Australian Government

Australian Security Intelligence Organisation

report to parliament 2009-10

ASIO Report to Parliament 2009–10

ISSN 0815-4562

Australian Government

Australian Security Intelligence Organisation

Director-General of Security

12 October 2010

eA1179839

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 2010.

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

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

Yours,

David Irvine

David Irvine

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

Contents

Director-General's Review

Australians enjoy an unrivalled combination of national stability, individual freedoms and personal safety, based on our democratic system and the rule of law. But threats to our national security and the wellbeing of our citizens persist, including the possibility of attacks aimed at creating mass casualties. Attacks on Australians could occur at home or overseas.

It is the role of the Australian Security Intelligence Organisation (ASIO) to help defend Australia against nations, groups or individuals who seek to undermine or attack our national institutions, weaken our democracy or harm our people. It is a solemn responsibility; one that ASIO accepts along with the full acknowledgement that its actions in protecting Australia and Australians must exemplify the values and ideals that it seeks to safeguard. In 2010, the *Australian Security Intelligence Organisation Act 1979* was amended to expand ASIO's security intelligence functions to include border security. ASIO's work in this area will focus its capabilities on assisting the broader government efforts against people smuggling.

The environment in which ASIO must carry out its security intelligence responsibilities is constantly changing, requiring the Organisation to adapt, consolidate and then adapt all over again. For this reason, ASIO has initiated an important program of organisational renewal and modernisation. Aimed at ensuring ASIO remains equipped to identify and respond to national security threats into the future, the program will consolidate the Organisation's growth and provide a foundation for ASIO's future development. It will help ASIO keep pace as both state and non-state adversaries adopt more sophisticated methodology and tactics, multiplying their potential to cause serious economic or social harm, and in the case of terrorism, mass casualties. It also aims to enhance ASIO's ability to be agile, efficient and effective in meeting its statutory responsibilities in a constantly evolving operational environment.

Technology and the forces of globalisation are two of the principal drivers of our business modernisation. Australia's security and prosperity is today joined inextricably within a global network of interdependencies and linkages. Our security environment is therefore a product of both national and international factors. ASIO must consequently be positioned to operate in this interconnected world, able to identify and respond to threats wherever they emerge. This requires collaborative efforts with a range of partners, both in Australia and overseas. ASIO has particularly focused its efforts on contributing to better information and capability sharing arrangements within the Australian Intelligence Community and with law enforcement. For example, the establishment of the Counter Terrorism Control Centre in June 2010 harnesses the full capabilities of Australia's counter-terrorism agencies and will improve ASIO's ability to work effectively and collaboratively within the national security community in this key area.

Countering terrorism is not ASIO's only continuing focus. ASIO must also be highly capable within the cyber domain, working in close cooperation with the Defence Signals Directorate and the Attorney-General's Department. While ASIO's work remains very much a human endeavour, with espionage, terrorism and other politically inspired violence continuing to be driven by motivations of ideology, material gain and realpolitik, the communications revolution has fashioned new security frontiers. Cyber espionage is an emerging issue, requiring considerable attention across Government to address both the criminal and public protection aspects, as well as counter-espionage and other defence elements.

The speed and scale of technological development presents significant challenges for organisations like ASIO. It demands an increasing focus across all levels of Government on both the technological and the legal bases of the telecommunications interception regime. In response to these challenges, in 2010–11, ASIO will conduct a pilot study for the establishment of a National Interception Technical Assistance Centre, which will ultimately provide a central point for intelligence and law enforcement agencies to receive technical assistance to help keep pace with technological change in the digital age.

For terrorists, the Internet is a well-established and essential tool, providing not only a platform to support operations, but a means by which terrorist and other groups can amplify their messages to a global audience. Most recently, al-Qa'ida and its affiliates have been using the Internet to mainstream their message and reach out directly to English-speaking Muslims in western countries. Their objective is to tip those who sympathise with an extremist message into acting violently in support of it.

Espionage has also thrived on globalisation and the communications revolution. Digitisation means that massive amounts of information can be extracted, transferred and shuffled with ease. A single well-placed human agent becomes the potential source of archives worth of intelligence. Hostile intelligence agencies now also have a 'beyond-the-horizon' capability; they need not leave their own shores to target information held on our government, business and even personal computers.

Despite a low attrition rate, employment market conditions combined with the necessarily stringent and lengthy security vetting of potential new staff meant ASIO did not reach its ambitious recruitment targets for the year. ASIO's recruitment focus was on the more specialised areas of intelligence analysis and collection, where ready-made expertise is rare and must be taught in-house. Lower than anticipated staffing, and the decision to defer some expenditure to align better with the timing of ASIO's new building, resulted in ASIO returning a budget surplus. Recruitment will be a priority for the forthcoming year, with new people management strategies being developed to assist in meeting the higher net recruitment targets necessary to build and sustain a more effective national security intelligence capability.

The forthcoming period will be an important and challenging one. National security threats today emerge and mutate more rapidly. As a result, ASIO expects no let-up in the intensity or pace of its operating environment. The efforts ASIO has begun to ensure that it is positioned effectively to respond to security threats will be a continuing work in progress over the next few years to enable ASIO more vigorously and effectively to protect the security of Australia and Australians.

ASIO's Role and Functions

The Australian Security Intelligence Organisation (ASIO) is Australia's security service. It is a critical component of Australia's national security community and deals with threats to Australia's security. ASIO's roles and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). The *Anti-People Smuggling and Other Measures Act 2010*, which commenced on 1 June 2010, amended the definition of 'security' in the ASIO Act, enabling ASIO to use its existing capabilities to respond to people smuggling and other serious threats to Australia's territorial and border integrity. ASIO's primary function is to collect, analyse and disseminate security intelligence. For this, the ASIO Act defines 'security' as the protection of Australia, its people and interests against:

- espionage;
- sabotage;
- politically motivated violence;
- the promotion of communal violence;
- attacks on Australia's defence system; or
- acts of foreign interference;

and the protection of Australia's territorial and border integrity from serious threats.

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

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

- collects intelligence through a wide range of means, including human sources and technical operations, using the least intrusive means possible in accordance with guidelines issued by the Attorney-General;
- assesses intelligence and provides advice to Government, including in the form of Threat Assessments;
- investigates and responds to threats to security;
- maintains a national counter-terrorism capability; and
- provides Security Assessments, including for visa applicants and for access to classified material and designated security-controlled areas.

Under the ASIO Act and other legislation, ASIO can be authorised to use more intrusive powers under warrant. These include the interception of telecommunications, entering and searching premises, and compelling persons to appear before a prescribed authority to answer questions relating to terrorism matters. ASIO also has specialist capabilities that can be deployed to assist in intelligence operations and incident response.

The ASIO Act also gives ASIO a function of providing protective security advice to the Government.

ASIO is responsible for collecting foreign intelligence under warrant within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence, and in collaboration with the Australian Secret Intelligence Service or the Defence Signals Directorate.

As ASIO is the only agency in the Australian Intelligence Community authorised in the course of its normal duties to undertake investigations into, and collect intelligence on, the activities of Australian citizens, it operates within a particularly stringent oversight and accountability framework. The foundation of this framework is the ASIO Act, which has been crafted to ensure there is an appropriate balance between individual rights and the public's collective right to security. The Inspector-General of Intelligence and Security — an independent statutory authority — also plays an important role in overseeing ASIO's activities.

Organisational Structure

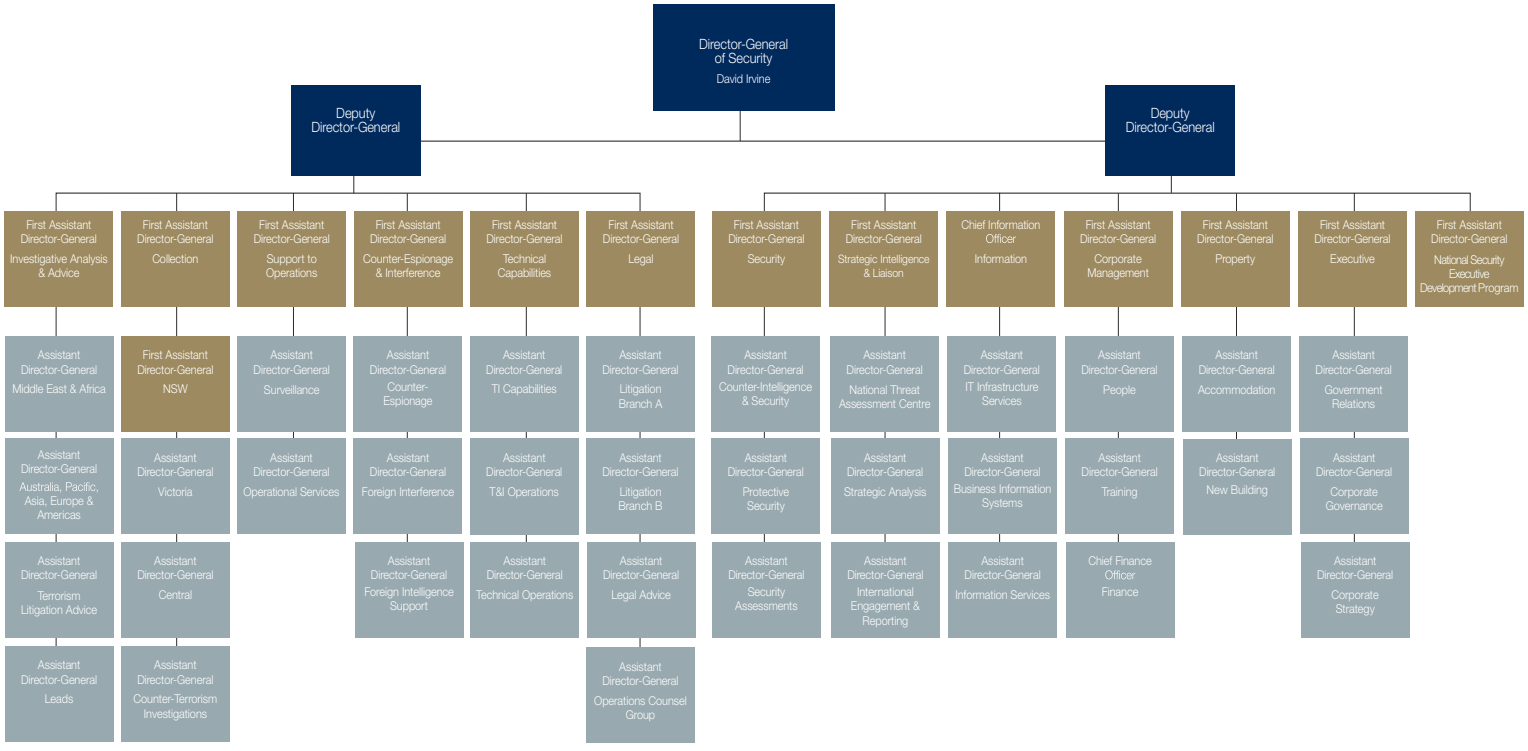


Figure 1: ASIO's Organisational Structure at 1 July 2009

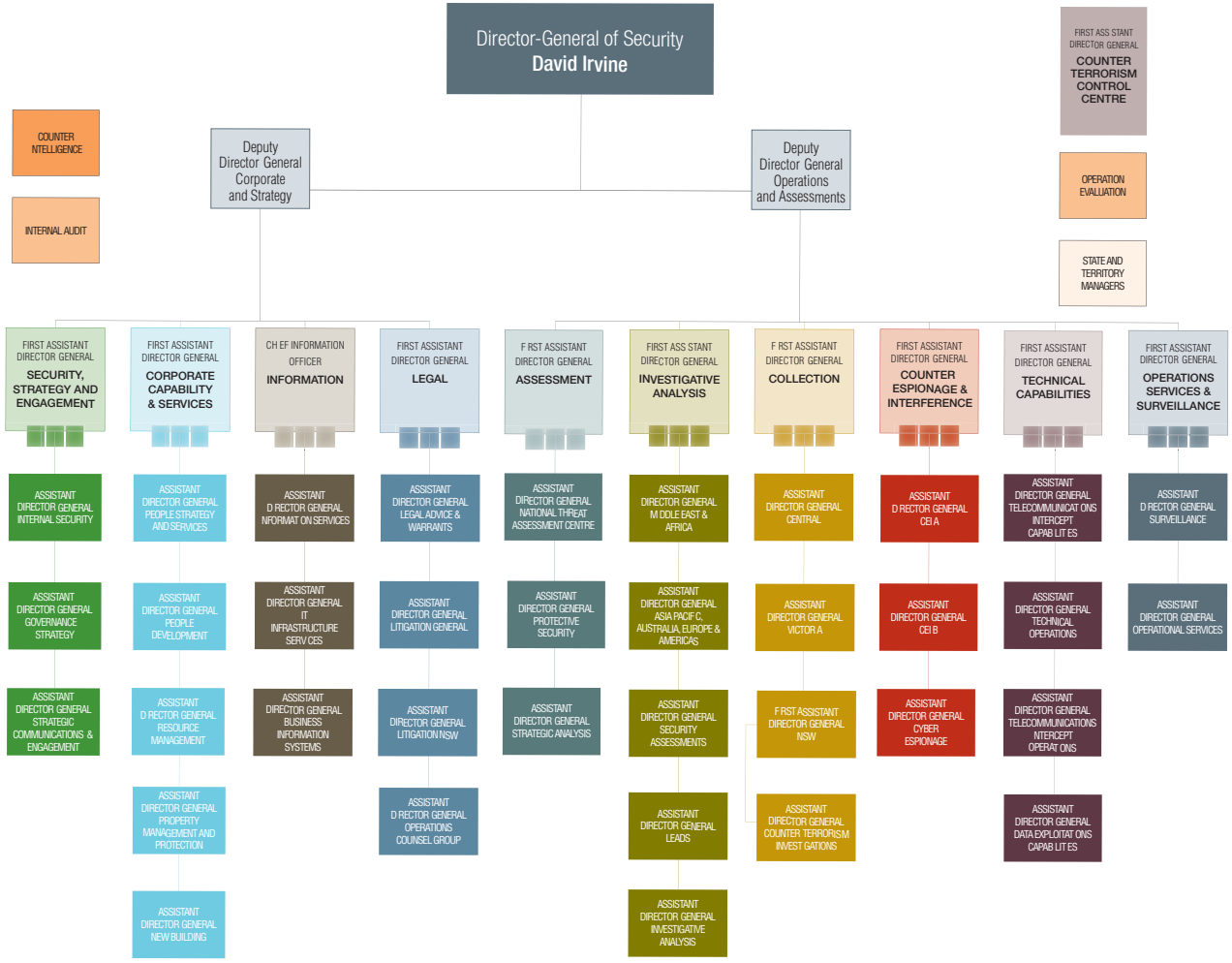


Figure 2: ASIO's Organisational Structure at 1 July 2010

ASIO's Funding, Outcome and Program Structure

In 2009–10, ASIO received funding from the Australian Government for 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.

Funding to ASIO expressed in terms of total price of program expenses was $368m, an increase of five per cent from the total cost in 2008–09 of $352m. The estimated total cost for program expenses for 2010–11 is $413m, an increase of twelve per cent from 2009–10.

Revenue from Government in 2009–10 increased 15 per cent to $406m, while revenue from independent sources (such as for services rendered) was similar to the 2008–09 figure of $10m.

This reporting period saw the last year of growth arising from the *Review of ASIO Resourcing* conducted by Mr Allan Taylor AM in 2005, and the end of consequential substantial funding increases to meet the additional staffing, operating and depreciation expenses.

Separately, ASIO received an equity injection of $16m for 2009–10, to fund additional capability ($14m), telecommunications interception capabilities ($2m) and for ASIO's new building ($589m).

ASIO achieved efficiency savings, including through the identification and elimination of duplication created during the period of sustained growth and the refinement of resource allocation and management across priorities.

A further equity injection will be received in 2010–11 of $89m. This provides funding for asset replacement ($28m) and for ASIO's new building project ($61m).

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

Client Survey

The annual Client Survey provides ASIO with valuable insight into the level of satisfaction of key partners, and the extent to which ASIO supports the attainment of partner agency outcomes. The quality (usefulness, uniqueness and timeliness) of ASIO advice and reporting is canvassed, as are suggestions for enhancing cooperation and collaboration. In 2010, interviews were conducted with representatives of key Commonwealth, state and territory agencies and private sector clients. Traditionally conducted at the Senior Executive Service (SES) level, in 2009–10 the survey was expanded to include respondents at Executive Level 2 to seek feedback on initiatives to promote understanding of ASIO's role and functions, and improve networks at middle management level. The survey was also extended to include Australian Government clients located at overseas posts.

ASIO's relationships with clients were viewed as generally positive and the Organisation's reporting product was regarded highly. Over the past year, some Commonwealth customers noted a significant improvement in their engagement with ASIO, citing Partnership Forums and other relationship-building activities, at both the SES and middle management level, as key to that improvement.

Federal, state and territory law enforcement agencies reported continued improvement in already strong relationships with ASIO. They also reported greater understanding of ASIO's responsibilities in 2009–10, especially through ASIO officers attached to those agencies. ASIO reporting was well-received and contributed directly to law enforcement efforts by police agencies. Nevertheless, some agencies noted better cooperation and communication with counterparts at middle management level was still needed.

In general, private sector clients were positive about their engagement with ASIO, particularly through the Business Liaison Unit and its associated website. Reporting was considered timely and was valued for offering a uniquely Australian perspective on global security issues. ASIO advice directly informed strategic decision-making for some customers. Private sector clients also commented on the value of maintaining their continued engagement with ASIO, a few noting a decline in the regularity of ASIO's engagement in the latter part of the reporting period.

Guide to the Report

ASIO produces a classified and an unclassified Annual Report. Section 94 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) requires the Director-General of Security, as soon as practicable after 30 June, to furnish the Minister with 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 Three of ASIO's *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.

Executive Summary

The Security Environment

Two key events in the reporting period highlighted the persistent threat of terrorism. Within Australia, a major counter-terrorism investigation culminated in the arrest of five individuals on terrorism-related charges. Offshore, three Australians were killed in Jakarta during an attack on the JW Marriott Hotel in July 2009.

The protection of Australia from espionage also became more complex with globalisation and rapid technological advances. ASIO continued to build on relationships with government, business and industry to raise awareness and promote security. Traditional forms of espionage also continued to be employed by foreign services attempting to access information.

Countering proliferation remained an international security challenge and ASIO continued to work with both domestic and international partners against the activities of foreign states that seek to gain materials or knowledge used to develop weapons of mass destruction.

ASIO's Activities and Outcomes 2009–10

ASIO continued to contribute significantly to the disruption of serious threats to security in 2009–10. As with the previous reporting period, much of ASIO's collection and analysis effort was focused on countering terrorism. However, foreign interference, espionage and proliferation remained of security concern in Australia and significant ASIO resources went to countering these threats.

In the reporting period, ASIO's contribution to protecting the security of Australia and its interests included the following:

- investigative and operational activity as part of a multi-agency investigation that culminated in the arrest of five individuals in Melbourne in August 2009 who were charged with conspiring to plan or prepare for a terrorist attack on home soil;
- identification of Australians overseas participating in terrorism-related activity and/or providing support to terrorist groups. This enabled preventative action to be taken;
- assessment of multiple terrorism-related threats against Australian or western interests in South-East Asia, Pakistan, the Middle East and Africa;
- identification of instances of foreign interference and espionage against Australia, including electronic espionage;
- production of, in concert with other departments and agencies, a long-term assessment on Australia's domestic security to 2030; and

- assessment of a large volume of lead information and implementation of a program of enhanced engagement with external stakeholders, resulting in more valuable lead intelligence being passed.

ASIO produces a range of intelligence reports for key customers, advising on a range of topics from terrorism threats to trends in radicalisation. This includes the provision of advice to Government on potential terrorism threats to Australia and Australian interests overseas. The provision of Threat Assessments is an ongoing function of ASIO and is performed by the National Threat Assessment Centre (NTAC). During the reporting period, ASIO made significant improvements to its intelligence reporting line, refining and rationalising reporting to better meet the needs of customers. In 2009–10, ASIO produced 3,274 reports and assessments. This number includes reports to Government and international partners, as well as reports to the private sector, via the Business Liaison Unit.

While the Attorney-General's Department is the lead agency for proscription of terrorist organisations in Australia, ASIO contributes security intelligence advice to the proscription process by informing the Attorney-General's consideration of whether a group should be proscribed in Australia. In 2009–10, one new group was proscribed and four were relisted.

Over the reporting period ASIO provided security assessment advice for Government consideration in a range of decision-making processes:

- ASIO conducted 38,438 visa Security Assessments and a further 989 assessments for protection visa applicants. 19 adverse assessments were made in relation to visas;
- ASIO issued adverse Security Assessments in respect of the Australian passports of eight individuals;
- ASIO completed 22,343 personnel Security Assessments; and
- ASIO conducted 98,086 counter-terrorism Security Assessments. These include assessments for aviation/maritime security identity cards and access to restricted areas and/or sensitive goods.

ASIO also continued to provide protective security advice and Threat Assessments for high-profile events.

- During the reporting period, preparations began for the Commonwealth Games, to be held in New Delhi in October 2010. This required significant analysis of intelligence and the provision of advice in Threat Assessments – this work is ongoing.
- ASIO's T4 Protective Security Directorate provided a range of protective security advice including risk reviews, certification for Australian top secret facilities, security

equipment evaluations, training, the detection of technical attacks and security reviews of Ministerial Offices.

ASIO continued to make strong contributions to whole-of-government national security policy coordination forums such as the National Security Committee of Cabinet and the National Intelligence Coordination Committee. These contributions included assisting the successful implementation of the new national security framework and seconding a senior ASIO officer to the Department of the Prime Minister and Cabinet to develop and pilot the National Security Executive Leadership Program and help develop the National Security College initiative identified in the then Prime Minister, the Hon. Kevin Rudd MP's 2008 National Security Statement.

ASIO continued to expand relationships with domestic and international partners, including intelligence agencies, law enforcement bodies and industry representatives.

- During 2009–10, ASIO continued a high-tempo of joint operational activity with the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD), and international partners in support of foreign intelligence collection priorities.
- Over the reporting period ASIO liaised with private enterprise and government bodies to investigate and counter cyber attacks against, or involving, Australian interests.
- At 30 June 2010, ASIO had liaison relationships with 329 security, intelligence and law enforcement agencies in 123 countries around the world.
- In February 2010, the then Prime Minister, the Hon. Kevin Rudd MP announced the creation of the Counter Terrorism Control Centre (comprising ASIO, ASIS, the Australian Federal Police and DSD) to coordinate the Commonwealth's counter-terrorism intelligence and investigative activities.

In 2009–10, ASIO was involved in over 40 litigation matters, including criminal (in particular terrorism) prosecutions, judicial and administrative review of Security Assessments, and a range of civil actions.

Recruiting suitable staff remains a challenge. ASIO made significant investments in developing staff, including in the areas of professional development, language and technical capabilities.

