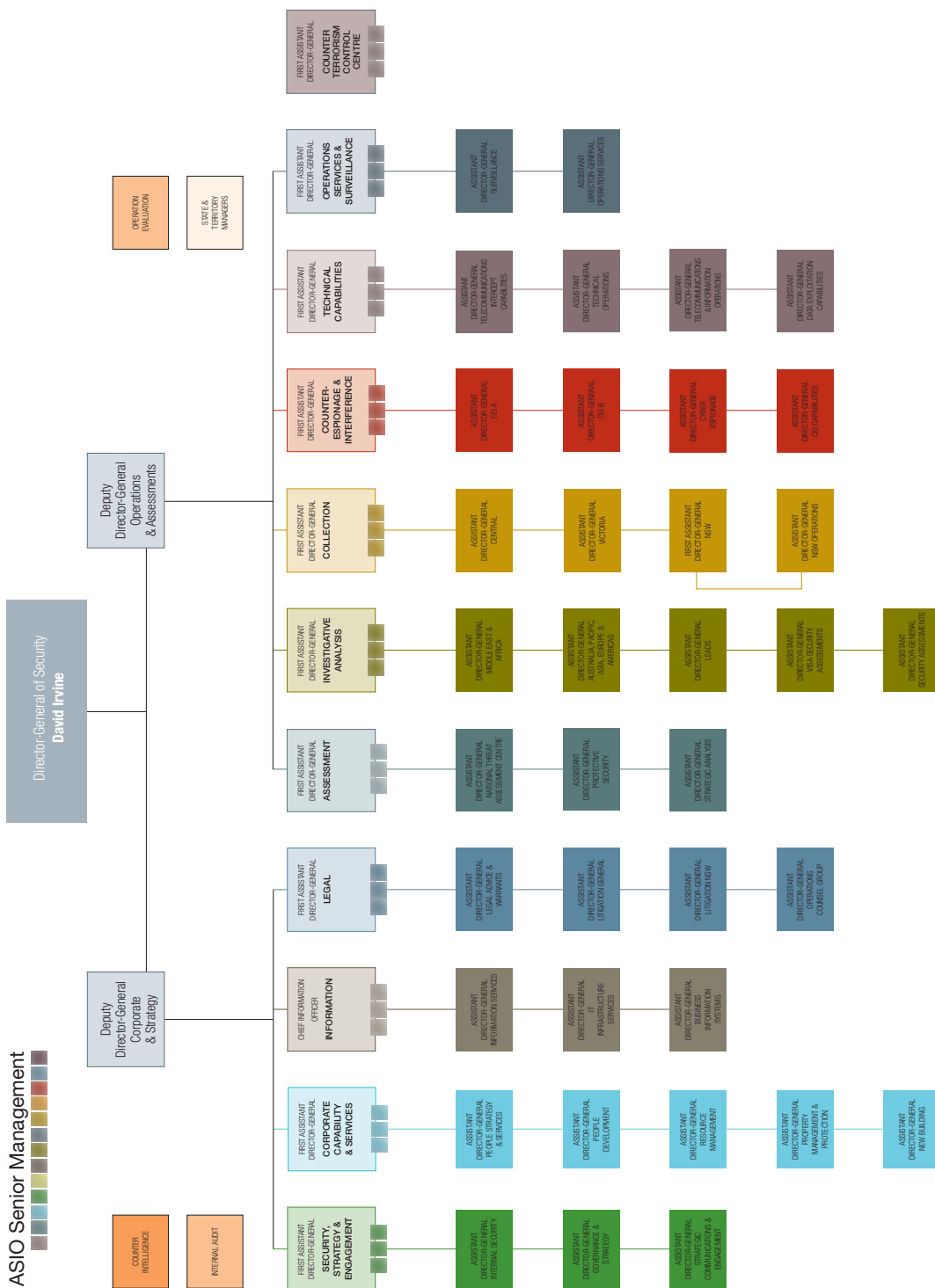


Figure 1. ASIO's organisational structure at 30 June 2011

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.