Construction is progressing on schedule for ASIO's new central office and is expected to be completed in 2012.

part
one

1

Threats and the Security Environment 2009–10

The Security Environment 2009–10 and Outlook

Tragically, the past year has again brought home to Australians the proximity and endurance of the threat posed by terrorism. Three Australian lives were claimed by a terrorist attack on a Jakarta hotel in July 2009.

Indonesian forensic investigators inspect the aftermath of a bomb blast at the JW Marriott Hotel in Jakarta, July 2009. Source AFP/PHOTO/POOL/DITA ALANGKARA.

Global interconnectivity enables 'home-grown' extremists to link into an overseas terrorist network, adapt a militant ideology to the local landscape, and plan, resource and stage an attack, without the material support or membership of a terrorist organisation. Over the past eight years, four potentially very serious attacks intended to produce mass casualties have been prevented. Five individuals were arrested in Melbourne in August 2009 and have been charged with conspiring to plan or prepare for a terrorist attack on home soil.

The impact of globalisation on Australian security is not a new development, but it is one that, with each technological advance, lends increasing complexity, proximity and pace to ASIO's operating environment. Globalisation has been a significant influencing factor in the evolution of terrorism. The nature of our world today — our ability to access and share information in real-time with others around the world, and the mass movement of people and money across borders — brings the terrorism threat closer to home than ever before. The publication of al-Qa'ida's online English-language magazine, *Inspire*, is a reminder

not only that terrorist organisations are actively seeking western recruits, but that they can do so most effectively using a tool that epitomises the globalised world.

The use of the Internet as a propaganda and recruitment tool has enabled al-Qa'ida and other terrorist organisations to access and influence a vast, international audience. Users of the Internet can access extremist ideology through many jihadist websites and be drawn into the process of radicalisation without leaving their homes. This in turn translates into changed methods of attack that are more likely to be locally financed, involve little training and use readily available weapons or materials.

As well as forging virtual paths in extending their influence beyond actual theatres of conflict, the constant movement of people across borders presents terrorist groups with opportunities. Of the millions of people entering Australia every year, there is a small proportion whose motives in travelling to Australia are inimical to Australia's national security interests.

Australia has previously been targeted for attack by an individual who was sent here by an overseas terrorist group. In that instance, it was information provided by a foreign partner that triggered ASIO's investigation and consequent intelligence and law enforcement disruption activity. With substantial volumes of people entering Australia every year this scenario could be repeated and reinforces the value of ASIO's international partnerships, as well as its relationships with local communities.

Al-Qa'ida-affiliated groups and others inspired by similar ideology are likely to be the primary source of terrorism threat to western lives and interests for years to come. Al-Qa'ida has responded to international counter-terrorism efforts by expanding its operations to increase its reach and access to more resources, recruits and support networks. Its strategy of decentralisation has seen the al-Qa'ida network mitigate setbacks such as failed operations and loss of leadership figures, to maintain a leadership role in the international jihadist movement.

Since al-Qa'ida first claimed Australians among its victims in New York on 11 September 2001, over 100 Australians have died in terrorist attacks. ASIO and its partners continue to respond to a range of terrorism-related activity both within Australia and overseas.

While in recent times the terrorism threat in South-East Asia has been overshadowed by the more volatile security environments in South Asia, the Middle East, East Africa and elsewhere, it was a suicide bombing in a Jakarta hotel in July 2009 that claimed Australian lives most recently. Despite the region's best known terrorist group, Jemaah Islamiyah, suffering the loss of several high profile operatives in recent times — Noordin Muhammad Top in September 2009 and Dulmatin in March 2010 — the group's networks are deeply entrenched, resilient and capable of resurgence. The successes of Indonesian counter-terrorism authorities against the terrorism threat in Indonesia are most welcome; but, given its proximity to Australia and the strong business, trade and government interests

that connect us to our neighbours, monitoring the Islamist terrorism threat in South-East Asia must remain a priority for ASIO.[1]

South Asia remains a key region for Islamist terrorist activity, and Pakistan is still al-Qa'ida's preferred sanctuary. The volatility of the Afghan conflict and the lawlessness of the Pakistan border region create an operating environment conducive to the recruitment, training and deployment of militants. The failed Times Square bomber, Faisal Shahzad, a naturalised American from Pakistan, claims to have undertaken training in Pakistan prior to the operation in New York in May 2010. Australians have also undertaken militant training and engaged in fighting in Pakistan and Afghanistan.

While al-Qa'ida has long been established in the Middle East, concern is also growing about the entrenched terrorism threat emanating from Yemen. The regional al-Qa'ida presence, al-Qa'ida in the Arabian Peninsula (AQAP), orchestrated the attempted bombing of a Northwest Airlines flight between Amsterdam and Detroit on Christmas Day, 2009. Umar Farouk Abdulmutallab, a Nigerian citizen, was a student in Yemen, where he received support, training and materiel assistance from AQAP to undertake the operation. It is likely that Abdulmutallab was inspired by Anwar al-Aulaqi, an al-Qa'ida-linked cleric based in Yemen, with whom Abdulmutallab had prior contact. A number of Australians have been drawn to extremist figures in Yemen, including via the Internet. Australians resident in Yemen have also participated in terrorism-related activity. The effectiveness of Yemen's counter-terrorism campaign will impact directly the global threat environment.

Al-Shabaab, the Somali Islamist terrorist group engaged in violent opposition to the Somali Transitional Government forces, has been linked to al-Qa'ida and has supporters in Australia. With the collapse of law and order in parts of Somalia, the terrorism threat from the East Africa region is likely to remain a threat to international security for the foreseeable future.

ASIO's investigative and operational activity has shown consistently that overseas drivers and links remain central to the threat to Australia. Australians travel and live in all corners of the globe, and Australian interests — government, business and industry — are also scattered widely, including in locations with volatile and unpredictable security environments such as Pakistan and Afghanistan. This provides opportunity for those seeking to target Australia. At the same time, concerns are growing at the rise of 'home-grown' potential terrorists and an increase in the number of Australians seeking to travel overseas for terrorism-related purposes. ASIO assessment and advice contributes to the protection of Australian interests around the world, including through Threat Assessments and Security Assessments.

1. On 9 August 2010, Indonesian police arrested Abu Bakar Ba'asyir on suspicion of a series of terrorist activities in Aceh and Bandung in Indonesia. Abu Bakar Ba'asyir is a founding member of Jemaah Islamiyah and is a leader of the group Jamaah Ansharut Tauhid.

Espionage is a constant in the international threat environment and draws increasingly on ASIO's resources. Technological developments present foreign states and non-state actors with greater opportunities to access and exploit electronic information systems remotely. ASIO works with the Government, and business and industry sectors to raise awareness and promote appropriate security against cyber intrusion and exploitation. In January 2010, a multi-agency initiative was established to coordinate work against the threat. The Cyber Security Operations Centre was established in the Defence Signals Directorate in 2009 as an initiative of the *Defence White Paper* to coordinate work against this threat. Personnel from ASIO, the Attorney-General's Department and the Australian Federal Police are embedded within the Centre.

Electronic espionage is one means by which foreign services attempt to access Australian military, security, diplomatic, scientific and commercial information. Traditional methods, such as cultivating the cooperation of Australian citizens in positions of access or influence, also continue.

The ambitions of some states to obtain weapons of mass destruction continue to threaten global security. As part of a whole-of-government approach, ASIO's counter-proliferation work aims to identify and prevent illicit efforts by foreign governments to gain technological knowledge and materials in Australia; however, the proliferation threat remains a serious and lasting one.

International cooperation contributed vital intelligence to ASIO investigations, and, in view of the increasingly transnational nature of security threats, will continue to be a crucial element.

ASIO continues also to rely heavily on relationships with local communities. These are vital alliances, as community members are often the first to become aware of issues or events related to security, from instances of communal violence to interference by foreign governments in expatriate communities. ASIO continues to stress that its activities target terrorism, they do not target ethnic groups, a particular religion or its role in the Australian community.

ASIO maintains strong relationships with a range of international partners to ensure best possible coverage, cooperation and sharing of information. In the 2009–10 reporting period, ASIO provided frequent support to the investigative and analytical requirements of foreign partners and received strong reciprocal assistance.

ASIO also engaged with its domestic partners on a range of new issues, as the terrorism threat increasingly intertwines with law enforcement areas such as identity fraud and border security. In recognition of this, new legislation (*Anti-People Smuggling and Other Measures 2010*), which came into effect in June 2010, paves the way for ASIO to contribute to the whole-of-government effort to maintain border security.

ASIO is implementing new initiatives to capitalise on existing partnerships with security and law enforcement agencies, such as the recently established Counter Terrorism Control Centre (CTCC). The CTCC, announced in the February 2010 *Counter-Terrorism White Paper*, is a joint agency team which will manage the intelligence community's response to national counter-terrorism intelligence priorities and improve agency interoperability and cooperation.

As well as forging closer relationships with established partners, ASIO is engaging with non-traditional partners to contribute to government initiatives aimed at countering the terrorism threat, such as programs to identify and respond to signs of radicalisation of people in the community.

ASIO continues to contribute in a significant way to the disruption of serious threats to Australia's national security, although much of ASIO's work will quite properly never be acknowledged publicly – regardless of its success. ASIO intends to keep pace with emerging sources of threat by utilising strategic partnerships, observing trends in the international security environment, and applying lessons learnt — its own and others' — to its work.

part
two

2

Program Performance

part two

Security Intelligence Analysis and Advice

Analysis in ASIO

ASIO's analytical work meets a diverse range of requirements for intelligence analysis and advice from a broad group of mostly – but not exclusively – government customers and clients.

As ASIO is an operationally focused agency and as a collector of intelligence, much of ASIO's analysis serves primarily to meet ASIO's operational and investigative requirements. For example, it might assist in the planning and execution of an intelligence collection operation, or contribute to a focused terrorism or espionage investigation. These in turn form the basis from which advice is provided or action taken to counter threats to security.

ASIO analysis can also support other agencies' operational requirements, such as providing security for events of national significance. ASIO's Threat Assessments are used by agencies to calibrate their operational advice and responses, including for police protective security for Parliamentarians, or for the Department of Foreign Affairs and Trade (DFAT) public Travel Advisories.

Some ASIO analysis is aimed at meeting the Australian Government's strategic requirements, particularly support for policy development and implementation.

To serve the diverse range of analysis requirements, there are a number of different but complementary intelligence assessment disciplines within ASIO. Some rely heavily on technical and information technology expertise, while others rely on investigative skills and an ability to identify important details from within large quantities of information.

By its nature, however, intelligence can sometimes be imprecise and incomplete. So ASIO relies heavily on the professional judgment and experience of its analysts.

Strategic Assessment

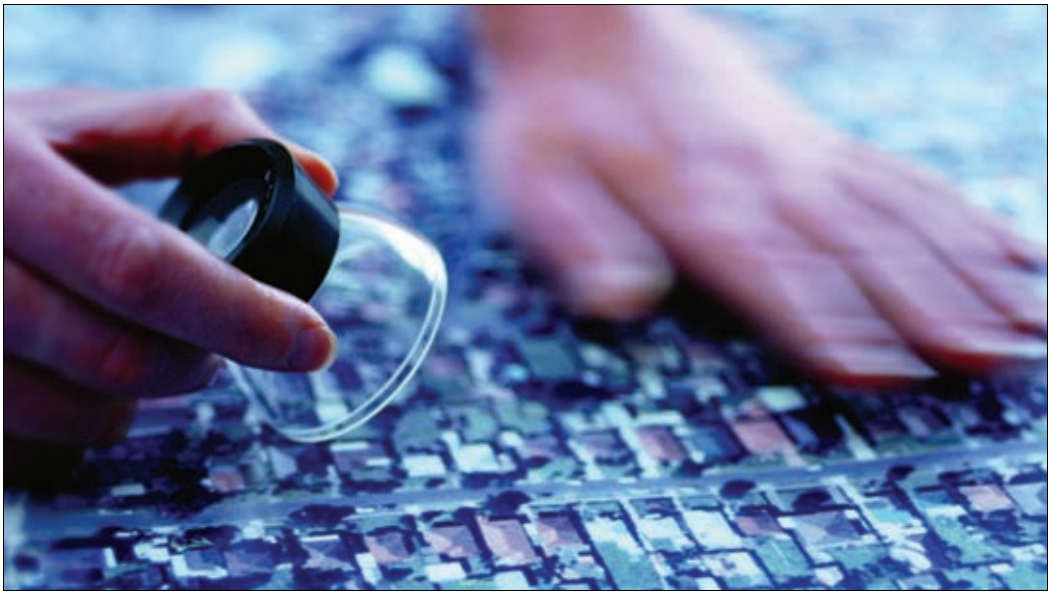
ASIO strategic assessment is typically thematic and nationally focused and usually forward-looking. It aims to assist senior national security policy and decision makers to prepare for, and respond effectively to, current and emerging threats and opportunities. Drawing on ASIO's long history and expertise in examining issues such as terrorism and espionage, strategic intelligence seeks to provide unique insights into issues of national significance, identifying trends, patterns and key developments important to the development of policy and strategy.

As well as drawing on the expertise of its analysts, ASIO is increasingly employing a range of technical analysis and visualisation tools in strategic assessments as a way of presenting complex data in a manner that better assists decision-making. In 2009–10, this was well-received by ASIO customers, particularly police services.

In 2009–10, ASIO supported decision-makers by providing a range of strategic and thematic assessments relating to extremism in Australia, radicalisation, global terrorism, and terrorists' modus operandi. In 2009, ASIO again produced a classified comprehensive and long-term national assessment on Australia's domestic national security outlook to 2030.

A collaborative effort by ASIO and a range of other departments and agencies, the 2030 report concluded that in addition to 'home-grown' local developments, Australia's domestic security environment would remain inextricably linked to developments overseas. It found that transnational terrorism would pose the most visible and immediate threat to Australia and Australians over the next two decades. Other matters such as organised criminal activity (particularly any intersection with terrorists or state-sponsored activity) and espionage and foreign interference were noted as having potential to harm national security by undermining public confidence in the Government or economy. The most severe impacts of climate change were not expected to be realised in the period to 2030, though climate change-linked social challenges in Australia or elsewhere are seen as likely.

The 2030 report was ASIO's second collaborative domestic security forecast. Having been received positively by a range of customers, ASIO expects to continue the series in future years.



Threat Assessment and Analysis

ASIO has provided threat assessment advice for more than 30 years as a central plank of its functions in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). In 2004, the Australian Government established the National Threat Assessment Centre (NTAC) as a multi-agency centre within ASIO to provide threat assessment advice to federal, state and international partners on threats to Australian interests both onshore and offshore arising from terrorism, politically motivated violence, communal violence and violent protest.

Threat Assessments are the major medium through which ASIO disseminates advice to Commonwealth and state and territory governments and to relevant private sector entities on threats to Australia and Australian interests domestically and overseas. They are a key element in Australia's coordinated protective security arrangements.

In 2009-10, ASIO produced 588 Threat Assessments. During the reporting period, the NTAC revised and enhanced its approach to provide more forward-looking, consolidated and strategic advice, particularly in connection with the assessment of several discrete but related lines of threat reporting. This resulted in the production of higher value threat assessment advice in fewer reports that were more durable and aligned more closely with customer requirements. NTAC also consolidated routine weekly threat assessment advice into one product where previously multiple individual assessments were issued.

Investigative Analysis

Investigative analysis underpins ASIO's ability to identify individuals or groups who threaten, or have the potential to threaten, the security of Australia and Australians. As

part of the investigative process, information collected from ASIO's investigative and operational activity (including physical surveillance, human intelligence and technically-derived intelligence) is evaluated and assessed along with intelligence from a range of other classified and unclassified sources in order to determine and investigate potential threats.

Investigative analysis of identified threats is used to refine intelligence requirements that guide further intelligence collection, including by ASIO's partners within the national security community. The outcomes of ASIO's investigative analysis provide the basis of intelligence advice and reporting that informs policy development, decision-making and operational responses.

In recent years, ASIO intelligence investigations have:

- identified and assisted in disrupting a number of terrorist cells and plans for attack in Australia — and contributed to successful terrorism prosecutions in Australian courts;
- identified Australians overseas participating in terrorism;
- led to Australians being prevented from travelling overseas to participate in terrorism-related activity;
- revealed threats to Australia and Australian interests overseas;
- uncovered serious cases of electronic espionage and other espionage and foreign interference activity;
- provided valuable insights into the activities, objectives and modus operandi of overseas groups that impact on Australia's security; and
- contributed to overseas agencies' terrorism and espionage investigations, including threat-to-life investigations.

The pace of investigative analysis remained intense in 2009–10. In addition to the major counter-terrorism operation in Melbourne, ASIO provided considerable support to a threat-to-life investigation of an international partner agency. Other investigations revealed that terrorism-related activity continued to take place in Australia, and that Australians overseas continued to support terrorism. Preventative action such as passport cancellations was again taken in 2009–10.

ASIO's investigative analysis during the reporting period also focused on groups threatening Australian interests overseas, particularly in South-East Asia, Pakistan, the Middle East and East Africa.

Threats to the integrity of Australia's national institutions and economic interests from espionage and foreign interference were also identified.

Leads Development and Analysis

Lead intelligence is vitally important to ASIO's ability to uncover threats and ASIO relies heavily on lead information that is passed to it by people within the local community, overseas liaison services, the police, other government agencies, and the public — particularly through the National Security Hotline (NSH). ASIO also generates its own leads through day-to-day operational activity, scanning of open sources and periodic 'cold case' reviews.

In most instances, ASIO will determine that a lead is not a security concern and does not require further investigative (or other government) attention. This is important as it provides a measure of assurance to the Government and the public that a threat does not exist. In some cases, however, leads — including through the NSH — become major investigations and have resulted in ASIO uncovering serious cases of espionage and foreign interference, weapons proliferation, criminal activity (which is referred to the police as incidentally collected intelligence) and terrorism.

Even seemingly insignificant information can be important in lead investigation and analysis, and can be the missing piece of the puzzle that reveals whether or not a threat exists. Such fine detail is often obtainable only through ASIO working directly with other agencies, or the public. ASIO relies heavily, therefore, on their readiness to contact the Organisation, and willingness to cooperate.

Managing the significant volumes of lead information entering ASIO remains a challenge. Consequently, the Organisation continually reviews processes, procedures and technological aids to respond efficiently and effectively to leads. Ongoing specialised training for leads analysts was a priority in 2009–10.

Information referred to ASIO from staff at major sea and air ports is also an important source of lead intelligence. In 2009–10, ASIO introduced a national briefing program to enhance the awareness of frontline Department of Immigration and Citizenship (DIAC) staff of ASIO's role and highlight the valuable role that DIAC staff can play in assisting ASIO to identify threats to Australia's national security. ASIO had input into a similar program run by the Australian Customs and Border Protection Service, another longstanding ASIO partner with a crucial role. ASIO also worked closely with the Attorney-General's Department (AGD) which manages the NSH. The aim of this engagement is better focused and more valuable lead intelligence.

During the reporting period, ASIO worked closely with overseas partners on best-practice lead generation methodology. Priority was given during the year to leads generation from ASIO's own intelligence holdings, including review of historical 'cold cases', using advanced data analysis techniques. These techniques help to identify trends, patterns and indicators that would otherwise be not readily identifiable to analysts.

Complex Technical and Tactical Analysis

Complex technical and tactical analysis typically involves manipulation, sorting and cross-checking of large data sets, or complex computer simulations. The demand for such capability increased in 2009–10, particularly to support ongoing ASIO counter-terrorism investigations and in response to a greater requirement for complex financial transaction analysis.

Intelligence Reporting

ASIO draws on all sources of intelligence, including its own intelligence collection, in providing a range of regular intelligence reporting. In 2009–10, ASIO published 3,274 intelligence reports for a regular customer set of over 90 Commonwealth, state and territory government customers as well as international partners. In addition to its published intelligence reports, ASIO also continued to exchange information with a variety of agencies, particularly the police and close foreign partners.

In 2009–10, ASIO reviewed comprehensively its intelligence reporting product line to rationalise the variety of reports being produced, tailor reporting to a diverse and busy customer set and ensure that the reporting is immediately recognisable as originating from ASIO. Because ASIO serves a diverse customer set ranging from Ministers to tactical response agencies – at federal and state level, and both within Australia and overseas – tailoring intelligence reporting to meet varied requirements can be a challenge. The new line of specifically-focused products should assist customers identify the intelligence likely to be of most value to them.

ASIO's published intelligence reports

ASIO Analytical Report

ASIO Analytical Reports provide strategic assessment or investigative analysis of current or emerging security issues. They are also used to report the outcomes of ASIO's security intelligence operations and investigations.

ASIO Analytical Reports are used by Australian decision-makers, policy departments, and operational agencies to gain insight into, and respond to, complex security matters.

ASIO Threat Assessment

ASIO Threat Assessments assess the level of threat – primarily from politically motivated violence – to Australia's domestic and overseas interests, foreign country interests within Australia and to major events.

Threat Assessments inform components of Department of Foreign Affairs and Trade Travel Advisories and are used by a range of operational agencies to calibrate protective security measures according to the level of threat determined by ASIO.

ASIO Intelligence Report

ASIO Intelligence Reports contain single source, unassessed (raw) intelligence obtained through ASIO's security intelligence activities. Because ASIO Intelligence Reports contain unassessed intelligence – and are typically highly sensitive – they are distributed to a targeted audience appropriate to the subject matter.

ASIO Intelligence Reports aim to provide Australian and foreign liaison partners with unique and/or actionable intelligence.

Research and Monitoring Report

Research and Monitoring Reports summarise the available classified and unclassified reporting on a specific topic. They are particularly valuable for subject familiarisation and as a foundation for strategic assessments and to guide investigative activity.

ASIO Brief

The ASIO Brief is designed specifically for senior national security partners. It provides a summary of key threat and security intelligence assessments produced and a brief update on investigative matters.

Business Liaison Unit Reports

Business Liaison Unit Reports provide advice on a range of general security and incident reporting relevant to key Australian industries and infrastructure.

ASIO's Business Liaison Unit is responsible for the reports, which are aimed at assisting Australian companies understand better the security environment and the threats they may face, and assist with security planning.

Intelligence Advice

In addition to regular published intelligence reports ASIO provides tailored intelligence advice to clients for specific purposes.

National Security and Intelligence Policy Advice

In 2009–10, ASIO made a strong contribution to whole-of-government national security policy coordination forums such as the National Security Committee of Cabinet and the National Intelligence Coordination Committee.

ASIO worked closely with the National Security Adviser and the Department of the Prime Minister and Cabinet (PM&C) to drive the successful implementation of the new national security framework, including through development of a set of national security priorities, a coordinated national security budget and a national security evaluation mechanism.

In 2009, a senior ASIO officer was seconded to PM&C to develop and pilot the National Security Executive Leadership Development program and help develop the National Security College initiative identified in the then Prime Minister, the Hon. Kevin Rudd MP's 2008 National Security Statement.

ASIO continued its program of briefing Ministers, Parliamentarians and senior level officials of partner departments and agencies on priorities, capabilities and the breadth of ASIO functions. ASIO also continued to provide advice to foreign liaison partners.

Proscription-related Advice

The mechanism legally to proscribe certain groups as terrorist organisations is an important component of Australia's counter-terrorism arrangements. Proscription explicitly criminalises political, material and economic support for a specified terrorist group. It serves to deter anybody sympathetic to the group's cause from becoming involved in its activities, in Australia or overseas, and it ensures Australia is a non-conducive environment for the group's operations. When a group is proscribed by regulation it is accepted as a matter of Australian law that the entity is a terrorist organisation. A counter-terrorism control order Under Division 104 of the *Criminal Code Act 1995* may be possible if the person has provided training to, or received training from, a proscribed group.

ASIO has no decision-making powers in relation to proscription. AGD is the lead agency for proscription in Australia, and ASIO contributes security intelligence advice to the proscription process by informing the Attorney-General's consideration of whether a group should be proscribed in Australia.

Before the Governor-General makes a regulation specifying an organisation as a terrorist organisation, the Attorney-General must be satisfied on reasonable grounds that the organisation:

- 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).

To support the Attorney-General's consideration, ASIO provides a Statement of Reasons. Although generally unclassified, the Statement of Reasons is underpinned by all the relevant intelligence available to ASIO, all of which is available to the Attorney-General. The statement is prepared in consultation with DFAT, AGD and the Australian

Government Solicitor. The Parliamentary Joint Committee on Intelligence and Security reviews each proscription listing.

The proscription of groups is kept under constant review, both in terms of groups to be added to the list, and removed. A group does not need, however, to be proscribed in Australia to be considered by ASIO, Australian courts, or the international community, as a terrorist organisation.

Groups proscribed, re-listed and delisted in Australia in 2009–10

In 2009–10, one new group was proscribed and four groups were relisted.

The proscription of al-Shabaab occurred on 21 August 2009, after the group met the legislative test for proscription as a terrorist group under the *Criminal Code Act 1995*. ASIO commenced the proscription process against al-Shabaab in February 2009 when al-Shabaab escalated its jihadist campaign against the Somali Transitional Government and openly announced its links to al-Qa'ida. These two developments constituted, in ASIO's judgment, sufficient evidence to trigger consideration for the legislative proscription of al-Shabaab as a terrorist organisation. ASIO engaged in deliberation with the Australian Government and partner agencies for six months to carefully collate and analyse open source material and intelligence reporting to support its recommendation to proscribe al-Shabaab.

Groups that were re-listed in September 2009 were Lashkar-e-Tayyiba, Hamas's Izz al-Din al-Qassam Brigades, Palestinian Islamic Jihad and the Kurdistan Workers' Party (PKK).

A list of proscribed terrorist organisations as at 30 June 2010 is at Appendix C.

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

In 2009–10, ASIO worked closely with the Department of Health and Ageing in providing advice on terrorist interest in, and any attempts to acquire, biological agents. This contributed to the development of a framework for authorising access to security sensitive biological agents.

ASIO also provided regular Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) weaponry threat briefings to key stakeholder bodies, including the National Counter-Terrorism CBRNE Security Sub Committee and National Government Advisory Group on Chemical Security.

ASIO continued to work with relevant policy agencies to improve industry and public reporting of suspicious incidents relating to CBRNE materials, for example, through contributing to the explosive precursor awareness campaign launched by the Attorney-General in 2009.

In 2009–10, ASIO published regular Threat Assessments on the threat to Australia's domestic security from chemical and biological terrorism. Unclassified CBRNE-related reports were posted on the Business Liaison Unit (BLU) website, including an unclassified Threat Assessment tailored for the chemical industry. One of the most widely accessed BLU documents, the report received considerable positive feedback.

Security Assessment Advice

ASIO's security assessment function is an important component of Australia's national security defences. It provides a mechanism for 'security' (as defined in the ASIO Act) to be considered in certain regular government decision-making processes (defined as 'prescribed administrative actions' in the ASIO Act). For example, in the issuing of passports, granting of visas, granting of access to sensitive government information (security clearances), and access to restricted areas such as ports and airports and sensitive goods such as ammonium nitrate.

Security Assessments are not, however, an end in themselves. Consistent with ASIO's role as an intelligence agency, they are a means by which ASIO provides advice. And they only consider factors related to 'security', which in practice is usually terrorism, other forms of politically motivated violence, espionage and foreign interference, and threats to Australia's territorial and border integrity.

Security Assessments are not criminal or character checks, and factors such as criminal history, dishonesty or deceit are only relevant to ASIO's advice if they have a bearing on security considerations. Character is not itself sufficient grounds for ASIO to make an adverse security finding.

Most ASIO Security Assessments are made at the request of another department or agency, though ASIO can, and particularly in relation to passports does, issue assessments as a consequence of an ASIO intelligence investigation. Security Assessments can include a simple check of personal details against ASIO's intelligence holdings, or an in-depth intelligence investigation to determine the nature and extent of an identified threat to Australia's national security. Each Security Assessment is handled on a case-by-case basis.

Upon making an assessment ASIO may provide:

- non-prejudicial advice, which means that ASIO has no security-related concerns about the proposed 'prescribed administrative action';
- a qualified assessment, which generally means that ASIO provides to the agency concerned information about the assessment subject relevant to security, but is not making a prejudicial recommendation in relation to the 'prescribed administrative action'; or

- an adverse assessment in which ASIO recommends that a 'prescribed administrative action' be taken (cancellation of a passport, for example), or not taken (declining access to a security controlled area, for example).

The consequence of an ASIO Security Assessment depends on the purpose for which it is made and the associated legislation, regulation or policy. In some cases decision-makers are obliged to take (or are prevented from taking) actions because of an ASIO Security Assessment — such as granting visas to travel to, or remain in, Australia. In other cases the assessment is only a single component to be considered among a range of other factors, for example, for granting access to national security information. In all cases, ASIO itself is not permitted by the ASIO Act to take any administrative action in relation to the assessment subject.

Visa Security Assessments

Any person applying for a visa to travel to, or remain in, Australia may have the application referred by DIAC to ASIO for a Security Assessment. Given the large volume of visa applications, it is not practicable for each one to be assessed by ASIO. A risk-managed referral framework has, therefore, been developed so that applications more likely to be of concern are drawn to ASIO's attention. Still, ASIO assesses many thousands of visa applications annually.

In most visa categories, a visa may not be issued (or must be cancelled) where ASIO determines the applicant to be directly or indirectly a risk to 'security' (as defined in the ASIO Act). The enabling legislation in this instance is the *Migration Act 1958*, specifically the *Migration Regulations 1994* and public interest criterion 4002.

Separately to visa application referrals from DIAC, ASIO's security intelligence investigations will from time to time determine that the holder of a valid visa to Australia (who is sometimes already in Australia, and other times overseas) presents a risk to Australia's security. In such circumstances ASIO may provide to the Minister for Immigration and Citizenship an adverse Security Assessment, which would lead the Minister to cancel the visa.

ASIO completed 38,438 visa Security Assessments in 2009–10. Nineteen adverse assessments were made in relation to visas. Fourteen of these adverse assessments were issued on counter-terrorism grounds and five were issued on counter-espionage or foreign interference grounds.

In 2009–10, ASIO diverted resources to undertaking security assessment of Irregular Maritime Arrivals (IMAs) for DIAC. Consequently the resources available to assess protection visa and other refugee referrals were limited and this caseload experienced delays. ASIO continued to work very closely with DIAC to ensure visibility of the overall visa Security Assessment caseload and agree priorities.

Type of entry	Number of assessments completed
Temporary visas	24,208
Permanent Residence	8,624
Onshore Protection	989
Offshore Refugee/Humanitarian	1,795
Irregular Maritime Arrivals	2,822
TOTAL	38,438

Table 1: Visa Security Assessments completed in 2009–10

During the reporting period, ASIO engaged an independent assessor to review ASIO's visa security checking processes. In close consultation with DIAC, ASIO subsequently implemented a number of recommendations designed to improve efficiency of the visa Security Assessment process and better manage risk.

The reduction in the total number of visa Security Assessments by ASIO compared with 2008-09 is a result of improved focus on a smaller number of visas, and represents an attempt to target ASIO's resources in this area. This is reflected in the fact that, despite assessing fewer total visa applications, ASIO has issued an increased number of adverse Security Assessments since the major changes to the referral guidelines (introduced 9 May 2009).

Passport Cancellations

Under the *Australian Passports Act 2005*, ASIO may request on security grounds the Minister for Foreign Affairs cancel an Australian passport, or refuse an application for an Australian passport. In the counter-terrorism context, 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.

In 2009–10, ASIO issued adverse Security Assessments in respect of the Australian passports of eight individuals. The greater number of passport cancellations, compared with 2008–09, reflected an increase in the number of Australians identified as seeking to travel overseas for terrorism-related activities. Australians already overseas were also identified as supporting terrorism and their passports withdrawn on that basis.

In 2009–10, ten individuals, whose passports were previously cancelled or refused by the Minister for Foreign Affairs on advice from ASIO, became eligible to hold a passport following non-prejudicial assessments by ASIO.

Counter-Terrorism Security Assessments

ASIO conducts counter-terrorism checks at the request of AusCheck and the Australian Federal Police (AFP). ASIO completed 98,086 counter-terrorism Security Assessments in 2009–10, 99 per cent of which were completed within five days.

AusCheck refers applicants for Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC) for a counter-terrorism check. ASICs and MSICs ensure that those with access to sensitive air and maritime port areas undergo appropriate background checking. ASICs are administered under the *Aviation Transport Security Act 2004* and associated regulations. MSICs are administered under the *Maritime Transport and Offshore Facilities Security Act 2003* and associated regulations.

ASIO's role in the ASIC and MSIC process is primarily to consider any terrorism concerns. AusCheck coordinates the larger suite of background checks (including criminal history) and assesses the applicant's overall suitability to hold an ASIC or MSIC. ASIO's advice may recommend against the issuance of an ASIC or MSIC if there are assessed security concerns.

ASIO completed 88,367 ASIC and MSIC checks in 2009–10. No adverse or qualified Security Assessments were made.

ASIO provides (via the AFP) counter-terrorism background checks for licensing by the Australian states and territories for access to security sensitive ammonium nitrates (SSANs – used as an explosive particularly by the mining industry, and as a fertiliser in agriculture). Each state and territory has its own licensing regime, consistent with a set of principles agreed in 2005 by the Council of Australian Governments. ASIO may recommend against a license for access to SSANs. ASIO completed 7,803 SSAN checks in 2009–10.

ASIO also provides, via the AFP, security assessment advice on any terrorism concerns for individuals requiring access to the Australian Nuclear Science and Technology Organisation nuclear facility at Lucas Heights. In 2009–10, ASIO completed 1,371 checks. The AFP also requests counter-terrorism checks for people requiring accreditation for special events. During the reporting period, ASIO conducted 322 checks for people requiring accreditation for the Pacific Islands Forum in August 2009 (see Table 2).

Type of check	Number
Aviation/Maritime Security Identity Cards	88,367
Flight Crew	223
Security Sensitive Ammonium Nitrate	7,803
Australian Nuclear Science and Technology Organisation	1,371
Special Event (Pacific Islands Forum)	322
Total	98,086

Table 2: Counter-terrorism checks 2009–10

Personnel Security Assessments

The Protective Security Policy Framework sets out Australian Government policy and guidance on protective security, including policy for the granting of clearances for access to national security classified information. In almost all circumstances a department or agency must request security assessment advice from ASIO as part of their overall consideration of whether or not to grant a national security clearance. In making the assessment, ASIO reviews any intelligence it may hold, as well as considering known security risk factors.

Except for its own staff (and in a limited number of cases where ASIO is the clearance sponsor), ASIO is not the issuing authority for security clearances and it is up to individual departments and agencies to consider ASIO's advice.

ASIO completed 22,343 personnel Security Assessments in 2009–10. ASIO issued one adverse and one qualified personnel Security Assessment in 2009–10 (see Table 3).

From 1 October 2010, all Commonwealth security clearances for access to national security classified information will (except for a few exempt agencies) be undertaken by a single security vetting agency – the Australian Government Security Vetting Agency (AGSVA). The AGSVA will be located in the Department of Defence and will consequently become ASIO's primary client for Security Assessments for national security clearances.

Type of assessment	Number
Confidential	3,052
Secret	11,929
Top Secret	4,931
Top Secret Positive Vet	2,431
Total	22,343

Table 3: Personnel Security Assessments 2009–10

Critical Infrastructure Protection Advice

Critical infrastructure includes physical facilities, systems, information technologies and networks that if destroyed, degraded or rendered unavailable for an extended period, would impact significantly on Australia's social or economic well-being, or affect Australia's defence or national security capabilities.

In close partnership with industry, Australia takes an intelligence-led whole-of-government approach to the protection of critical infrastructure from terrorism. ASIO's role in critical infrastructure protection includes providing strategic Threat Assessments for industry sectors; producing Threat Assessments for specific nationally vital critical infrastructure facilities; delivering classified briefings to Government and private sector critical infrastructure owners and operators; and managing a database of critical infrastructure (on behalf of Commonwealth and state and territory governments).

Critical infrastructure threat advice, primarily through Threat Assessments and classified briefings, helps inform the risk management activities of private sector owners and operators and policy and regulatory activity.

In 2009–10, ASIO produced 25 critical infrastructure protection reports, including seven broad-based strategic threat assessments for industry sectors, and undertook 17 briefing sessions encompassing over 150 government and private sector stakeholders from the transport, energy, water supply, banking and finance and communication sectors.

Advice to Business

ASIO's BLU provides an interface between the private sector and the Australian Intelligence Community. It seeks to provide corporate security managers with credible, intelligence-backed reporting that enables them to brief executive management and staff authoritatively, and to use this knowledge for their risk management and continuity planning. This service is free of charge.

A particular focus in 2009–10 was on raising awareness of corporate security threats drawing on ASIO's physical security experience and capability. This tactical style of reporting included potential threats and mitigation strategies on issues including information, personnel and protective security, and was in addition to the regular threat information sourced from both ASIO and its overseas partner agencies.

In 2009–10, ASIO continued to provide advice to the private sector, including through briefings to industry events that focused on corporate security. As part of its important interface role between the intelligence community and the private sector, in 2009–10 the BLU facilitated six high-level meetings between company chief executive officers and the Director-General of Security.

The BLU website was upgraded during 2009–10, with improved functionality for users. At the end of the reporting period there were more than 200 reports on the BLU website. These reports cover domestic and international security perspectives and general advice about protective security designed to assist risk management decision-making. The BLU website includes reporting on:

- the current security environment;
- terrorist incidents;
- threats to industry sectors;
- 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.

As at 30 June 2010, there were 778 subscribers to the BLU website, covering 227 corporations and a range of government agencies. This is an increase of 33 per cent since 2008–09. Industries such as utilities, transport and banking and finance are the best represented sectors.

The BLU also maintains a register of Australian business interests that helps to protect Australian assets and personnel by keeping track of where public and private sector interests are located around the world. It allows Australian companies, through a secure interface, to record the locations of their overseas staff, facilities and emergency contact details. Using information from the register, ASIO is able to develop a detailed understanding of Australian business operations overseas and provide more targeted security advice and reporting to corporate security managers. At the end of the reporting period the register had over 150 participating companies with over 1,226 facilities registered in 81 countries.

Cyber Security Advice

Increasing reliance on modern information technology and communication systems creates vulnerabilities to cyber intrusions, whether by amateur hackers, criminal gangs or nation-states. For ASIO, cyber intrusions are of concern when they intrude into the national security arena, for example, threatening the integrity of government information systems or nationally significant private sector interests. The September 2009 Distributed Denial of Service attacks launched against government websites by an issue motivated group, 'Anonymous', demonstrated potential vulnerabilities of government websites that can be exploited to hamper government service delivery.

In 2009–10, ASIO expanded its engagement with industry on the threat of electronic espionage, particularly in the resources and energy sectors. ASIO liaised with a small number of private sector companies which were the targets of electronic intrusions. In 2009–10, ASIO sponsored a resource sector information technology forum to deliver high-level briefings on cyber security and espionage threats and mitigation strategies to a range of resource sector companies. The forum coincided with National Cyber Awareness Week.

In 2009–10, ASIO continued to investigate and provide advice on cyber intrusions against, or involving, Australian interests. ASIO worked closely with the Cyber Security Operations Centre in the Defence Signals Directorate, in which key policy and operational agencies are represented, including ASIO, the AFP and Australia's national computer emergency response team — CERT Australia. The Centre provides Government with a greater understanding of cyber threats against Australian interests, and response options for significant cyber events across Government and systems of national importance.

Advice for Special Events

ASIO provides threat assessment and protective security advice for events that may be targets for terrorist attack or violent protest activity. ASIO's strong record of supporting events of international significance means its expertise is increasingly sought out, including by liaison partners.

In 2009–10, ASIO contributed to a number of special events, including:

- Asia Pacific Economic Cooperation forum-related events in Singapore culminating in Leaders Week in November 2009;
- the Commonwealth Heads of Government Meeting in Trinidad and Tobago in November 2009;
- the Parliament of World Religions in December 2009;
- the United Nations Climate Change Conference in December 2009;
- the Winter Olympics in Vancouver in February 2010;
- the Hockey World Cup in India in 2010;
- the Anzac Day commemoration in Turkey in April 2010;
- the G8 and G20 in Canada in June 2010; and
- the FIFA 2010 World Cup in South Africa in June 2010.

In addition, ASIO, alongside other Australian agencies, organisers and international partners began preparation for the Commonwealth Games to be held in New Delhi, India in October 2010 — with a focus on the security environment and likely security threats that may arise prior to and during the Games. ASIO will continue to work with other Australian government agencies and international partners on the provision of Threat Assessments and advice for the security of Australian participants and spectators and the Games in general.

ASIO also began working with United Kingdom agencies to support security planning for the London 2012 Olympic Games.

Involvement in Litigation

ASIO information is often sought by Commonwealth prosecutors and subpoenaed by defendants for use as evidence. It can also form part of civil and administrative legal proceedings, often not involving ASIO directly (for example Freedom of Information applications to other agencies holding ASIO information). Demand for such material has continued to increase dramatically. Much of it is sensitive and some has been collected pursuant to special powers warrants. ASIO accordingly aims to balance protection of officer and source identities, collection methods and capabilities, and domestic and foreign relationships with the need to support prosecutions and other legal processes in the interests of open justice.

In 2009–10, ASIO was involved in over 40 litigation matters, including criminal (in particular terrorism) prosecutions, judicial and administrative review of Security Assessments, and a range of civil actions. Consistent with the significantly higher level of activity experienced every year since 2005, this large number of diverse and complex matters generated a significant work load.

Sydney Pendennis, the longest-running terrorism prosecution in Australian history, concluded in 2009–10. On 16 October 2009, a jury found five defendants guilty of conspiring to do act(s) in preparation for a terrorist act or acts. On 15 February 2010, the New South Wales Supreme Court sentenced them to terms of imprisonment ranging from 21 to 28 years. All have lodged appeals against conviction and sentence.

In August 2009, Melbourne Pendennis defendant Shane Kent, who had pleaded guilty to membership of a terrorist organisation and recklessly making a document connected with preparation for a terrorist act, was sentenced to five years' imprisonment. Along with fellow Melbourne Pendennis defendants Amer Haddara and Abdullah Merhi, Mr Kent has served his sentence[2] and been released on parole.

ASIO continued to support ongoing Commonwealth terrorism prosecutions in Melbourne.

ASIO was also directly involved in two legal matters initiated by Mr Mamdouh Habib:

- Mr Habib's appeal to the High Court of Australia against the November 2007 decision of the Administrative Appeals Tribunal (AAT) upholding an adverse Security Assessment and denying him an Australian passport. In May 2010 the High Court remitted this matter, with the parties' consent, to the AAT for re-hearing; and
- his Federal Court of Australia compensation claim alleging that the Commonwealth defamed him and was complicit in his alleged mistreatment while he was detained overseas between 2001 and 2005. In February, the Full Federal Court of Australia

2. Including time served before sentencing.

dismissed a Commonwealth application seeking to set aside Mr Habib's claims of misfeasance in public office and harassment. Those claims, together with his defamation and complicity claims, are tentatively listed for Federal Court hearing in 2011.

ASIO was also involved in challenges to a number of its Security Assessments. On 30 September 2009, the Federal Court of Australia at Melbourne dismissed three applicants' notices of motion seeking production of ASIO documents. These matters are listed for further hearings in February 2011.

On 18 May 2010, the ACT Court of Appeal upheld former ASIO officer James Seivers's appeal against his conviction for the unauthorised communication of intelligence.

To ensure both its management of legal issues across the Organisation and its support to Commonwealth litigation, ASIO continued to invest in its legal capability. It has established legal teams in Sydney and Melbourne, and has integrated lessons learned from prosecutions and other legal proceedings into its policies and procedures.

Protective Security Advice

ASIO's T4 Protective Security Directorate has responsibility for providing protective security advice to the Australian Government. This work often extends to state and territory governments (and private sector agencies). Protective security advice typically includes physical security, as well as procedural, personnel and information security. This advice can be in the form of Protective Security Risk Reviews (PSRRs), vulnerability assessments or general physical security advice. In addition, T4 also provides a national technical surveillance counter measures (TSCM) capability to contribute to the protection of sensitive discussions.

In 2009–10, T4 Protective Security increased its engagement with foreign government security agencies to enhance information-sharing. This allowed overseas security practices to inform T4's advice in the context of the Australian security environment. It also enabled T4 to provide advice that met and exceeded international standards and continued to enable ASIO to lead government security practices.

Security awareness briefings continued in 2009–10, including through participation in a new program of activity by the Parliamentary Joint Committee on Intelligence and Security to brief Commonwealth Members of Parliament and Senators.

ASIO worked closely with the Department of the Prime Minister and Cabinet and the Attorney-General's Department (AGD) on the 2009 Council of Australian Governments (COAG) Critical Infrastructure Review, to drive outcomes that ensure continued quality, timely and targeted products and briefings on the security environment for critical infrastructure stakeholders.

The year saw substantial engagement with relevant government agencies in providing e-security advice, and in policy development relevant to the National Broadband Network.

Reflecting an increase in stakeholder understanding of the security environment, and in particular the threat posed from terrorism, ASIO diversified its critical infrastructure work to address a wider and more complex range of subjects and topical issues. Demand for ASIO's protective security advice from Government and industry is expected to remain high.

Protective Security Risk Reviews (PSRR)

T4 contributes to the protection of Australia's nationally vital critical infrastructure through the conduct of PSRRs. These PSRRs, as mandated by COAG, are undertaken in accordance with recognised Australian and international risk management standards.

A T4 staff member inspecting a vehicle access control gate as part of a security vulnerability assessment

Drawing on information available from specialist areas within ASIO, T4 Protective Security has been able to analyse risks more accurately, and ensure a consistent approach to recommended security solutions, commensurate with the expected level and type of threats. In 2009–10, ASIO completed seven PSRRs, and three vulnerability assessments.

A review of the T4 risk management methodology was conducted in 2009–10. This review decreased the level of subjectivity inherent in assessing risk, and increased the transparency behind the risk analysis. ASIO's PSRRs now provide critical infrastructure owners with a more comprehensive understanding of the reasoning behind T4's protective security recommendations. The result is a more focused security solution for critical infrastructure, which contributes to the continued protection of Australia's national interests.

Top Secret Certifications

ASIO is the sole agency responsible for the certification of all Australian top secret facilities, as mandated by the *Australian Government Protective Security Manual*. This arrangement ensures a consistent approach using sound risk management principles. In 2009–10, ASIO provided advice on the construction of top secret areas for government agencies, and those private sector agencies that directly support government functions. ASIO certified 28 Top Secret facilities during the reporting period.

Security Equipment Evaluations

On behalf of the Security Construction and Equipment Committee (SCEC), ASIO tests and evaluates security products for use by Australian government facilities and critical infrastructure. These products must meet specific performance criteria in order to be included in the SCEC security equipment catalogue. Requirements for the evaluation of particular types of equipment, and the levels of resistance they offer, are dynamic and as such, there remains a heavy reliance on SCEC and ASIO to meet the demand and to remain at the forefront of evaluation techniques.

In 2009–10, ASIO completed 14 security equipment evaluations; 18 locksmith evaluations; 19 container maintenance evaluations; two courier evaluations; and three classified waste service evaluations.

Training for Agency Personnel

In 2009–10, ASIO's T4 Protective Security Directorate provided comprehensive training to Australian Government Agency Security Advisers and agency security personnel. ASIO delivered three Agency Security Adviser courses (48 participants in total), providing participants with the skills and knowledge required to effectively manage their own department's security responsibilities. ASIO also provided six training courses for AGD's Protective Security Training Centres (96 participants in total).

Technical Surveillance Counter Measures Services (TSCM)

ASIO's TSCM team contributed to the protection of national security and sensitive discussions throughout Australia in 2009–10. Using sophisticated equipment and specialist techniques, ASIO's TSCM team conducted monitoring and electronic surveys to detect technical attacks.

TSCM team members took part in a major multi-national technical security training and capability development exercise. The exercise used scenarios which were focused on operational security.

Ministerial Office Security Reviews

As a consequence of a security review in 2000 by the Inspector-General of Intelligence and Security, ASIO examines on a regular basis the security status of ministerial offices (with a focus on the protection of classified information) and provides recommendations for improvement. These reviews are undertaken on two occasions during the life of the Parliament.

During 2009–10, ASIO commenced the second round of reviews for the current parliamentary period, and completed six reviews.

Contact Reporting Scheme

In accordance with the requirements of the Australian Government Contact Reporting Scheme as outlined in the *Australian Government Protective Security Manual*, ASIO investigates and analyses reporting from Australian government employees, particularly those who hold security clearances, on suspicious, unusual or persistent contact with foreign nationals that may indicate efforts to obtain unauthorised access to sensitive information. ASIO engages regularly with agencies to promote awareness of the important role of the Scheme in protecting Australian government interests.

National Classification System

The Attorney-General launched a new Protective Security Framework in June 2010. This followed a major review of protective security policy in 2009–10, including a review of the security classification system. The former system divided information into non-national and national types with sub-classifications. As the interpretation of national security has broadened over time, in particular to encompass additional areas such as transnational crime and border protection, the classification division was no longer practicable. ASIO participated in the review to identify a streamlined National Classification System to replace the existing system and provide a more effective and comprehensive approach to Australia's protective security framework.

Security Intelligence Investigations and Capabilities

ASIO's operating environment is increasingly demanding — threats from non-state actors are now more likely; geography and borders mean little to those who threaten Australia; and a 'home-grown' threat, albeit usually influenced from overseas, is just as likely as an imported one. This underpins the importance of Australia's intelligence and security agencies working together as a single, flexible and responsive capability, able to respond wherever the threats to Australia or Australian interests emerge.

In 2009–10, ASIO responded to the increasing complexity of threat by working more closely with its partners in the national security community, including through the exchange of people, information and intelligence and greater sharing of capabilities. ASIO expanded its officer attachment arrangements with Australian agencies to enhance inter-agency understanding, cooperation and information-sharing.

A key initiative in 2009–10 that will serve to enhance coordination of the Commonwealth's operational counter-terrorism activities and improve the effectiveness of Australia's counter-terrorism partnerships at home and abroad was the establishment of the Counter Terrorism Control Centre in ASIO in June 2010.

Counter Terrorism Control Centre

COUNTER TERRORISM CONTROL CENTRE

In February 2010 the Australian Government announced the creation of the Counter Terrorism Control Centre (CTCC) to coordinate, at the tactical and operational level, the Commonwealth's terrorism intelligence and investigative activities.

The CTCC, which is a permanent joint unit within ASIO, brings together, at a senior level, the intelligence collection agencies and the Australian Federal Police. It provides a more flexible and focused counter-terrorism intelligence response and one that harnesses the full capabilities of Australia's counter-terrorism agencies. The CTCC is an important development and a significant evolution in the way counter-terrorism intelligence is managed in Australia.

In responding to the increasingly transnational nature of the threats, including the proliferation of weapons of mass destruction, terrorism and espionage (including via the Internet), ASIO also continued to develop and expand its extensive network of relationships with overseas partners. The extent and depth of ASIO's engagement efforts continue to be crucial to ASIO's ability to counter threats to national security.

Investigations and Operations

Counter-Terrorism

ASIO's counter-terrorism-related investigative and operational activity over the reporting period highlighted two key features of Australia's security landscape – the re-emergence of the trend of Australians seeking to travel overseas to engage in terrorism-related violence and/or training; and the greater accessibility of overseas-based English speaking sheikhs who can serve as a source of inspiration and extremist advice for young Muslims.

ASIO's investigations in 2009–10 again identified Australians who have been radicalised and adhere to an extreme interpretation of Islam, which includes support for the use of violence. In 2009–10, ASIO identified several Australians seeking contact with Islamic extremist religious figures overseas, some of whom have links to terrorism. Of the 38 Australians who have been charged with terrorism offences in Australia since 11 September 2001, most were born in Australia, or have lived here since childhood. This reinforces the significance of the 'home-grown' terrorism threat in Australia.

Much of ASIO's effort on counter-terrorism contributes to countering the outcomes of violent extremism. Through operational work in the field, ASIO aims to understand why people turn to violence and identify the factors that influence some people to adopt a violent extremist ideology. ASIO's work complements the work of other agencies and ASIO is using its knowledge to help them develop strategies to prevent radicalisation.

In 2009–10, ASIO continued its efforts to identify individuals and groups intent on or supporting violence and, in cooperation with the police, prevent any harm.

Counter-Espionage and Foreign Interference

Espionage and foreign interference in, and against, Australia is a constant feature of the security environment where Australian intelligence, military, diplomatic, scientific and commercial information will continue to be targeted.

In 2009–10, espionage and foreign interference continued to threaten the integrity of Australia's national institutions as well as Australia's economic competitiveness and community cohesion. During the reporting period, ASIO issued five adverse visa Security Assessments on espionage and/or foreign interference grounds.

Investigation into cyber espionage activity, which impacts on important national interests in both private and government sectors and threatens Australia's critical infrastructure, is an increasingly important part of ASIO's counter-espionage effort. It complements and builds on ASIO's work on more traditional forms of espionage, which also threaten Australia's information systems. ASIO's response to this resource-intensive threat in 2009–10 included the development of new patterns of international cooperation and liaison.

ASIO's investigations and operations throughout the reporting period highlighted the evolution in the techniques and technologies utilised for espionage. ASIO maintained efforts to build its counter-espionage and foreign interference capability, including through increasingly close engagement with both national and international partners. ASIO worked closely with the Defence Signals Directorate and, in particular, with the newly formed Cyber Security Operations Centre. Raising awareness within both the public and the private sector of the threat posed by foreign espionage or attempts by foreign interests to influence covertly the legitimate political processes in Australia remained an important element of ASIO's work.

Violent Protest and Communal Violence

There was little violent protest activity within communities in Australia in 2009–10.

ASIO observes the provisions of section 17A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), which protects the right of persons to engage in lawful advocacy, protest or dissent. ASIO does not target particular groups or individuals, unless there is a security-related reason to do so – it is behaviour and activity that directs ASIO's interest.

The promotion of communal violence, meaning activities directed at promoting violence between different groups of persons in the Australian community so as to endanger the peace, order or good government of the Commonwealth, is an area of security specifically defined in the ASIO Act and is, therefore, of interest to ASIO. ASIO continues to utilise its Community Contact Program to enhance community leaders' understanding of ASIO's roles and functions, particularly as it relates to violent protest activity. In 2009–10, ASIO maintained a dialogue with representatives of community, ethnic and religious groups to ensure issues of concern to ASIO and the relevant community groups could be aired and discussed directly and discreetly.

ASIO continues to liaise closely with law enforcement agencies and will continue to assess possible threats to the community that may arise through the incitement or promotion of communal violence.

Counter-Proliferation

ASIO's counter-proliferation work focuses on thwarting the efforts of countries or individuals of proliferation concern accessing weapons of mass destruction (WMD) technology and materials.

Australia supports international efforts to prevent the spread of WMD and participates in major arms control treaties and multilateral export control regimes. Australia is a signatory to the United Nations Security Council Resolution 1540 which requires states to criminalise the proliferation of WMD, enact strict export controls and secure sensitive materials.

Counter-Terrorism Response

In 2009–10, ASIO worked with the Australian Federal Police (AFP) to develop the Commonwealth Technical Response Capability (CTRC), effective from 1 July 2010.

The CTRC will provide state and territory law enforcement agencies with the ability to draw on the technical resources of ASIO and the AFP at short notice in circumstances of urgency (such as a terrorist incident) or during peak requirements (such as a major event).

Capabilities

ASIO is a key component of Australia's national security defences – it is vital to identifying, investigating and preventing threats, and central to an effective government response in the event that threats are realised. In 2009–10, ASIO continued to test and update its capability to enable it to respond rapidly to the complex and evolving challenges of the security environment.

ASIO has no executive powers – its officers do not carry weapons and do not have powers of arrest. ASIO's strength lies in its intelligence collection capability, which is underpinned by a range of sources of information including covert human sources, authorised warrant operations and surveillance. ASIO works in close partnership with the Australian community against those who pose a threat to the security of Australia and Australians. In 2009–10, ASIO continued to receive valuable assistance from many areas of the community, including through its long-term engagement with influential community and religious figures and associations.

ASIO's investigative and operational activity is characterised by a graduated approach – security intelligence is collected according to the principle of proportionality, whereby the means for obtaining information is proportionate to the gravity of the threat posed and the probability of its occurrence. ASIO officers undertake their duties methodically, deliberately and with great regard for the personal and collective rights of all Australians.

In 2009–10, ASIO continued to build its human intelligence capability, including through the implementation of a strategy to enhance ASIO's human intelligence work. The maintenance and development of ASIO's physical surveillance and language capability were also priority areas for growth in 2009–10. During the reporting period, ASIO strengthened its foreign language capability, including by enhancing relationships with key domestic and foreign partners and streamlining processes to maximise efficiencies in the processing and dissemination of foreign language product. Maintenance of ASIO's physical surveillance and language capability, including through the recruitment of linguists and surveillance officers, remained challenging and resource-intensive.

ASIO also maintains an open source intelligence capability through its Research and Monitoring Unit (RMU). In 2009–10, the RMU's 24/7 all source monitoring and alert

capability continued to support ASIO's security intelligence activity, including through its support to investigative and operational activity.

ASIO's cooperation and collaboration, both nationally and internationally, remains critical to maintaining and enhancing ASIO's investigative and operational capability. In 2009–10, ASIO increased its investigative capability through the establishment of several new liaison relationships with public and private sector agencies, including in the aviation and maritime sectors. ASIO's overseas liaison network remained a critical component of its intelligence collection capability. It helps discover and respond to threats to Australia and the lives of Australians wherever they might arise – whether inside or beyond Australia's borders.

International Engagement

ASIO has maintained an overseas presence since 1951. The diversity of threats Australia faces means that ASIO's collection and analysis capability today is more reliant than ever before on the cooperation of overseas partners. The international dimension of ASIO's work is particularly important because many security threats have their origins in other parts of the world.

At 30 June 2010, ASIO had liaison relationships with 329 security, intelligence and law enforcement agencies in 123 countries around the world. ASIO's overseas liaison posts contribute to the exchange of a high volume of security intelligence reporting from a wide variety of sources and pursue active engagement with a growing range of international partners. Liaison with overseas services is an important source of intelligence for Australia across a wide spectrum. ASIO's program of international engagement covers not only counter-terrorism but also counter-espionage, counter-proliferation, training and technical exchanges. ASIO engages with foreign services on a range of matters including security intelligence analysis, operational cooperation, capability enhancement and training.

Intelligence-sharing between countries is critical to identifying and preventing terrorism and other security threats, and underpins the importance of efforts to foster intelligence linkages with international partners. ASIO has mature and dynamic intelligence-sharing relationships with agencies in key countries, especially the United States of America, the United Kingdom, Canada, New Zealand and key European, Asian and Middle Eastern partners. These partners are particularly attuned to passing threat information relevant to Australian interests.

International Engagement — counter-terrorism capacity-building training

In 2009–10, ASIO continued to provide training to overseas intelligence and security agencies, including under the auspices of the Counter-Terrorism Intelligence Training Program (CTITP). Established in 2005, CTITP delivers counter-terrorism training and capacity-building to enhance counter-terrorism cooperation with, and between, partner agencies. Requests for CTITP's training programs from foreign partners have continued to grow as have the range of partners seeking assistance. In 2009–10, CTITP delivered training to the intelligence and law enforcement agencies of 23 countries. Delegates from 24 intelligence and security agencies from 14 countries attended CTITP's annual International Counter-Terrorism Seminar in 2009–10. These counter-terrorism and capacity-building initiatives have enhanced the counter-terrorism capability of overseas partner agencies, including through encouraging inter-agency cooperation and information exchange.

Special Powers Under Warrant

The ASIO Act and the *Telecommunications (Interception and Access) Act 1979* (TIA Act) enable ASIO, subject to a warrant approved by the Attorney-General, to use methods of investigation such as telecommunications interception and access, listening devices, entry and search of premises, computer access, tracking devices and examination of postal and delivery service articles.

The ASIO Act also enables ASIO, with the Attorney-General's consent, to seek warrants from an independent issuing authority (a federal magistrate or judge) for questioning of persons for the purpose of investigating terrorism. The warrants may authorise police officers to detain persons in limited circumstances. Any questioning pursuant to a questioning, or questioning and detention warrant must be undertaken in the presence of a prescribed authority (a former superior court judge, a current state or territory judge, or the President or Deputy President of the Administrative Appeals Tribunal) under conditions determined by that authority. The Inspector-General of Intelligence and Security (IGIS) has a statutory right to attend during any questioning or detention under the warrant. In 2009–10, one questioning warrant was issued. No questioning and detention warrants were issued for this period (see Appendix D).

Only the Director-General of Security may seek a warrant. A written statement, specifying the grounds on which it is considered necessary to conduct an intrusive investigation, must accompany each warrant.

ASIO warrants are issued for specified 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 ASIO warrant material and conducts regular and frequent inspections of ASIO's 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 warrants.

Technical Collection

In 2009–10, ASIO made significant gains in the development and delivery of its technical collection capability through close cooperation with national and international partners including industry.

ASIO continues to invest in the development and deployment of technical collection capabilities. These provide important sources of information in all areas of ASIO's intelligence collection. Consistent with all ASIO collection activities, these capabilities are exercised in strict observance of the principle of proportionality. Intrusive activity such as the use of telecommunications interception, listening devices and other aspects of ASIO's 'special powers' are only exercised when strictly imposed thresholds are reached and only then in accordance with a warrant authorised by the Attorney-General.

Safe and secure technical collection often requires in-house development of sophisticated and specialised capabilities. ASIO has high-end engineering capability in a range of disciplines for this purpose. ASIO works closely with Australian and international partners, both in government and industry, to maximise the effectiveness and efficiency of its complex development work.

Effective technical collection requires close coordination of capability development with the equally specialised operational deployment. ASIO recruits operational staff with well-developed technical skills and further enhances those skills through a range of in-house training and development activity, benchmarked for best-practice with ASIO's peers.

Information and communication technology (ICT) is a field of rapid and constant change. ASIO staff using these technologies in support of technical collection activity maintain and extend their skills through a combination of in-house or industry-based training and academic study.

Telecommunications Interception

ASIO has been designated by the Attorney-General as the Commonwealth lead agency for technical advice relating to telecommunications interception. In this role, ASIO represents the interest of all Australian interception agencies when working with industry to develop interception capability to meet regulatory obligations.

The pace and scale of change in the telecommunications industry is placing considerable strain on all interception agencies to maintain capability in the face of rapid technological advancements. As lead agency, ASIO provides technical advice to the two relevant policy departments which work with industry and agencies to help address challenges: the Attorney-General's Department (AGD), which administers the TIA Act; and the Department of Broadband Communications and Digital Economy, which administers the *Telecommunications Act 1997*.

At the same time ASIO, in partnership with the AFP, is working to provide coordinated technical assistance to other Australian interception agencies. In 2010–11, ASIO will be conducting a pilot study for the establishment of a National Interception Technical Assistance Centre (NiTAC). The NiTAC is planned to provide a central point of reference from which agencies can receive technical assistance to help keep pace with technical change.

In 2009–10, the increasing complexity of Internet applications continued to offer challenges in telecommunications interception. To counter this, ASIO promoted high-level government awareness through briefing programs, devised new processes and initiatives in data exploitation, strengthened partnerships with relevant government partners, and continued enhancement of industry and international partnerships.

ASIO, in its role as lead agency on telecommunications interception, had confidential meetings with a wide range of telecommunications companies. In 2010, ASIO provided industry-wide briefings on some of the challenges of telecommunications interception as part of the AGD-hosted National Telecommunications Interception Conference. This forum also provided the opportunity to discuss development of policy and regulatory issues.

Information and Communication Technology Capability and Connectivity

A significant expansion of ASIO's ICT capability occurred in response to recommendations from the *Review of ASIO Resourcing* conducted by Mr Allan Taylor AM in 2005. ASIO's ICT services and systems have continued to evolve in accordance with the Organisation's intelligence needs. Ensuring ASIO's ICT systems support its work in the immediate term and remain able to keep pace with organisational needs into the future were a key component of ASIO's efforts to enhance organisational capability in 2009–10.

ASIO worked effectively and collaboratively on information technology (IT) issues within the national security community, including as part of efforts to leverage capability across the community. ASIO assisted the National Security Chief Information Officer in the development and formulation of the National Security Information Environment Roadmap, including through the secondment of an ASIO Senior Executive Service officer to the Office of the National Security Chief Information Officer.

In August 2009, ASIO began implementing an updated ICT Strategic Plan. The key elements of ASIO's ICT Strategic Plan are in line with the Government-adopted recommendations from Sir Peter Gershon's 2008 *Review of the Australian Government's Use of Information and Communication Technology*. The Plan continues to drive the Organisation's ICT forward work program. A key element in the plan is the redevelopment of ASIO's records management framework to ensure information held by ASIO, in whatever form, is readily accessible.

As part of its ICT Plan for 2009–13, ASIO commenced and/or implemented a number of projects in 2009–10. These included:

- upgrading ASIO's records management system to allow ASIO to manage and store documents and records in a single system. This will improve ASIO's search capabilities significantly and result in greater efficiencies in the management of ASIO's record keeping responsibilities;
- enhancing ASIO's advanced analytical capability;
- strengthening ASIO's data quality management capability; and
- developing a Case Management System on ASIO's corporate system to facilitate improved accountability, cooperation and accuracy in the management of cases and related activities.

A review of ASIO's ICT Strategic Plan was subsequently undertaken in March 2010.

TOP SECRET Connectivity: TS Enclave

Maintaining information technology systems that have the necessary controls and security to communicate at the TOP SECRET level is expensive, both in the cost of security and the associate resource costs in people. Considerable personnel, security infrastructure and policy is required, which can present a significant barrier to new members of the national security community in building and maintaining these capabilities.

In 2009–10, in order to seek efficiencies of scale, ASIO built and continues to support a TOP SECRET environment on behalf of the Department of the Prime Minister and Cabinet, the Australian Customs and Border Protection Service and the Australian Federal Police. This environment will allow those agencies to communicate and collaborate at the TOP SECRET level and also provide broader access to AICNET. It is anticipated that the TS Enclave, when fully populated, will support 200 users from these three agencies at less cost-per-user to each agency.

TS Enclave Memorandum of Understanding Signing

Maintaining ASIO's ICT capability remains a challenge – enhancements must be achieved in an environment where the pace of technological change continues to accelerate, in an environment of persistent and evolving terrorist and espionage and electronic attack threat and where ASIO has increasing connectivity, collaboration, accountability, litigation and legislative requirements.

Information Technology Traineeship

In 2009–10, six IT trainees were engaged in a two-year structured pilot program, which will conclude in December 2010. On the job training has been provided through scheduled rotations across ASIO, with performance assessment through a structured competencies workbook. Mentoring relationships were established to provide support and guidance to trainees. The trainee pool provides both a feeder group into the IT Officer stream, and additional capability for ASIO's existing IT needs.

Research and Development

ASIO places a strong emphasis on research and development (R&D) and continued to make personnel and financial investments in its R&D capabilities throughout 2009–10.

ASIO's Science Adviser works closely with partners in Australia and overseas to help all parts of the Organisation plan for, and capitalise on, technological advances. Close partnership with the National Security Science and Technology Branch of the Department of the Prime Minister and Cabinet and the Defence Science and Technology Organisation has been important in developing the Science Adviser role in ASIO. ASIO participated in

Australia-wide seminars sponsored by the Department of the Prime Minister and Cabinet, which provided an opportunity to discuss national security research requirements.

ASIO contributed to the development of Australia's first National Security Science and Innovation Strategy and is involved actively in its implementation.

ASIO is increasing outreach and engagement with Australian academic institutions and other research providers, explaining ASIO research and development requirements to encourage application of innovative solutions to national security challenges.

ASIO is fostering a culture of innovation through mechanisms such as its in-house 'innovation challenge', which invites whole-of-agency suggestions to propose ideas to enhance ASIO's technical collection capabilities.

Protecting Capabilities and Information

Those who would threaten the security of Australia or its allies can endeavour to monitor security intelligence activity in order to identify, create and exploit potential vulnerabilities. Protecting ASIO's security intelligence, its sources and the relationships and capabilities which facilitate its collection and analysis from unnecessary exposure 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. In 2009–10, ASIO worked closely with external stakeholders such as the Commonwealth Director of Public Prosecutions and the AFP to ensure a meaningful contribution to Commonwealth litigation within the requirements of the justice process as well as to minimise the risk to ASIO's ongoing effectiveness.

Foreign Intelligence Collection

In the report of the 1984 *Royal Commission on Australia's Security and Intelligence Agencies,* The Hon. Mr Justice Robert Hope noted that he was satisfied Australia had a need to collect foreign intelligence that related to its national security and other national interests, and that it would be highly advantageous for Australia to be able to collect foreign intelligence within its own territory where that was possible. Hope's recommendation was accepted by the Government and the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) was amended to provide the Organisation a specific function of obtaining foreign intelligence within Australia under warrant using ASIO's special powers. That function is enshrined in s17 (1)(e) of the ASIO Act.

The process for acquiring a foreign intelligence collection warrant is set out in s27A and s27B of the ASIO Act. At the request of the Minister for Foreign Affairs or the Minister for Defence, ASIO collects foreign intelligence — intelligence related to the capabilities, intentions or activities of a foreign power — under warrant within Australia. This collection is done in collaboration with the Australian Secret Intelligence Service and the Defence Signals Directorate.

part
three

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.

part four

4

Accountability

ASIO and Accountability

ASIO works to protect Australia and Australia's interests and it operates within strict policies, procedures and legislative parameters. ASIO's accountability regime includes the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), which defines ASIO's specific roles and functions and sets the parameters for ASIO's role in Australia's democracy. The ASIO Act also allows the Attorney-General to issue guidance on the performance of ASIO's functions and powers. The Australian Government, particularly through the Attorney-General, monitors ASIO actions, scrutinises performance and decides what resources ASIO should have. The ASIO Act also emphasises the responsibility of the Director-General of Security for providing impartial advice and states clearly that the Director-General of Security has a special responsibility to ensure ASIO is kept free from any influences not relevant to its functions.

ASIO is subject to scrutiny and oversight by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Inspector General of Intelligence and Security (IGIS). ASIO also appears publicly in Senate Standing Committee on Legal and Constitutional Affairs hearings. Two aspects of ASIO's activities are subject to appeal to the Administrative Appeals Tribunal — Security Assessments and requests under the *Archives Act 1983*.

Attorney-General

Throughout the reporting period, ASIO provided advice to the Attorney-General on a range of investigative, operational, administrative and security issues, including through 285 written submissions, the presentation of special power warrant requests, and oral briefings.

Parliamentary Oversight

National Security Committee of Cabinet

The National Security Committee of Cabinet (NSC) is the Australian Government's peak decision-making body on security-related policy, strategy and resource issues. The NSC determines the strategic direction of Australia's intelligence effort, including resourcing for Australia's intelligence agencies, determining national security priorities, and monitoring performance against those priorities throughout the year. The NSC is supported by the Secretaries Committee on National Security (SCNS). The Director-General of Security participates in NSC meetings and is a member of SCNS.

Parliamentary Joint Committee on Intelligence and Security

The PJCIS reviews ASIO's administration and expenditure, and may also conduct inquiries into matters relating to the intelligence agencies that have been referred to the PJCIS by the responsible Minister or by a resolution from either House of Parliament. The PJCIS is also responsible for reviewing the listing of an organisation as a terrorist organisation under the *Criminal Code Act 1995* (Cth) and reviewing ASIO's questioning and detention powers. The Committee's comments and recommendations are reported to each House of the Parliament and to the responsible Minister.

In 2009–10, ASIO provided a classified report on its administration and expenditure to the PJCIS (*Review of Administration and Expenditure No. 8: 2008–09*). An unclassified version of this report is available on the PJCIS website (www.aph.gov.au/house/committee/pjcis/reports.htm). In addition to written reporting, ASIO appeared in front of a PJCIS hearing to respond to questions on administration and expenditure.

During the reporting period, ASIO provided other classified briefings to the PJCIS, including on the construction of ASIO's new central office. Members of the PJCIS also met with a group of ASIO's Intelligence Officer trainees. ASIO used these outreach activities to provide the PJCIS with further insight into ASIO's operating environment and to introduce the Committee to a broader range of ASIO staff.

Senate Standing Committee on Legal and Constitutional Affairs

ASIO was called to the Senate Standing Committee on Legal and Constitutional Affairs hearings twice in 2010 (Additional Estimates on 8 February 2010 and Budget Estimates 24 May 2010). At both hearings the Director-General of Security was accompanied by ASIO's Deputy Director-General, Mr David Fricker.

ASIO responded to questions on a range of issues including:

- ASIO's detention powers under warrant;
- Security Assessments;
- the *Counter-Terrorism White Paper;*
- national security legislation;
- ASIO's new central office;
- budget and staffing;
- complaints to the IGIS;
- the Counter Terrorism Control Centre; and
- the 2011 Intelligence Review.

ASIO also responded in writing to 22 Questions on Notice.

Mr Fricker also appeared before the public hearing of the Senate Standing Committee on Legal and Constitutional Affairs's inquiry into the *Anti-People Smuggling and Other Measures Bill 2010*, on 16 April 2010.

Inspector-General of Intelligence and Security

The IGIS is an independent statutory office holder who reviews the activities of the agencies of the Australian Intelligence Community (ASIO, the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate and the Office of National Assessments). The IGIS's mandate is to ensure the Australian intelligence agencies act legally, with propriety, comply with ministerial guidelines and directions and respect human rights.

The IGIS is a core component of the rigorous oversight and accountability framework within which ASIO operates. In respect of ASIO, the IGIS has both an inspection and an inquiry role.

Inspection

The IGIS conducts ongoing inspection and monitoring of ASIO activities (particularly operational activities), which include regular reviews of:

- investigation authorisation and warrant documentation;
- the conduct of counter-terrorism, counter-espionage and counter-intelligence investigations, including special powers operations;
- engagement with other Australian agencies, and ASIO's access to their data;
- interactions with international liaison partners and ASIO's communications on Australian citizens and residents to those partners; and
- compliance with legislation, Attorney-General's Guidelines, and internal policies and procedures.

Inquiry

The IGIS has the authority to inquire into public complaints, conduct inquiries referred by Government, and initiate 'own motion' inquiries. At the conclusion of an inquiry, the IGIS reports conclusions and recommendations. While there is no legal obligation for the Director-General of Security to comply with the recommendations, ASIO works collaboratively with the IGIS to resolve issues.

Regular engagement with ASIO's Senior Executive

ASIO coordinates a regular monthly senior meeting with the IGIS that allows an exchange of views on strategic issues of common interest, an opportunity to elevate issues arising out of inspections or inquiries, or for the IGIS to be provided with specific briefings if requested or considered useful by ASIO.

Where appropriate and relevant to issues of legality, propriety and human rights, ASIO consults the IGIS on the development of policy guiding its activities. ASIO, on an ongoing basis, also seeks to provide the IGIS with early advice of emerging issues impacting on the Organisation, to assist understanding of the environment ASIO is operating in and challenges faced. In 2009–10, ASIO consulted with the IGIS in drafting internal policy documents including on ASIO communication with foreign authorities, and the consolidation of ASIO's internal policies and practices prohibiting use or involvement in torture and other cruel, inhuman or degrading treatment or punishment.

Further details can be found in the IGIS's *Annual Report* at www.igis.gov.au.

Internal Audits and Fraud Control

ASIO has an active, risk-based, internal audit and evaluation program. Fourteen audits were completed in 2009–10. No loss of public monies was identified. At the end of the reporting period, three audits were ongoing, carrying over into 2010–11.

All internal audit reports, including recommendations arising, are reviewed by ASIO's Audit and Evaluation Committee. The Committee and relevant work areas accepted all audit recommendations with the exception of one, which was rejected on a sound operational basis and agreed to by the Committee and Internal Audit.

In 2009–10, ASIO's internal audit function received additional resources. This allowed internal audit to expand beyond compliance activities to include a broader range of performance audits focused on ASIO's high risk areas.

There were no suspected incidents of fraud reported in the reporting period. In 2010, ASIO's *Fraud Risk Assessment* was revised in line with Australian Government *Fraud Control Guidelines*, with a new Fraud Control Plan to be implemented in late 2010. In 2009, ASIO completed the Commonwealth Fraud Control Guidelines Annual Questionnaire.

Throughout their employment, ASIO staff participate in regular programs related to values and ethics, accountability, organisational oversight mechanisms, fraud prevention, legislative provisions, personal and professional security practices and occupational health and safety. Importantly, ASIO identifies strongly and aligns with the values and behaviours required of the public sector. In 2009–10, 71 new officers completed induction training and 488 new and ongoing staff completed ASIO's compulsory ethics and accountability workshops.

Audit of Assumed Identities

Cover arrangements and assumed identities are used to prevent compromise of ASIO's activities and to protect the identity of ASIO officers.

The use of assumed identities in ASIO is authorised under the *Crimes Act 1914* (Cth) (Crimes Act), and in accordance with the *Law Enforcement and National Security (Assumed Identities) Act 1998* (NSW). Amendments to Part IAC of the Crimes Act became effective on 19 February 2010.

As required under legislation for both the Commonwealth and New South Wales assumed identity schemes, audits were conducted in January and July 2010 on records of authorisations, variations and cancellations in 2009–10. No discrepancies were detected.

All use of assumed identities by ASIO officers must be authorised by the Director-General of Security or an approved delegate in accordance with the Crimes Act. With the changes to the Commonwealth legislation in February 2010, there will only be an occasional requirement to seek separate approvals under the *Law Enforcement and National Security (Assumed Identities) Act 1998* (NSW). Current NSW authorisations will be managed as legacy items until cancelled, with only a small number requiring ongoing management.

As required by the legislation, a report for 2009–10 on the number of authorisations, the general activities undertaken with the use of assumed identities, and relevant audit results was provided to the IGIS.

Outreach

ASIO has introduced initiatives in recent years to improve accessibility and contact points into ASIO. This will remain an enduring priority and focus. In 2009–10, the Director-General of Security decided, under the provisions of the ASIO Act, to reveal publicly the identity of one of ASIO's Deputy Directors-General, Mr David Fricker. Throughout the reporting period, ASIO engaged in outreach activities to promote understanding of ASIO's unique role, to highlight challenges in the security environment, and to contribute to broader policy considerations and debate. The audience included Commonwealth and state and territory partners through initiatives such as Partnership Forums; academia through seminars; as well as the wider community through ASIO's new website.

Partnership Forum

In 2010, ASIO continued its program of inviting Senior Executive Service officers from partner government agencies to its Partnership Forums (formerly known as the Customer Seminar Program). The forum was expanded in 2009–10 to include a module specifically designed for senior officers, to broaden and strengthen understanding of ASIO roles and capabilities. The forums included targeted presentations and case studies to highlight linkages between ASIO and participating agencies. The Partnership Forums, which complement the ASIO-initiated regular briefing programs for partner agencies, enhanced ASIO's interactions with government agencies and provided senior officers with further opportunities to build and enhance networks.

Academic Outreach

Over the past year, ASIO has widened its range of engagement with Australian universities, research institutions and think tanks. In a complex and dynamic operating environment, ASIO recognises the need to tap a wide range of expertise and knowledge. ASIO is working increasingly with universities to help develop its capabilities through access to applied research and advice, and the delivery of training services and the recruitment of suitably qualified new staff. Exchanges with, and participation in, policy think tanks offers an opportunity to gain wider perspectives and to test the Organisation's strategic thinking.

New ASIO website

A redeveloped modern website (www.asio.gov.au) was launched by the Attorney-General, the Hon. Robert McClelland MP, in 2010.

A number of journalists from the Parliament House Press Gallery attended the launch, which provided an opportunity for journalists to enter ASIO headquarters and meet ASIO staff.

The website has a contemporary design and provides easy-to-access information across a range of topics, including broad details on the nature of ASIO's work.

The careers section of the website provides information about roles within the Organisation and what applicants may expect from the recruitment process. Short videos provide an understanding of a range of roles within ASIO.

Attorney-General, the Hon. Robert McClelland MP (right) and David Fricker, ASIO Deputy Director-General at the launch of the new ASIO website. Source AAP Image/Alan Porritt

Security in ASIO

The information held by ASIO is often highly sensitive in nature and, if compromised, has the potential to damage Australia's national security. These serious ramifications necessitate the need for stringent security practices at both the organisational level and also for each member of ASIO staff.

In the reporting period, ASIO continued to bolster security at ASIO's central office with the introduction of biometric measures to access the building. ASIO also updated internal

security instructions documenting sound security practices and requirements for everyone working in ASIO.

The protection of information held by ASIO is ultimately the responsibility of every member of ASIO staff. For this reason all ASIO permanent staff must maintain a security clearance of Top Secret. In the reporting period ASIO conducted 291 probation revalidations and 149 full re-evaluations.

Counter-intelligence remains key to protecting ASIO and its staff from security threats. Reporting mechanisms identified similar security issues as the previous reporting period, specifically individuals impersonating ASIO staff and the unauthorised filming of ASIO premises and staff.

part
five

5

Corporate Management

People

During 2009–10, ASIO staff maintained their high level of commitment and flexibility to respond effectively to changing priorities and emerging issues. ASIO staff participated proactively in the national security community and broader Government through a wide array of attachments outside of the Organisation, and participation in formal leadership and management programs.

Recruiting ASIO's People

As a consequence of the *Review of ASIO Resourcing* conducted by Mr Allan Taylor AM in 2005, ASIO's recruitment efforts have focused on achieving a substainital workforce growth program to culminate in staff numbers reaching 1,860 full-time equivalent (FTE) during 2011. As a result of shortfalls on net recruitment during 2009-2010, ASIO will not reach this target until the 2012-2013 budget cycle.

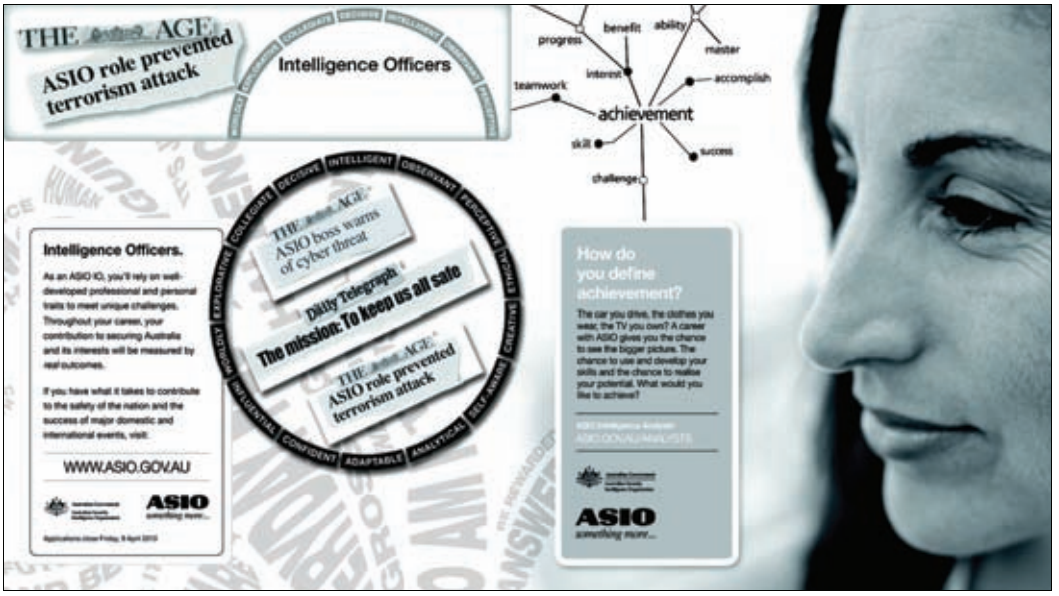
As at 30 June 2010, ASIO employed 1,692 staff which represents 1,600 FTE. In 2009-10, ASIO appointed 117 employees, with 79 per cent engaged on an ongoing basis. ASIO experienced a relatively low separation rate in 2009-10; ASIO's separation rate of five per cent compares favourably with the Australian Public Service (APS) rate of seven per cent.

Throughout the reporting period, recruitment activities focused on building intelligence and technical capabilities, and essential enabling functions. Recruiting high-calibre staff suitable to work in ASIO's high security environment – particularly in the more specialised areas of intelligence analysis and collection – proved particularly challenging. Difficulties in finding suitable candidates to undertake work in these specialised areas, coupled with the rigorous and lengthy security vetting of potential new staff, were key contributing factors to ASIO not meeting its ambitious 2009–10 growth targets.

ASIO is currently implementing recommendations of a commissioned independent review on recruitment and vetting. These measures have both a short and long-term focus, and will improve selection and vetting processes, management of resources and return on investment in each stage of the recruitment process. While increasing staffing levels to reach the final end-point, ASIO's strategic planning and people strategy initatives will enable the Organisation to transition into a workforce consolidation phase. ASIO's workforce statistics are at Appendix E.

Talent Acquisition

ASIO has introduced changes to the manner in which it engages with prospective applicants. This includes a larger and broader online presence which appeals more effectively to prospective employees. In 2009–10, recruitment media planning, coupled with online media (such as the placement of banner advertising on social networking site Facebook) will assist ASIO to attract and source job seekers in the future. ASIO's expenditure on recruitment advertising decreased from $1.962m in 2008–09 to $1.250m in 2009–10.



ASIO's recruitment advertising, 2009–10

Development of Selection and Assessment Methodologies

ASIO remains committed to developing and maintaining transparent, evidence-based selection methodology throughout the staff selection process. In 2009–10, ASIO enhanced its assessment centre activity, including a significant redesign of the Intelligence Officer and Intelligence Analyst programs. These changes allow ASIO to observe applicants in challenging and realistic workplace settings with scenario activities aligned more closely with applicable competencies. The implementation of a recruitment validation and process effectiveness project will provide further impetus towards ASIO's objective of industry best-practice by introducing an improved system of evaluation and refinement during 2010–11.

In 2009–10, an independent review was commissioned to identify options to enhance the efficiency and effectiveness of ASIO's recruitment processes, and to improve return on investment at each stage of the process – while maintaining current standards. Recommendations from this review will be assessed and implemented during 2010–11.

Developing ASIO's People

ASIO aims to build an adaptable, responsive and capable workforce to meet a wide range of challenges including rapidly shifting priorities in the security environment. ASIO invested $16.7m in people development during 2009–10, an increase of 38 per cent on the previous year. People development will continue to be central to the Organisation's strategic focus.

ASIO's core business of collecting and assessing information relevant to security generates a requirement for staff to develop and enhance specialist skills. This includes language skills and an increasingly wide range of skills relevant to professional disciplines such as information security, critical infrastructure protection, telecommunications and engineering, data analysis and information management. Investing in these skills has strengthened ASIO's ability to respond to the challenges of the security environment.

In 2009–10, ASIO began developing a new People Capability Framework. This framework defines key capabilities critical to the success of ASIO in order to enhance effectiveness across the Organisation, in line with the strategic imperative to develop ASIO officers' skills to increase flexibility and responsiveness within the Organisation. The framework will also help ASIO create better linkages and synergies with other agencies, as well as underpin a number of systems, including career planning; informing the development of training initiatives; improving recruitment through consistent criteria and terminology; and informing performance management discussion.

Staff Placements

In 2009, ASIO developed a strategically-focused internal framework to ensure staff are deployed to work areas according to organisational priorities and requirements, and to encourage career growth and diversity. The framework is a successful talent management and retention strategy for ASIO officers, and enhances the Organisation's ability to adapt to the changing security environment.

ASIO also encourages personnel exchanges with Australian and international partners. The number of attachments to and from other agencies increased in 2009–10 as ASIO continued to build on its outreach and engagement strategy. In 2009–10, there were attachments to and/or from:

- the Attorney-General's Department;
- the Australian Crime Commission;
- 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, Transport, Regional Development and Local Government;
- the Department of the Prime Minister and Cabinet; and
- the Office of National Assessments.

In addition to fostering collaboration and interoperability, attachments provide an opportunity for ASIO officers to obtain diverse career experiences and develop and enhance capabilities.

Training and Professional Development

ASIO's internal training, 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 and cultural awareness.

In 2009–10, ASIO's programs were aligned with development programs across government, notably the establishment of the National Security College at the Australian National University, as well as through the programs, seminars and other events sponsored by the Australian Public Service Commission. During the reporting period, approximately 100 ASIO officers attended orientation or senior officer courses run by the national security community designed to foster cooperation and mutual understanding of roles and functions within the community.

ASIO's learning culture aims to foster professionalism. During 2009–10, the Organisation provided assistance to 270 officers for external study programs across a range of disciplines. Eighteen officers undertook language development training that was fully, or partly, funded by ASIO. Assistance included additional leave to attend classes and examinations and financial assistance for continuation of study considered to be particularly relevant to the needs of the Organisation. ASIO's study assistance program forms a key component of ASIO's people retention, rewards and recognition strategy. In addition to study assistance, 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's leadership programs are designed to build skills required for the public sector, not just for ASIO. ASIO's programs connect well to external programs and develop its leaders as individuals with the resilience and dexterity to manage and lead. In 2009–10, ASIO implemented a residential leadership program that challenges a 'vertical slice' of ASIO's leadership ranks to work across internal boundaries to undertake and implement projects that further the achievement of ASIO's strategic goals. ASIO's seminar series reaches out to Government and academia to source presenters who can challenge and contextualise ASIO's work with reference to broader government priorities, as well as providing insights and techniques for connecting within Government. This seminar series is a new initiative that commenced in May 2010 and will continue on a monthly schedule.

ASIO's Leadership Strategy

ASIO's Leadership Strategy was launched on 5 March 2010, and is a key initiative that aligns ASIO with the reforms related to providing strong leadership and strategic direction, flagged by *Ahead of the Game: BluePrint for Reform of Australian Government Administration*.

The strategy focuses on three key platforms – programs, seminars and systems – and emphasises the importance of leadership by all ASIO staff to position the Organisation to meet challenges of the current and future operating environment.

The leadership program is building leadership capability and driving strategic direction to position ASIO for the future. This includes engagement with the Director-General of Security and ASIO's Senior Executive and culminates with the establishment of 'Think Nets' – a group of peers from across the Organisation working together on key leadership projects supporting the strategic approach to ASIO's mission. All leaders in ASIO will participate in the program in the period to 2012.

Monthly seminars invite all staff to engage with a diverse range of leaders from Government, academia and the intelligence community as well as the private sector to consider topics related to leadership, national security and government issues. Speakers to date have provided insight into the global political landscape, the global security environment and broad public sector reform.

eLearning

ASIO invested $100,000 in eLearning capability in 2009–10. ASIO strengthened eLearning during 2009–10 with new modules including corporate and specialised ASIO programs. eLearning course content and learning outcomes are developed with the respective technical specialist areas in ASIO. This model ensures ASIO officers can access relevant self-paced training material at their desks, at a time that suits their work priorities and that is designed and delivered professionally to achieve learning outcomes.

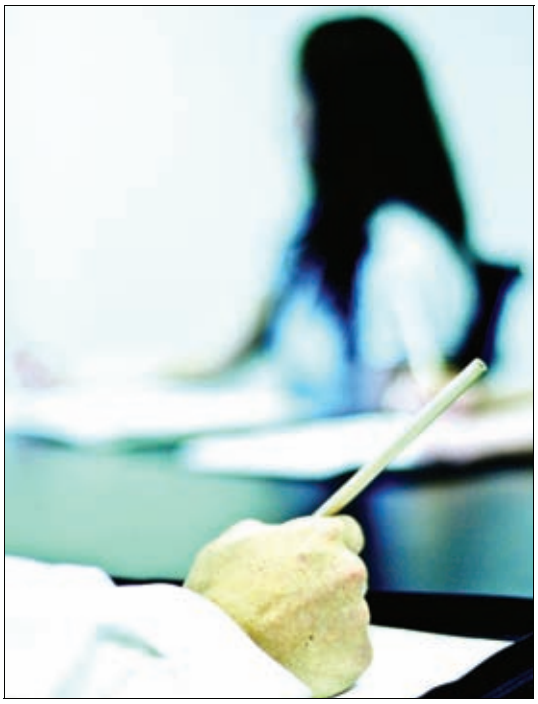
ASIO has used its eLearning expertise to assist other agencies in the national security community to deliver training packages across the community. For example, assistance was provided in the delivery of a training module that forms part of an orientation course for members of the Australian Intelligence Community.

Intelligence Training

In 2009–10, ASIO introduced a revised intelligence training program – the Intelligence Development Program. The program represents the Organisation's major training and development investment of $7.9m in 2009–10.

During the Intelligence Development Program, Provisional Intelligence Officers spend six months in training modules and six months attached to work areas. Throughout the program, skills acquisition and skills development are monitored closely by training staff, workplace coaches and line managers. On successful conclusion of the program, officers have their employment with ASIO confirmed and are posted to one of ASIO's intelligence business areas, usually in an intelligence collection or intelligence analysis role. A variety of mentoring and coaching arrangements are in place to ensure ASIO officers are supported through the program, both during training and while posted to the workplace.

In 2009–10, intelligence training modules were offered to staff across ASIO, regardless of their job families, allowing ASIO to diversify further the skill set of its workforce to respond to changes in priorities and to deal with new priorities as they emerge. Expanded intelligence training increased ASIO's ability to operate joint teams by building a common understanding of the way ASIO's intelligence collection activities are carried out.



Supporting and Retaining ASIO Staff

In 2009, ASIO established a Staff and Family Liaison Office (SFLO) to provide staff and immediate family members with access to a range of services and support, acknowledging employment with the Organisation is a lifestyle and career choice that, at times, impacts family life. Services provided by the SFLO range from routine relocation assistance and advice through to 24-hour crisis support and referral. The office has been particularly beneficial for Provisional Intelligence Officers and their families as many officers join the Intelligence Development Program from other parts of Australia.

In 2010, approximately 200 staff and family members attended an inaugural family information evening. Monthly meetings for staff on parental leave were launched in 2010. These meetings assist in reducing the sense of isolation experienced by some staff on leave and provide an informal networking opportunity. Sessions on topics, including 'adapting to part time work', are delivered during these meetings. Feedback on this initiative indicated participants feel supported and share a greater sense of community and connectedness.

The New Employee Support Officer (NESO) program links new staff members with an experienced officer to assist them to settle into the Organisation and provides an informal mechanism of support and guidance. A review of the NESO program during 2009 found it remained beneficial in assisting the successful integration of new staff into the Organisation.

Strategic Human Resources Capability Framework

In May 2010, ASIO commenced a review of current and future people management and development services and programs to ensure activities are effectively building and enhancing the capability of its people and supporting organisational objectives; and to ensure services are operating efficiently. One of the outcomes of the review was an holistic Strategic Human Resources Capability Framework, which will be implemented during 2010–11. This framework will provide a strategic overarching approach to people functions by linking all activities and outcomes (such as recruitment, learning and development, strategic workforce planning, and performance management) in an integrated system aligned with business strategy.

Strategic Workforce Planning

In 2009–10, ASIO commenced development of a Strategic Workforce Plan mapping capability supply and demand drivers. As a key component of ASIO's Strategic Human Resources Capability Framework, the Strategic Workforce Plan will contribute to talent acquisition, management and retention strategies and systems. It will ensure ASIO is positioning itself to continue to have a highly capable workforce able to respond effectively to internal and external drivers, and continue to meet government and community expectations. The plan will continue to be developed in 2010–11.

Employment Framework

ASIO's Enterprise Bargaining Agreement commenced on 1 January 2010 with a nominal expiry date of 30 June 2011. The Agreement complies with wider Australian Public Service parameters and aligns with public sector enterprise bargaining rules. The Agreement received 71 per cent acceptance from ASIO staff. Key outcomes of the Agreement include the development in 2010–11 of a Specialist Position Framework to capture critical capability requiring technical expertise, the creation of a Phased Retirement Package as part of a 'Mature Worker's Strategy' and the development of a new Performance Management Framework.

Performance Management

In 2009–10, ASIO developed a blueprint for a Performance Management Framework that promotes and enhances excellence at all levels. The framework, to be implemented in 2010–11, augments linkages between formal and informal feedback systems, performance metrics, learning and development opportunities and workforce planning to foster and maintain short and long-term capability. Senior Executive Service (SES) performance agreements were reviewed to ensure clear connections with ASIO's strategic goals.

Sustainable Excellence in ASIO is a blueprint to deliver an integrated Performance Management Framework beyond people management and performance monitoring. The blueprint is ASIO's commitment to drive a performance management culture beyond simplistic people management strategies to an Organisation that has advanced, integrated performance management approaches that capitalise on the initiatives delivered in line with ASIO's strategic goals.

Diversity, Harassment and Discrimination

As part of maintaining a harassment and discrimination free work environment, ASIO established a Complaints and Appeals Framework to ensure the timely and effective resolution of staff concerns. The framework includes the appointment of an independent Ombudsman to resolve issues impartially, informally and in a timely manner.

During 2009–10, the Harassment Contact Officer Network was reviewed to ensure appropriate coverage across ASIO. All Harassment Contact Officers undertook specialist training with an external provider.

The Organisation's *Workplace Diversity Program*, *Disability Action Plan* and *Reconciliation Action Plan 2009–12* continued to ensure ASIO promotes an inclusive work environment for all staff. Throughout 2009–10, ASIO continued to meets its responsibilities under the Commonwealth Disability Strategy.

In 2010, ASIO appointed its first external Ombudsman as part of the Organisation's commitment to ensuring it has robust mechanisms to deal with staff concerns and complaints impartially, informally and quickly.

Occupational Health and Safety

ASIO established a dedicated Injury Management team to manage injured staff, and to assist in reducing long-term injury costs. By implementing initiatives — such as corporate processes for injury management and rehabilitation, engaging injured staff early with effective return to work programs, and providing staff and line managers with ongoing case management support — there was a significant reduction in the likely future costs of injuries sustained in 2009–10 compared with the previous year. ASIO had a 56 per cent reduction in the number of compensable injuries during 2009–10 compared with 2008–09. This reduction, combined with more efficient and effective case management practices, led to a 90 per cent reduction in the total weeks of incapacity paid compared to the average total paid for the previous four years. ASIO continued to build a productive relationship with Comcare and to explore strategies aimed at reducing further the personal and organisational costs of work-related injuries.

During the reporting period, seven incidents were notified to Comcare under section 68 of the *Occupational Health and Safety Act 1991*, five of which related to exposure to a hazardous substance. There were no investigations conducted under section 41, or any notices issued under sections 29, 46 and 47 of the *Occupational Health and Safety Act 1991*.

ASIO's Injury Prevention team focused on creating an integrated safety culture across the Organisation. A major component of this initiative was the continuation of risk assessments for work areas and the provision of support to implement subsequent recommendations. In addition, ASIO progressed the implementation of medical standards for both existing staff and applicants for certain job categories. These standards will set clear health parameters, identify potential health concerns in a timely manner, and mitigate risks to the Organisation and staff.

The benefits of a robust safety culture are promoted through health and safety initiatives such as Health Week and workplace risk assessments. The renewed focus on ASIO's safety culture is expected to translate into increased engagement across the Organisation in the day-to-day health and safety of ASIO staff.

ASIO's Health and Safety Management Arrangements, required under subsection 16 (2) of the *Occupational Health and Safety Act 1991*, were reviewed in 2009–10. ASIO's commitment to health and safety is embedded in the current Enterprise Bargaining Agreement mandating health and safety training for all staff, to assist in further lowering the likelihood of serious injury.

Senior Executive Service Performance Pay

Sixty-three SES members received a performance bonus in 2009–10. Six 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 $2,200 - $10,840 with the average payment being $8,100. The total amount of performance pay for the SES was $559,550.

Corporate Capabilities

ASIO's rapid growth over recent years has presented challenges to its traditional methods of delivering corporate services. During 2009–10, ASIO embarked on an integrated, staged review and reengineering of corporate services to align them better to current and future needs. System modernisation initiatives enabled the transformation of business process and delivered improved access to corporate information and services.

Activities and work practices were streamlined and refined, resulting in the elimination of duplication and the delivery of more effective financial and payroll services to the Organisation. This included upgrades to ASIO's Financial Management Information System and to ASIO's Human Resource Information Management System, including an employee self-service system. A service centre approach for corporate services will ensure the most efficient and effective access to services possible, enabling staff to concentrate on operational matters.

The Organisation has developed a strategic change management strategy which includes assisting ASIO staff to identify, and work through, the changes required for effective operations in the new central office.

Corporate Strategy and Governance

ASIO's corporate governance arrangements reflect the Organisation's sustained focus on risk management, accountability, performance measurement, building capability and managing growth. In 2009–10, during a period of accelerated growth and the expansion of the national security community, ASIO prioritised efforts to ensure and promote an ASIO culture which supports and drives the Organisation's work. ASIO implemented strategies to ensure commitment to building external partnerships and contributing strongly to national security priorities continue to be embedded firmly in ASIO's culture.

At the core of ASIO's corporate governance structures are two high-level executive committees – the twice-weekly Director-General's Meeting and the twice-monthly Corporate Executive. ASIO's corporate committee structure is supported by a number of sub-committees and working groups that inform and strengthen the performance of the relevant committees, while also deeply embedding corporate governance principles at all levels of the Organisation (see Figure 3 on page 74).

Figure 3: Corporate Governance

Strategic Agenda - Business Review and Reform

Building and sustaining organisational capability across all parts of ASIO is central to its ability to perform effectively. Organisational capability covers a broad range of concepts that relate to the capacity of ASIO to achieve its business outcomes. Overall organisational capability is determined by a combination of people, processes, systems, culture, structures and assets.

In 2009–10, ASIO embarked on a comprehensive program of strategic business review and reform. The program has two overarching objectives – to ensure ASIO is working effectively and efficiently to meets its responsibilities, priorities, and tasking; and working effectively and cooperatively as part of the broader national security community.

An organisation-wide program of work has been underway to implement the results of several reviews, which examined the effectiveness of ASIO's work practices and processes, information technologies and systems, outreach and engagement, staff development and training, and legislative framework. Throughout the period, there has also been a focus on fostering a culture that identifies and addresses the critical issues and requirements of a security intelligence organisation in a rapidly evolving security environment.

Outcomes of ASIO's strategic work program in 2009–10 included a detailed examination of ASIO's operational and investigative process and procedures to reduce administrative overhead and maximise intelligence outcomes; the implementation of ASIO's new Leadership Development Strategy; the development of a People Capability Framework; streamlining of Visa Security Checking Processes through an enhanced risk management methodology; the rationalisation of ASIO's intelligence product lines; and review of ASIO's information management and IT systems, including the development of an Information Sharing Business Model, with a view to ensuring that information and data is always accessible to those who need it, when they need it.

In 2009–10, ASIO also improved its ability to work effectively and collaboratively within the national security community, including through the establishment of the Counter Terrorism Control Centre, and commencing a pilot study for the establishment of the National Interception Technical Assistance Centre.

An important feature of ASIO's corporate planning and governance arrangements is embedding ASIO's corporate goals into its business planning, accountability and performance management processes. ASIO's strategic agenda and associated work program will continue to evolve and become the primary means to transform ASIO's corporate strategy into workplace practices and processes that make a difference to the staff of ASIO and to the contribution they can make to national security.

Corporate Restructure

In 2009–10, ASIO's Senior Management group reviewed the Organisation's structure to position ASIO to meet future challenges through improving efficiency and functional alignment. The review of ASIO's structure was driven by ASIO's response to an evolving security environment as well as recent changes to ASIO's legislation and occurred in parallel with work being undertaken as part of ASIO's strategic agenda.

On 1 July 2010, ASIO will move from a twelve to a ten divisional structure to align key elements of functionality with the strategic framework (see Figure 2 on p. xii). The new structure will achieve a more efficient allocation of resources, with better alignment of staff skills and work unit functions resulting in an overall enhancement of organisational performance. It will better equip ASIO to contribute to a more broadly focused and interconnected national security community.

Risk Management

During the reporting period, ASIO's Corporate Executive Committee considered and endorsed a Strategic Risk Management Framework (SRMF) which identifies, treats and monitors strategic risks across the Organisation. The SRMF identifies key risks associated with collecting intelligence, assessing intelligence and providing advice, management and accountability and ensuring that appropriate strategies are in place to prepare for future challenges. Specific risk treatment plans have been developed to address a number of the identified risks to ASIO. As part of ASIO's governance cycle, the Corporate Executive will review the SRMF and progress against risk treatment plans on an annual basis. The outcomes of each annual review will inform business and budget planning for the following year.

Enterprise Resilience

In 2009–10, ASIO engaged a consultant to examine existing business continuity arrangements and to provide advice on best-practice arrangements to meet ASIO's future needs. As a result, a new Enterprise Resilience Program has been endorsed and implementation is underway. The program will deliver a more holistic approach to the resilience of the Organisation by integrating business continuity, security management, contingency planning and emergency response management arrangements. The transition to ASIO's new central office is built into the program.

ASIO Internal Performance Reporting

Changes to ASIO's internal performance reporting mechanisms in 2009–10 provided the Organisation with an improved tool to measure its performance against pre-determined benchmarks. The new reporting format captures performance indicators, outcomes and risks, which has resulted in more focused discussion and pro-active decision-making by ASIO's Corporate Executive Committee.

Revised ASIO Code of Conduct

In 2009–10, ASIO refined its Code of Conduct to enhance corporate governance arrangements. Refinements made to the Code of Conduct ensure it continues to articulate the professional and personal standards expected of ASIO officers while better reflecting the nature of the work undertaken, and the challenges and complexity of ASIO's operating environment.

Legislation

In 2009–10, ASIO continued to work collaboratively with other Commonwealth departments and agencies on policy development and proposed legislative amendments to ensure that the legislative framework supports ASIO's functions and capabilities. The legislative developments relevant to ASIO which occurred during the reporting period are detailed below.

Anti-People Smuggling and Other Measures Act 2010

The *Anti-People Smuggling and Other Measures Act 2010* (Cth) received Royal Assent on 31 May 2010. The Act strengthens the Commonwealth's anti-people smuggling legislative framework through amendments to:

- the *Criminal Code Act 1995* (Cth) and the *Migration Act 1958* (Cth) to create and harmonise offences and penalties in relation to people smuggling;
- the *Migration Act 1958* (Cth), the *Proceeds of Crime Act 2002* (Cth), the *Surveillance Devices Act 2004* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) to make consequential amendments;
- the *Australian Security Intelligence Organisation Act 1979* (Cth), to enable ASIO to carry out its intelligence functions in relation to territorial and border security issues; and
- the *Telecommunications (Interception and Access) Act 1979* (Cth) to enable foreign intelligence to be collected in certain circumstances and clarify that only the Minister for Defence and the Minister for Foreign Affairs can advise the Attorney-General on the need to issue a warrant for the collection of foreign intelligence.

The amendments to the *Australian Security Intelligence Organisation Act 1979* (Cth) introduced provision for the protection of Australia's territorial and border integrity from serious threat. This amendment enables ASIO to contribute to the Commonwealth's response, including people smuggling.

The Act also amended the definition of 'foreign intelligence' in the *Telecommunications (Interception and Access) Act 1979* (Cth) to align it with the concept of foreign intelligence currently contained in the *Intelligence Services Act 2010* (Cth).

Crimes Legislation Amendment (Serious and Organised Crime) Act 2010

The *Crimes Legislation Amendment (Serious and Organised Crime) Act 2010* received Royal Assent on 19 February 2010. The Act amended, amongst other matters, Part IAC of the *Crimes Act 1914* (Cth) to implement the new national model laws regime for assumed identities endorsed by the Standing Committee of Attorneys-General in 2004.

The new assumed identities regime provides a more detailed process for issuing, using and obtaining evidence in support of assumed identities used by ASIO, other intelligence agencies and law enforcement.

Tax Laws Amendments (2010 Measures No.3) Act 2010

The *Tax Laws Amendments (2010 Measures No.3) Act 2010* received Royal Assent on 29 June 2010. Schedule 3 to the Act amends the *Taxation Administration Act 1953* to remove the possibility of conflict between Australia's national security interests and obligations imposed by Commonwealth tax laws. It does this by empowering the Director-General of Security and the Director-General of the Australian Secret Intelligence Service to declare that specified transactions are to be disregarded in determining tax liabilities, obligations or benefits under Commonwealth law.

When any declarations under this Act are made, tax liabilities, obligations and benefits will not apply in relation to the specified transactions. As a result there will be no obligation to provide information about these transactions to the tax authorities and no power to seek that information. This ensures that information that bears on the operational activities of Australia's security and intelligence agencies, which should remain secret in the interests of national security, will not be disclosed.

Declarations are subject to review by the Inspector-General of Intelligence and Security, and also fall generally within the mandate of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its role to review the administration and expenditure of ASIO.

Information Services

Release of ASIO Records

ASIO is an exempt agency under the *Freedom of Information Act 1982* (FOI Act), but is subject to release of its records under the *Archives Act 1983* (Archives Act), which, until recent legislative changes, allowed for public access to all Commonwealth records over 30 years old – the 'open' period. Amendments to the FOI Act and subsequently to the Archives Act were passed in Parliament in May 2010 resulting in the change in the 'closed' period for access from 30 years to 20 years. This change will be implemented from

1 January 2011 with a transition period resulting in full implementation of the change by 2020. It is anticipated there will be a significant increase in workload with a greater number of records released during and following the transition period, but also a greater percentage of material being partially or totally exempted due to the sensitivities of the material.

Requests to access ASIO records that are in the 'open' period and not released publicly are made to the National Archives of Australia (NAA). 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 with the need to protect sensitive information. In most cases, the information is released and is available for public access.

During 2009–10, ASIO received 583 applications for access to records, an increase from 454 in 2008–09. A total of 641 requests were completed in 2009–10, including some requests carried over from previous years. The total number of folios examined during 2009–10 was 65,952 – a decrease from the 74,039 folios assessed in 2008–09.

Subject of Assessment	2008–09	2009–10
Percentage of Folios released without exemption	62%	61%
Percentage of Folios released with part of text claimed as exempt	37%	37%
Percentage of Folios claimed as totally exempt	1%	2%
Percentage of Folios completed within the 90 days	82%	86%
Total folios assessed	74,039	65,952

Table 4: Folios released 2008–10

ASIO gives greater priority to requests from those seeking records on themselves or family members. There were 153 such requests completed in 2009–10 compared with 169 in 2008–09. Ninety-nine per cent of requests from those seeking records on themselves or family members were completed within the benchmark of 90 days in 2009–10 – an improvement on 86 per cent for 2008–09.

ASIO completed 86 per cent of all requests within the 90 days in 2009–10, a slight increase from 82 per cent in 2008–09. This reflects the ongoing impact of assessing numbers of very large and complex requests and also assessing in priority order, where multiple requests are lodged by one applicant.

Applicants dissatisfied with exemptions of records released by ASIO can request a reconsideration of the decision. In 2009–10, there were six reconsiderations (one family and five non-family requests). In all cases, the NAA upheld the ASIO exemptions.

Applicants may appeal to the Administrative Appeals Tribunal (AAT) on two grounds – for review of ASIO exemptions; and if their request is not completed within 90 days. There were no appeals received by the AAT during the reporting period. However, two applications from earlier reporting periods were processed by the AAT in 2009–10. An appeal lodged in 2008–09 on a request not completed within 90 days resulted in records being provided to the applicant in November 2009. The applicant initiated further appeal action in the AAT against exemptions but it was withdrawn. The outcome for the other application was still to be resolved at the close of the reporting period.

Official History of ASIO

In 2009–10, the Australian National University continued its five-year research project on the *History of ASIO*. A two-volume unclassified work will cover the history of the Organisation from its establishment in 1949 through to the introduction of the ASIO Act in 1979. An Advisory Committee, including external representatives, was established and met in 2010.

Property

New Central Office

In July 2009, a sod-turning ceremony held on the site of ASIO's new central office on Constitution Avenue in Parkes, Canberra marked a significant project milestone. As at 30 June 2010, the base building architectural design work had been completed and the fit-out design was 85 per cent complete. Excavation work, which required the removal of 90,000 tonnes of rubble for the main building and structured car park facility, was completed.

Construction of the building commenced in September 2009 with construction of levels one, two and three well underway at the end of the reporting period. During 2010–11, construction activity will include the completion of the remaining building levels and the erection of the facade, to be followed by the commencement of the interior fit-out.

Construction is progressing on schedule for the building to be handed over to ASIO in mid-2012, with the main relocation of ASIO staff to commence in late 2012.The building is located within the Parliamentary Triangle in close proximity to 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.

The building is being designed and constructed in partnership with the Department of Finance and Deregulation and will accommodate up to 1,800 people. It will operate 24 hours per day, with a level of security commensurate with ASIO's intelligence functions.

In the 2008-09 Budget the Australian Government approved $606m for the new building. This was reduced to $589m in the 2009-10 Budget when the proposed subtenant, the Office of National Assessments, withdrew from the project to pursue

ASIO's new central office construction site June 2010

alternative leased accommodation. Close financial management by ASIO and the Department of Finance and Deregulation has ensured the project is proceeding within budget. 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 in order to maintain ASIO's capability to provide sound advice to Government on issues of national security.

ASIO has developed an asset management plan to align the replacement of furniture and Information and Communication Technology assets with the relocation to the new building, and to maximise the re-use of furniture and equipment where possible.

Authority Approvals

The building is being designed in close consultation with the National Capital Authority (NCA) to maintain adherence with the National Capital Plan and sympathy to the Griffin Legacy. The NCA has determined the development is consistent with the Plan and has provided works approvals for site establishment works, site works and building works (structural).

The project is being delivered in accordance with the Implementation Guidelines for the National Code of Practice for the Construction Industry and the requirements of the Office of the Federal Safety Commissioner.

In May 2010, a project update was provided to the Parliamentary Standing Committee on Public Works. The project team also provides regular briefings to government and commercial stakeholders and distributes newsletters to local residents advising of current and future site activity.

Environmental Management

Surveys of the site for the new central office identified it was formerly used as a landfill area revealing a small percentage of soil was contaminated by bonded asbestos sheeting. The majority of soil that contained the sheeting has now been removed successfully from the site. The remainder of the material lies under the existing engineering service lines and will be removed progressively as these services are upgraded during construction. The removal process was approved by the ACT Environmental Protection Authority and the work practices were endorsed by WorkCover ACT. Chilean Needle Grass, which is a noxious weed in the Australian Capital Territory, was also removed from the site in accordance with the legislative requirements of the Australian Capital Territory and New South Wales.

The size and footprint of the building required the removal of most of the existing trees on the site. The trees removed were recycled as mulch and donated to the local community for the regeneration of school gardens. A landscape master plan has been prepared for the site which includes significant new plantings. Management plans have been established for the preservation of a significant row of oak trees along Constitution Avenue.

More information on the new building is available from the ASIO website (www.asio.gov.au).

State and Territory Offices

To accommodate ASIO's growth, a national program to deliver new and upgraded accommodation commenced in 2006. Accommodation projects in the states and territories are nearing completion. These projects have delivered quality accommodation that is flexible, multi-functional and that meets the operational needs of the Organisation. In addition to providing additional space for ASIO staff, ASIO's new and upgraded accommodation has enabled the Organisation to increase operational capability in the states and territories.

ASIO has developed considerable expertise in managing high security accommodation projects with complex infrastructure requirements. Each project has been delivered on time and within budget. The lessons learned from each project have passed to the next project and where practicable are applied to the much larger new central office project in Canberra.

Consistency in the design and fit-out of ASIO's state and territory accommodation work has been accomplished to consolidate estate management plans and information. This work will stand the accommodation projects area in good stead as it transitions from capital projects to property management and becomes more involved in preparations for occupation of the new central office from late 2012.

Environmental Performance

ASIO's new central office is architecturally designed to meet Australian Government environmental targets for both the National Australian Built Environment Rating System (NABERS) and Green Star office design. The design features include a ventilated double skin on the south western glass facade of the building. This will provide excellent thermal performance and adjustability of conductive heat gain via ventilation control and offer reductions in radiant heat gain through the use of controlled external blinds. As well as managing solar gain, the system will provide shading to reduce glare and regulate the ambient temperature inside the building.

The new central office fit-out cultivates a healthy work environment and will include a range of renewable energy sources that provide a whole-of-life benefit environmentally, as well as reducing the running costs over the life of the building.

ASIO currently occupies an older central office building where there are limited opportunities for energy savings. The nature of ASIO's business, especially its large information technology infrastructure, continues to place heavy demands on ASIO's available power supply.

ASIO has been able to slow the growth of its energy consumption by taking cost effective energy savings measures. In the past year, ASIO's facilities management and information technology areas have undertaken an energy efficiency program in the current central office building that achieved savings in electrical energy of $270,000. These measures included:

- the installation of high efficiency light fittings;
- the installation of motion activated lighting in low traffic areas;
- an increase in temperature set points in air conditioning where practicable;
- upgrading the Building Management Control System to allow for more dynamic manual adjustments as well as improved scheduling of services to match occupancy in workspaces;
- continued purchasing of ten per cent green power;
- exploring greater use of cogeneration, tri-generation and solar power; and
- greater use of LPG and hybrid cars in the vehicle fleet.

ASIO has also improved its waste management practices by introducing co-mingle recycling. ASIO continues to recycle items such as fluorescent tubes, mobile telephones, batteries, and toner cartridges.

Estate and Asset Management

ASIO maintains its properties, plant and equipment to ensure optimal levels of service. Planned maintenance schedules are followed for plant and equipment. Due to the recent accommodation program it will be some time before new or renovated properties are scheduled for any significant refurbishment. However, the process of asset replacement is ongoing and ensures ASIO's assets, such as furniture and fittings, are replaced at the end of their useful and economical life. The asset management plan also aligns the replacement of furniture and information technology assets with the relocation to the new central office, and will maximise the re-use of furniture and equipment where possible. Assets within the current central office building have already been identified for transfer.

Financial Services

Purchasing

Quality procurement advice, documentation and training ensured ASIO's procurement activity continued to function within the *Director-General Finance Instructions and the Commonwealth Procurement Guidelines*, subject to authorised exemptions for the protection of National Security. ASIO adhered to the Australian Government's core procurement policy framework, and ensured value for money was achieved through competitive procurement processes where practicable.

In 2009–10, ASIO's investment in capability continued with procurement activity focused on key business areas, including technical capabilities, information technology infrastructure and protective security.

Details of ASIO agreements, contracts and standing offers may be made available to Members of Parliament as a confidential briefing or to the PJCIS.

Consultants

During 2009–10, ASIO let 16 consultancy contracts. The total expenditure during the year on consultancy contracts valued at $10,000 or more (including contracts let during the previous year) totalled $1.320m.

Subject to authorised exemptions for the protection of national security, a list of consultancy let contracts to the value of $10,000 or more (GST inclusive), and the total value of each of those contracts, may be made available to Members of Parliament as a confidential briefing, or to the PJCIS on request.

Competitive Tendering and Contracting

ASIO released five restricted requests for tender during 2009–10. In each case the requests for tender were not advertised publicly for national security reasons – rather, a restricted set of suppliers was invited to tender.

part six

6

Financial Statements

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2010 are based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.

David Irvine
Director-General of Security

12 October 2010

INDEPENDENT AUDITOR'S REPORT

To the Attorney-General

Scope

I have audited the accompanying financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2010, 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 to and forming part of the Financial Statements, including a Summary of Significant Accounting Policies.

The Responsibility of the Director-General of Security for the Financial Statements

The Director-General of Security is responsible for the preparation and fair presentation of the financial statements in accordance with the Agreement with between the Attorney-General and the Finance Minister. This Agreement requires the financial statements to be prepared in accordance with the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, including the Australian Accounting Standards (which include the Australian Accounting Interpretations), 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's responsibility includes establishing and maintaining internal controls relevant to the preparation and fair presentation of the financial statements that are free from material misstatement, whether due to fraud or error; selecting and applying appropriate accounting policies; and making accounting estimates that are reasonable in the circumstances.

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 whether the financial statements are free from material misstatement.

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

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 and fair presentation of the financial statements 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 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 the audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

Auditor's 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 2010 and its financial performance and cash flows for the year then ended.

Australian National Audit Office

Simon Kidman
Executive Director

Delegate of the Auditor-General

Canberra
12 October 2010

STATEMENT OF COMPREHENSIVE INCOME

for the period ended 30 June 2010

	Notes	2010 $ '000	2009 $ '000
EXPENSES			
Employee benefits	3A	**178,361**	150,961
Suppliers	3B	**138,632**	133,457
Depreciation and amortisation	3C	**53,544**	52,090
Finance costs	3D	**369**	626
Write-down and impairment of assets	3E	**4,776**	7,238
Foreign exchange losses	3F	**2**	2
Net losses from sale of assets	3G	**131**	242
Total Expenses		**375,815**	344,616
Less:			
OWN SOURCE INCOME			
Revenue			
Sale of goods and rendering of services	4A	**5,913**	5,230
Total Own-Source Revenue		**5,913**	5,230
Gains	4B	**3,813**	3,847
Total Gains		**3,813**	3,847
Total Own-Source Income		**9,726**	9,077
Net Cost of Services		**366,089**	335,539
Revenue from Government	4C	**405,518**	352,653
Surplus attributable to the Australian Government		**39,429**	17,114
OTHER COMPREHENSIVE INCOME			
Changes in asset revaluation reserves		**(792)**	-
Total Comprehensive Income attributable to the Australian Government		**38,637**	17,114

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

BALANCE SHEET

as at 30 June 2010

	Notes	2010 $ '000	2009 $ '000	2008 $ '000
ASSETS				
Financial Assets				
Cash and cash equivalents	5A	**17,525**	10,246	29,168
Trade and other receivables	5B	**311,220**	283,286	207,373
Other financial assets	5C	**874**	1,061	1
Total financial assets		**329,620**	294,593	236,542
Non-Financial Assets				
Land and buildings	6A,D	**95,422**	89,019	59,264
Infrastructure, plant and equipment	6B,D	**82,338**	102,317	95,144
Intangibles	6C,E	**10,559**	21,247	26,369
Other non-financial assets	6F	**12,289**	12,254	12,582
Total non-financial assets		**200,609**	224,836	193,359
Total Assets		**530,229**	519,429	429,901
LIABILITIES				
Payables				
Suppliers	7A	**10,151**	13,673	16,022
Other payables	7B	**4,321**	3,918	2,270
Total payables		**14,471**	17,591	18,292
Lease Liabilities				
Lease incentives	8	**3,869**	3,989	2,589
Total lease liabilities		**3,869**	3,989	2,589
Provisions				
Employee provisions	9A	**41,898**	35,585	36,457
Other provisions	9B	**9,447**	7,764	5,987
Total provisions		**51,345**	43,349	42,444
Total Liabilities		**69,685**	64,929	63,325
Net Assets		**460,544**	454,500	366,576
EQUITY				
Contributed equity		**392,187**	424,780	353,970
Reserves		**8,102**	8,894	8,894
Retained surplus		**60,255**	20,826	3,712
Total Equity		**460,544**	454,500	366,576

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

STATEMENT OF CHANGES IN EQUITY

as at 30 June 2010

	Retained Earnings		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2010	2009	**2010**	2009	**2010**	2009	**2010**	2009
	$'000	$'000	**$'000**	$'000	**$'000**	$'000	**$'000**	$'000
Opening Balance	**20,826**	3,712	**8,894**	8,894	**424,780**	353,970	**454,500**	366,576
Comprehensive Income								
Changes in Asset Revaluation Reserves								
Asset revaluations	**-**		**(989)**		**-**		**(989)**	
Restoration obligations revaluations	**-**		**197**		**-**		**197**	
Surplus for the period	**39,429**	17,114	**-**		**-**		**39,429**	17,114
Total comprehensive income	**39,429**	17,114	**(792)**		**-**		**38,637**	17,114
Transactions with Owners								
Distributions to Owners								
Return to consolidated revenue [1]	**-**		**-**		**(49,050)**		**(49,050)**	
Contributions by Owners								
Appropriation (equity injection)	**-**		**-**		**16,457**	70,810	**16,457**	70,810
Closing Balance attributable to the Australian Government	**60,255**	20,826	**8,102**	8,894	**392,187**	424,780	**460,544**	454,500

1. Net Cash arangements

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

CASH FLOW STATEMENT

for the period ended 30 June 2010

	Notes	2010 $ '000	2009 $ '000
OPERATING ACTIVITIES			
Cash received			
Goods and services		**5,987**	8,066
Appropriations		**341,406**	270,000
Net GST received		**13,112**	19,083
Other cash received		**4,966**	5,722
Total cash received		**365,472**	302,871
Cash used			
Employees		**171,312**	150,928
Suppliers		**155,725**	153,455
Total cash used		**327,037**	304,383
Net cash from or (used by) operating activities	10	**38,435**	(1,512)
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		**506**	542
Total cash received		**506**	542
Cash used			
Purchase of property, plant and equipment		**35,023**	82,978
Purchase of intangibles		**661**	7,815
Total cash used		**35,684**	90,793
Net cash from or (used by) investing activities		**(35,178)**	(90,251)
FINANCING ACTIVITIES			
Cash received			
Appropriations - contributed equity		**4,022**	72,842
Total cash received		**4,022**	72,842
Net cash from or (used by) financing activities		**4,022**	72,842
Net increase or (decrease) in cash held		**7,279**	(18,922)
Cash and cash equivalents at the beginning of the reporting period		**10,246**	29,168
Cash and cash equivalents at the end of the reporting period	5A	**17,525**	10,246

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

SCHEDULE OF COMMITMENTS

as at 30 June 2010

	Notes	2010 $ '000	2009 $ '000
BY TYPE			
Commitments receivable			
Sublease rental income		**5,628**	7,257
GST recoverable on commitments		**11,010**	11,304
Total commitments receivable		**16,638**	18,561
Commitments payable			
Capital commitments			
Land & buildings		**158,897**	165,093
Infrastructure, plant and equipment	A	**638**	295
Intangibles		**12**	-
Total capital commitments		**159,547**	165,388
Other commitments			
Operating leases	B	**217,653**	233,492
Other commitments		**11,701**	9,354
Total other commitments		**229,355**	242,846
Net commitments by type		**372,264**	389,673

Commitments are GST inclusive where relevant.

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:

Nature of lease / General description of leasing arrangement

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 CPI; and
biennial review based on market appraisal.

Agreements for the provision of motor vehicles to senior executive and other officers.

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

	Notes	2010 $ '000	2009 $ '000
BY MATURITY			
Commitments receivable			
Sublease rental income			
One year or less		**1,697**	1,629
From one to five years		**3,931**	5,628
Total operating lease income		**5,628**	7,257
Other commitments receivable			
One year or less		**2,573**	2,433
From one to five years		**5,491**	5,663
Over five years		**2,945**	3,208
Total other commitments receivable		**11,010**	11,304
Commitments payable			
Capital commitments			
One year or less		**98,391**	24,764
From one to five years		**61,156**	140,624
Total capital commitments		**159,547**	165,388
Operating lease commitments			
One year or less		**38,012**	36,943
From one to five years		**117,778**	129,175
Over five years		**61,863**	67,374
Total operating lease commitments		**217,653**	233,492
Other commitments			
One year or less		**8,657**	8,695
From one to five years		**3,044**	659
Total other commitments		**11,701**	9,354
Net commitments by maturity		**372,264**	389,673

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

SCHEDULE OF CONTINGENCIES

as at 30 June 2010

	2010 $ '000	2009 $ '000
	Claims for damages or costs	
Contingent liabilities		
Balance from previous period	-	-
New	-	27
Total contingent liabilities	-	27
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 2010

	Land $'000	Buildings $'000	Buildings- Leasehold Improvement $'000	Infrastructure, Plant & Equipment $'000	Intangibles $'000	Total $'000
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**	**18,149**	**16,712**	**1,833**	**36,869**

	Land $'000	Buildings $'000	Buildings Leasehold Improvement $'000	Infrastructure, Plant & Equipment $'000	Intangibles $'000	Total $'000
Non-financial non-current assets added in 2008-09						
Additions funded in the current year						
By purchase appropriation equity		1,707	39,967	25,757	5,410	72,842
By purchase appropriation ordinary annual services				14,835	3,117	17,952
Total additions funded in the current year		1,707	39,967	40,592	8,527	90,794
Additions recognised in 2008-09 to be funded in future years						
Restoration obligations			580			580
Total additions funded in future years			580			580
Total asset additions		1,707	40,547	40,592	8,527	91,374

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

for the year ended 30 June 2010

Note 1: Summary of Significant Accounting Policies

1.1 Objective of ASIO

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 following outcome:

> A secure Australia for people and property, Government business and national infrastructure, and special events of national and international significance.

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 continued 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 2009* except where the disclosure of information in the notes to the financial statements would, 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 (FMOs) for reporting periods ending on or after 1 July 2009; 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 Judgements 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 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 nor 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 a service 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 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 days terms, are recognised at nominal amounts due less any impairment allowance amount. Collectability of debts is reviewed at balance date. Provisions are made when collectability of the debt is no longer probable.

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 non-current 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

"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 currently used by ASIO to fund capital requirements were returned to consolidated revenue as required.

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 present value of the estimated future cash outflows to be made in respect of services provided by employees up to the reporting date.

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 applied 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 termination 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 3 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 each balance date.

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.

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.

Other financial 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 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 settlement is not probable or 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 agency'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' taken up.

Revaluations

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

Asset Class	*Fair value measured at:*
Land	Market selling price
Buildings	Market selling price
Leasehold	Depreciated replacement cost
Plant & 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 through surplus and deficit. Revaluation decrements for a class of assets are recognised directly through the operating result 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:

	2010	2009
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 2010. 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

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 lives of ASIO's software is 4-5 years (2008-09: 4-5 years).

All software assets were assessed for indications of impairment as at 30 June 2010.

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 2010 financial statements. (2009: Nil)

Note 3: Expenses	2010 $ '000	2009 $ '000
Note 3A: Employee benefits		
Wages and salaries	**137,269**	121,221
Superannuation:		
Defined contribution plans	**8,819**	6,438
Defined benefit plans	**18,165**	17,336
Leave and other entitlements	**11,889**	5,698
Separation and redundancies	**2,219**	268
Total employee benefits	**178,361**	150,961
Note 3B: Suppliers		
Provision of goods - related entities	**1,038**	1,326
Provision of goods - external entities	**8,439**	7,606
Rendering of services - related entities	**28,094**	25,677
Rendering of services - external entities	**78,964**	75,416
Operating lease rentals - related entities:		
Minimum lease payments	**3,626**	3,051
Operating lease rentals - external entities:		
Minimum lease payments	**16,913**	19,036
Workers' compensation premiums	**1,558**	1,345
Total supplier expenses	**138,632**	133,457
Note 3C: Depreciation and amortisation		
Depreciation		
Infrastructure, plant and equipment	**30,549**	28,377
Buildings	**11,737**	12,079
Total depreciation	**42,286**	40,456
Amortisation - Intangibles - computer software	**11,258**	11,634
Total depreciation and amortisation	**53,544**	52,090
Note 3D: Finance costs		
Unwinding of discount - restoration obligations	**369**	626

	2010 $ '000	2009 $ '000
Note 3E: Write down and impairment of assets		
Asset write-downs from:		
Impairment of receivables	**2**	1,123
Writedown of land and buildings	**184**	85
Writedown of property, plant and equipment	**4,469**	4,756
Writedown of intangible assets	**121**	148
Impairment of intangible assets	**-**	1,125
Total write-down and impairment of assets	**4,776**	7,238
Note 3F: Foreign exchange losses		
Non-speculative	**2**	2
Note 3G: Net losses from asset sales		
Infrastructure, plant and equipment		
Proceeds from sale	**(506)**	(512)
Carrying value of assets sold	**667**	754
Intangibles		
Proceeds from sale	**(30)**	(30)
Carrying value of assets sold	**-**	30
Total losses from asset sales	**131**	242

Note 4: Income

Note 4A: Sale of goods and rendering of services		
Provision of goods - related entities	**31**	225
Provision of goods - external entities	**35**	5
Rendering of services - related entities	**3,704**	4,658
Rendering of services - external entities	**2,142**	341
Total sale of goods and rendering of services	**5,913**	5,230
Note 4B: Gains		
Resources received free of charge	**100**	100
Rent	**1,515**	1,512
Interest	**-**	7
Repayment of costs shared by other agencies	**1,836**	1,490
Miscellaneous	**362**	738
Total other gains	**3,813**	3,847

Note 4C: Revenue from Government	2010 $ '000	2009 $ '000
Appropriation - Departmental outputs	**405,518**	352,653

Note 5: Financial Assets

Note 5A: Cash and cash equivalents

Cash on hand or on deposit	**17,525**	10,246

Note 5B: Trade and other receivables

Goods and services		
Related entities	**2,927**	1,677
External entities	**138**	165
Total receivables for goods and services	**3,065**	1,842
Appropriations Receivable for existing outputs	**306,273**	278,775
GST receivable from the Australian Taxation Office	**1,882**	2,670
Total trade and other receivables (gross)	**311,220**	283,287
Less impairment allowance account:		
Goods and services	**-**	1
Total trade and other receivables (net)	**311,220**	283,286

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

Receivables are aged as follows:		
Not overdue	**310,801**	282,671
Overdue by:		
less than 30 days	**180**	98
30 to 60 days	**90**	452
61 to 90 days	**29**	25
more than 90 days	**120**	40
Total receivables (gross)	**311,220**	283,286

Reconciliation of the Impairment Allowance Account	**Goods & Services**	Goods & Services
Opening balance	**1**	-
amounts written off	**(1)**	-
increase/decrease recognised in net surplus	**-**	1
Closing balance	**-**	1

	2010 $ '000	2009 $ '000
Note 5C: Other financial assets		
Accrued Revenue	**874**	1,061

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**	1,385
Buildings on freehold land		
fair value	**7,653**	8,593
accumulated depreciation	**(105)**	(676)
accumulated impairment losses	**-**	-
Total buildings on freehold land	**7,548**	7,917
Leasehold improvements		
work in progress	**17,562**	6,715
fair value	**71,267**	92,898
accumulated depreciation	**(2,470)**	(19,897)
Total leasehold improvements	**86,359**	79,717
Total land and buildings (non-current)	**95,422**	89,019

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.

Note 6B: Infrastructure, plant and equipment

Infrastructure, plant and equipment		
work in progress	**756**	411
fair value	**87,137**	150,746
accumulated depreciation	**(5,555)**	(48,840)
Total Infrastructure, plant and equipment (non-current)	**82,338**	102,317

All revaluations were conducted in accordance with the revaluation policy stated at Note 1. On 31 March 2010 an independent valuer (Australian Valuation Office) conducted the revaluations.

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

No infrastructure, plant or equipment is expected to be sold or disposed of within the next 12 months.

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

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

Note 6C: Intangibles	2010 $ '000	2009 $ '000
Computer Software		
purchased - at cost	**17,884**	17,882
internally developed - in progress	**194**	1,351
internally developed - in use	**20,807**	19,823
accumulated amortisation	**(27,202)**	(16,684)
accumulated impairment	**(1,125)**	(1,125)
Total computer software	**10,559**	21,247
Total intangibles (non-current)	**10,559**	21,247

No indicators of impairment were found for intangibles.
No intangibles are expected to be sold or disposed of within the next 12 months.

Note 6D: Analysis of Property, Plant and Equipment

TABLE A - Reconciliation of the opening and closing balances of property, plant and equipment (2009-10)

	Land	Buildings	Buildings- Leasehold Improvement	Infrastructure Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000
As at 1 July 2009					
Gross book value	1,385	8,593	99,613	151,157	260,748
Accumulated depreciation / amortisation 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
Revaluations and impairments through comprehensive income	130	(61)	(69)	(989)	(989)
Depreciation / amortisation 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 by:					
Gross book value	1,515	7,653	88,828	87,893	185,889
Accumulated depreciation / amortisation and impairment	-	(105)	(2,470)	(5,555)	(8,130)
	1,515	7,548	86,359	82,338	177,760

TABLE B - Reconciliation of the opening and closing balances of property, plant and equipment (2008-09)

	Land	Buildings	Buildings Leasehold Improvement	Infrastructure Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000
As at 1 July 2008					
Gross book value	1,385	6,885	62,797	121,748	192,815
Accumulated depreciation / amortisation and impairment		(237)	(11,566)	(26,604)	(38,407)
Net book value 1 July 2008	1,385	6,648	51,231	95,144	154,408
Adj Gross book value			(543)	(3,695)	(4,238)
Accumulated depreciation / amortisation and impairment			543	3,695	4,238
Adjusted Net book value 1 July 2008	1,385	6,648	51,231	95,144	154,408
Additions by purchase		1,707	39,967	40,592	82,267
Reclassifications			243	469	712
Depreciation/ amortisation expense		(439)	(11,639)	(28,377)	(40,455)
Disposals			(85)	(5,511)	(5,597)
Net book value 30 June 2009	1,385	7,917	79,717	102,317	191,336
Net book value as at 30 June 2009 represented by:					
Gross book value	1,385	8,593	99,613	151,157	260,748
Accumulated depreciation / amortisation and impairment		(676)	(19,897)	(48,840)	(69,413)
	1,385	7,917	79,717	102,317	191,336

Note 6E: Intangibles

TABLE A - Reconciliation of the opening and closing balances of intangibles (2009-10)

	Computer software internally developed $'000	Computer software purchased $'000	Other Intangibles $'000	Total $'000
As at 1 July 2009				
Gross book value	**24,095**	**14,961**	**-**	**39,056**
Accumulated depreciation / amortisation and impairment	**(11,778)**	**(6,032)**	**-**	**(17,809)**
Net book value 1 July 2009	**12,317**	**8,929**	**-**	**21,247**
Adj Gross book value [1]	**(542)**	**542**	**-**	**-**
Accumulated depreciation / amortisation and impairment	**-**	**-**	**-**	**-**
Adjusted Net book value 1 July 2009	**11,775**	**9,471**	**-**	**21,247**
Additions:				
by purchase	**-**	**849**		**849**
internally developed	**985**	**-**	**-**	**985**
Amortisation expense	**(6,417)**	**(4,841)**	**-**	**(11,258)**
Disposals	**(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 depreciation / 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 has been revised based on a review of intangibles undertaken in 2009 10.

TABLE B - Reconciliation of the opening and closing balances of intangibles (2008-09)

	Computer software internally developed $'000	Computer software purchased $'000	Other Intangibles $'000	Total $'000
As at 1 July 2008				
Gross book value	21,698	19,679	1,937	43,314
Accumulated depreciation / amortisation and impairment	(6,465)	(9,721)	(759)	(16,945)
Net book value 1 July 2008	15,233	9,958	1,178	26,369
Adj Gross book value		(8,631)	(225)	(8,856)
Accumulated depreciation / amortisation and impairment		8,631	225	8,856
Adjusted Net book value 1 July 2008	15,233	9,958	1,178	26,369
Additions by purchase or internally developed	4,509	4,017		8,527
Reclassification	(712)			(712)
Amortisation expense	(5,515)	(4,986)	(1,133)	(11,634)
Impairment	(1,125)			(1,125)
Disposals	(73)	(60)	(45)	(178)
Net book value 30 June 2009	12,317	8,929		21,247
Net book value as at 30 June 2009 represented by:				
Gross book value	24,095	14,961		39,056
Accumulated depreciation / amortisation and impairment	(11,777)	(6,032)		(17,809)
	12,317	8,929		21,247

Note 6F: Other non-financial assets	2010 $ '000	2009 $ '000
Prepayments	**12,289**	12,254

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

No indicators of impairment were found for prepayments.

Note 7: Payables

Note 7A: Suppliers

Trade creditors and accruals	**10,151**	13,575
Operating lease rentals	**-**	98
Total supplier payables	**10,151**	13,673
Supplier payables expected to be settled within 12 months:		
Related entities	**1,398**	1,711
External entities	**8,753**	11,962

Settlement is usually made net 30 days.

Note 7B: Other payables

Salaries and wages	**3,172**	2,530
Superannuation	**459**	365
Unearned income	**8**	613
Fringe Benefits Tax	**682**	410
Total other payables	**4,321**	3,918

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

Note 8: Lease Liabilities

Lease incentives	**3,869**	3,989
Lease incentives are expected to be settled in:		
No more than 12 months	**535**	539
More than 12 months	**3,334**	3,450

Note 9: Provisions	2010 $ '000	2009 $ '000	2008 $ '000
Note 9A: Employee provisions			
Leave [1]	**39,683**	35,585	36,457
Redundancies	**963**	-	-
Superannuation	**1,252**	-	-
Total employee provisions	**41,898**	35,585	36,457
Employee provisions are expected to be settled in:			
No more than 12 months	**27,138**	20,655	25,246
More than 12 months	**14,760**	14,930	11,211
Total employee provisions	**41,898**	35,585	36,457

1. During 2009-10, ASIO detected an error in the valuation of Employee Provisions as at 30 June 2009. This was due to a miscalculation of the daily salary rate used to value long service leave entitlements. 2008-09 comparatives have been restated to reflect correction of the error. There is no effect on 2007-08 comparatives.

   The adjustment affects the following line items:

	Prior to correction $'000	Amount of correction $'000	After correction $'000
Income Statement			
Expenses – Employee benefits	158,508	(7,547)	150,961
Surplus	9,567	7,547	17,114
Balance Sheet			
Employee provisions	43,132	(7,547)	35,585
Equity – Retained surplus	13,279	7,547	20,826
Statement of Changes in Equity			
Surplus for the period	9,567	7,547	17,114

Note 9B: Other provisions	2010 $ '000	2009 $ '000
Restoration obligations	**6,797**	6,526
Rent payable	**2,345**	1,238
Reorganisation costs	**305**	-
Total other provisions	**9,447**	7,764
Other provisions are expected to be settled in:		
No more than 12 months	**2,345**	1,285
More than 12 months	**7,102**	6,479
Total other provisions	**9,447**	7,764

	Restoration Obligations $'000	Rent Payable $'000	Total $'000
Carrying amount 1 July 2009	**6,526**	**1,238**	**7,764**
Additional provisions made	**175**	**1,107**	**1,282**
Lease expiry	**(76)**	**-**	**(76)**
Revaluation	**(197)**	**-**	**(197)**
Unwinding of discount or change in discount rate	**369**	**-**	**369**
Closing balance	**6,797**	**2,345**	**9,142**

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

Note 10: Cash Flow Reconciliation

	2010 $ '000	2009 $ '000
Reconciliation of cash and cash equivalents per Balance Sheet to Cash Flow Statement		
Report cash and cash equivalents as per:		
Cash Flow Statement	**17,525**	10,246
Balance Sheet	**17,525**	10,246
Reconciliation of net cost of services to net cash from operating activities:		
Net cost of services	**(366,089)**	(335,539)
Add revenue from Government	**405,518**	352,653
Adjustment for non-cash items		
Depreciation/amortisation	**53,544**	52,090
Net write down of non-financial assets	**4,774**	6,114
Net write down of other provisions	**197**	-
Net loss on disposal of assets	**131**	242
Changes in assets/liabilities		
(Increase)/decrease in receivables	**(64,548)**	(77,945)
(Increase)/decrease in accrued revenue	**187**	(1,060)
(Increase)/decrease in prepayments	**(35)**	328
Increase/(decrease) in employee provisions	**6,313**	(867)
Increase/(decrease) in other provisions	**1,683**	1,777
Increase/(decrease) in lease incentives	**(120)**	1,400
Increase/(decrease) in supplier payables	**(3,522)**	(2,349)
Increase/(decrease) in accrued expenses	**403**	1,644
Net cash from/(used by) operating activities	**38,435**	(1,512)

Note 11: Contingent Liabilities and Assets

Quantifiable contingencies

The Schedule of Contingencies reports contingent liabilities in respect of claims for damages/costs of $ NIL (2009: $27,000). This amount represents an estimate of ASIO's liability based on precedent cases. ASIO is defending the claims.

Unquantifiable contingencies

At 30 June 2010, 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. (2009: 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 Australian National Audit Office. No other services were provided by the Auditor-General.

	2010	2009
Fair value	**$100,000**	$100,000

Note 13: Senior Executive Remuneration

Note 13A: Actual remuneration paid to senior executives

Executive remuneration

The number of senior executives who received or were due to receive:	**2010**	2009
less than $145 000	**1**	-
$145 000 to $159 999	**-**	-
$160 000 to $174 999	**1**	3
$190 000 to $204 999	**2**	4
$205 000 to $219 999	**8**	3
$220 000 to $234 999	**19**	7
$235 000 to $249 999	**7**	3
$250 000 to $264 999	**6**	6
$265 000 to $279 999	**4**	4
$280 000 to $294 999	**2**	6
$295 000 to $309 999	**1**	6
$310 000 to $324 999	**-**	7
$325 000 to $339 999	**-**	1
$340 000 to $354 999	**2**	2
$355 000 to $369 999	**-**	2
$370 000 to $384 999	**-**	3
$385 000 to $399 999	**-**	1
$400 000 to $414 999	**-**	1
$475 000 to $489 999	**1**	-
	54	59

Total expense recognised in relation to senior executive employment	**2010 $ '000**	2009 $ '000
Short-term employee benefits:		
Salary (including annual leave taken)	**8,906**	8,951
Vehicle costs (including parking)	**445**	742
Performance bonuses	**392**	403
Applicable Fringe Benefits Tax	**324**	267
Changes in annual leave provisions	**266**	166
Other [1]	**129**	153
Total short-term employee benefits	**10,462**	10,682
Superannuation (post-employment benefits)	**2,153**	2,286
Changes in long service leave provisions	**268**	1,155
Total benefits	**12,883**	14,123
Termination benefits paid to senior executives	**199**	-

Notes

1. "Other" includes salary in lieu of motor vehicle and other allowances.

Note 13B: Salary packages for senior executives as at 30 June

Average annualised remuneration packages for substantive senior executives

	as at 30 June 2010			as at 30 June 2009		
	Number of SES	Base salary [1] $ '000	Total Remuneration [2] $ '000	Number of SES	Base salary [1] $ '000	Total Remuneration [2] $ '000
Total remuneration						
less than $145 000	**1**	**116**	**140**	-	-	-
$175 000 to $189 999	**-**	**-**	**-**	1	129	185
$190 000 to $204 999	**-**	**-**	**-**	23	143	198
$205 000 to $219 999	**21**	**148**	**210**	13	143	219
$220 000 to $234 999	**15**	**148**	**222**	2	143	223
$235 000 to $249 999	**-**	**-**	**-**	8	175	239
$250 000 to $264 999	**6**	**181**	**252**	4	175	263
$265 000 to $279 999	**6**	**181**	**268**	5	179	268
$295 000 to $309 999	**1**	**201**	**298**	1	194	298
$325 000 to $339 999	**1**	**258**	**332**			
$355 000 to $369 999	**-**	**-**	**-**	1	321	361
$415 000 to $429 999	**1**	**371**	**418**	-	-	-
	52			58		

Notes

1. including annual leave
2. Non salary elements include superannuation, vehicle costs, performance bonuses and other allowances.

Note 14: Financial Instruments

	$'000	$'000
Note 14A: Categories of financial instruments		
Financial Assets		
Loans and receivables		
Cash and cash equivalents	**17,525**	10,246
Trade receivables	**3,065**	1,842
Accrued revenue	**874**	1,061
Carrying amount of financial assets	**21,465**	13,149
Financial Liabilities		
At amortised cost		
Trade creditors and accruals	**10,151**	13,673
Carrying amount of financial liabilities	**10,151**	13,673

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 2010. (2009: Nil). The total expense from financial assets through the profit and loss for the period ending 30 June 2010 was $2,315 (2009: $1,122,666).

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 2010 (2009: Nil).

Note 14D: Fair value of financial instruments

	2010 $'000 Carrying amount	2010 $'000 Fair value	2009 $'000 Carrying amount	2009 $'000 Fair value
Financial Assets				
Loans and Receivables				
Cash & cash equivalents	**17,525**	**17,525**	10,246	10,246
Trade receivables (net)	**3,065**	**3,065**	1,842	1,842
Accrued revenue	**874**	**874**	1,061	1,061
Total	**21,465**	**21,465**	13,149	13,149
Financial Liabilities				
At amortised cost				
Trade creditors and accruals	**10,151**	**10,151**	13,673	13,673

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.

	2010	2009
	$'000	$'000
Financial Assets		
Loans and receivables		
Cash and cash equivalents	**17,525**	10,246
Trade receivables	**3,065**	1,842
Accrued revenue	**874**	1,061
Total	**21,465**	13,149
Financial Liabilities		
At amortised cost		
Trade creditors and accruals	**10,151**	13,673

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

	2010	2009	**2010**	2009
	$'000	$'000	**$'000**	$'000
	Not past due nor impaired		**Past due or impaired**	
Loans and receivables				
Cash and cash equivalents [1]	**17,525**	10,246	**-**	-
Trade receivables [2]	**2,646**	1,227	**419**	615
Accrued revenue [3]	**874**	1,061	**-**	-
Total	**21,046**	12,534	**419**	615

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 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**

Ageing of financial assets that are past due but not impaired for 2009

	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	98	452	25	40	615

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, ensures 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 2008-09.

The following table illustrates the maturities for financial liabilities.

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

	2009 $'000 On demand	2009 $'000 within 1 year	2009 $'000 1 to 5 years	2009 $'000 > 5 years	2009 $'000 Total
At amortised cost					
Trade creditors and accruals	-	13,673	-	-	13,673

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 2008-09. ASIO is not exposed to 'Currency risk', 'Other price risk' or 'Interest rate risk'.

Note 15: Appropriations

Note 15A: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriation

	2010 $ '000	2009 $ '000
Balance carried from previous period	**225,545**	160,621
Appropriation Act:		
Appropriation Act (No.1) 2009 10 as passed	**408,518**	352,653
Appropriation Act (No.3) 2009 10 as passed	**-**	
Approprtiation reduced (Appropriation Act (No.1) 2009 10 section 10)	**(49,050)**	
FMA Act:		
Repayments to the Commonwealth (FMA Act s30)	**1,253**	1,975
Appropriations to take account of recoverable GST (FMA Act *s30A*)	**10,948**	11,692
Relevant agency receipts (FMA Act s31)	**11,459**	12,355
Total appropriations available for payments	**608,673**	539,296
Cash payments made during the year (GST inclusive)	**308,532**	313,751
Balance of Authority to draw cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriations	**300,141**	225,545
Represented by:		
Cash at bank and on hand	**17,525**	10,246
Receivables departmental appropriations	**278,218**	214,106
GST receivable from the Australian Taxation Office	**1,398**	1,193
Transfer to Department of the Prime Minister & Cabinet [1]	**3,000**	
Total	**300,141**	225,545

Note

1. Adjustment under section 101.13 of FMOs. One off measure for ASIO's contribution to the 2011 independent review of the intelligence community. The review is a recommendation from the 2004 Flood Inquiry into Australia's Intelligence Agencies.
   Determination has not yet been released by Department of Finance and Deregulation.

Note 15B: Acquittal of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriation	2010 $ '000	2009 $ '000
Balance carried from previous year	**65,736**	66,701
Appropriation Act:		
Appropriation Act (No.2) 2009-10 as passed	**16,457**	70,810
Appropriation Act (No.4) 2009-10 as passed	**-**	-
FMA Act:		
Appropriations to take account of recoverable GST (FMA Act *s30A*)	**2,164**	8,584
Total appropriations available for payments	**84,357**	146,095
Cash payments made during the year (GST inclusive)	**55,818**	80,359
Balance of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriations	**28,539**	65,736
Represented by:		
Receivables - departmental appropriations	**28,055**	64,669
GST receivable from the Australian Taxation Office	**484**	1,067
Total	**28,539**	65,736

Note 16: Compensation and Debt Relief

	2010	2009
No payments were made during the reporting period under the 'Defective Administration Scheme'. (2009: One payment made).	**-**	$1,247

Note 17: Reporting of Outcomes

Note 17A: Net Cost of Outcome Delivery	2010 $'000	2009 $'000
Expenses		
Departmental	**375,815**	344,616
Costs recovered from provision of goods and services to the non-government sector		
Departmental	**4,375**	2,574
Other external revenues		
Departmental	**5,350**	6,395
Net cost of outcome	**366,090**	335,646

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

part
seven

7

Appendices & Indices

Appendix A: Agency Resource Statement 2009–10

	Actual Available Appropriations for 2009–10 $'000	Payments Made 2009–10 $'000	Balance Remaining $'000
Ordinary Annual Services			
Departmental appropriation			
Prior year departmental appropriation	165,056	165,056	–
Departmental appropriation	405,518	127,300	278,218
S.31 Relevant agency receipts	4,600	5,913	(1,313)
Total	575,174	298,269	276,905
Departmental non-operating			
Prior year equity injections	64,669	53,071	11,598
Equity injections	16,457	–	16,457
Total	81,126	53,071	28,055
Total Resourcing and Payments	656,300	351,340	304,960

Appendix B: Expenses and Resources Table 2009–10

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 2009–10 $'000	Actual Expenses 2009–10 $'000	Variation 2009–10 $'000
Program 1.1: Security Intelligence			
Departmental expenses			
Ordinary annual services (Appropriation Bill No. 1)	405,518	375,815	29,703
Revenues from independent sources (section 31)	4,600	5,913	(1,313)
Expenses not requiring appropriation in the Budget year	100	100	–
Total expenses for Outcome 1	410,218	381,828	28,390

	2008–09	2009–10	
Average staffing level (number)	1,690	1,692	2

Appendix C: List of Proscribed Terrorist Organisations (30 June 2010)

Group	Initial Listing	Date last Re-listed[1]
Al-Shabaab	22 Aug 2009	
al-Qa'ida	21 Oct 2002	8 Aug 2008
Jemaah Islamiyah	27 Oct 2002	8 Aug 2008
Abu Sayyaf Group (ASG)	14 Nov 2002	3 Nov 2008
Jamiat ul-Ansar (JuA)	14 Nov 2002	3 Nov 2008
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	8 Aug 2008
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	3 Nov 2008
Kurdistan Workers Party (PKK)	17 Dec 2005	8 Sep 2009

Table 5: Proscribed Groups

1. Re-listing occurs every two years.

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	1
94(1A)(b)	The total number of warrants issued during the year under that Division	1
94(1A)(c)	The total number of warrants issued during the year under section 34E	1
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	5:48:03
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	2

Appendix E: Workforce Statistics

	2005–06	2006–07	2007–08	2008–09	2009–10
Ongoing Full-time	800	1,125	1,263	1,452	1,471
Non-ongoing Full time[1]	178	55	52	49	30
Ongoing Part time	50	94	108	116	134
Non-ongoing Part time	27	18	12	19	18
Non-ongoing Casual	55	64	57	54	39
Total	1,110	1,356	1,492	1,690	1,692

Table 6: Composition of workforce 2005–06 to 2009–10

1. Includes attachments, locally engaged staff and contractors/consultants

		2005–06	2006–07	2007–08	2008–09	2009–10
Band 1	Female	5	7	6	7	6
	Male	17	17	29	35	35
Band 2	Female	1	2	2	4	4
	Male	4	8	11	12	10
Band 3	Male	1	1	2	2	2
Total		28	35	50	60	57

Table 7: SES equivalent classification and gender 2005–06 to 2009–10 (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)	57	10	2	0	2	51
Senior Officers[3]	417	156	26	0	6	387
AO5[4]	570	284	41	0	5	335
AO1 – 4[5]	521	283	36	4	6	684
Information Technology Officers Grades 1 and 2	108	15	10	0	1	95
Engineers Grades 1 and 2	19	2	2	0	0	17
Total	1,692	750	117	4	20	1,569

Table 8: Representation of designated groups within ASIO at 30 June 2010

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
Women[1]	45.9	45.5	45.4	44.6	44.3
Non English Speaking Background	4.5	5.6	4.4	5.6	6.9
Aboriginal and Torres Strait Islander	0.4	0.3	0.3	0.2	0.2
People with a Disability	1.4	1.2	1.4	1.4	1.2

Table 9: Percentage of representation of designated groups in ASIO 2005–06 to 2009–10

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
AEO3	$115,881		
AEO2	$105,126	to	$115,881
AEO1	$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		
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 2010

Compliance Index

Part of Report	Description	Requirement	Page
	Letter of transmittal	Mandatory	iii
	Table of contents	Mandatory	v
	Index	Mandatory	149
	Glossary	Mandatory	147
	Contact officers(s)	Mandatory	back cover
	Internet home page address and Internet address for report	Mandatory	back cover
Review by Secretary	Review by departmental secretary (Director-General of Security)	Mandatory	vii
	Summary of significant issues and developments	Suggested	xvi
	Overview of department's performance and financial results	Suggested	xiii
	Outlook for following year	Suggested	3
	Significant issues and developments – portfolio	Portfolio departments – suggested	n/a
Departmental Overview	Overview description of department	Mandatory	ix
	Role and functions	Mandatory	ix
	Organisational structure	Mandatory	xi-xii, 75
	Outcome and program structure	Mandatory	xiii
	Where outcome and output structure differ from PB Statements/PAES or other portfolio statements accompanying any other additional appropriation bills (other portfolio statements), details of variation and reasons for change	Mandatory	n/a
	Portfolio structure	Portfolio departments – mandatory	n/a

Part of Report	Description	Requirement	Page
Report on Performance	Review of performance during the year in relation to programs and contribution to outcomes	Mandatory	Part 2[1]
	Actual performance in relation to deliverables and KPIs set out in PB Statements/PAES or other portfolio statements	Mandatory	Part 2, xiii, xiv, 59
	Performance of purchaser/provider arrangements	If applicable, suggested	n/a
	Where performance targets differ from the PBS/ PAES, details of both former and new targets, and reasons for the change	Mandatory	n/a
	Narrative discussion and analysis of performance	Mandatory	Part 2
	Trend information	Mandatory	Throug-hout
	Significant changes in nature of principal functions/services	Suggested	n/a
	Factors, events or trends influencing departmental performance	Suggested	Part 1
	Contribution of risk management in achieving objectives	Suggested	76
	Social justice and equity impacts	Suggested	n/a
	Performance against service charter customer service standards, complaints data, and the department's response to complaints	If applicable, mandatory	xiv, 56 78
	Discussion and analysis of the department's financial performance	Mandatory	xiii
	Discussion of any significant changes from the prior year or from budget	Suggested	n/a
	Agency resource statement and summary resources table by outcomes	Mandatory	133
	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	n/a

Part of Report	Description	Requirement	Page
Management Accountability			
Corporate Governance	Statement of the main corporate governance practices in place	Mandatory	73
	Names of the senior executive and their responsibilities	Suggested	n/a
	Senior management committees and their roles	Suggested	73-74
	Corporate and operational planning and associated performance reporting and review	Suggested	73
	Approach adopted to identifying areas of significant financial or operational risk	Suggested	76
	Agency heads are required to certify that their agency comply with the Commonwealth Fraud Control Guidelines	Mandatory	iii
	Policy and practices on the establishment and maintenance of appropriate ethical standards	Suggested	56
	How nature and amount of remuneration for SES officers is determined	Suggested	n/a
External Scrutiny	Significant developments in external scrutiny	Mandatory	54-56
	Judicial decisions and decisions of administrative tribunals	Mandatory	29, 78
	Reports by the Auditor-General, a Parliamentary Committee or the Commonwealth Ombudsman	Mandatory	n/a
Management of Human Resources	Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	Mandatory	65, 70
	Workforce planning, staff turnover and retention	Suggested	63, 69
	Impact and features of enterprise or collective agreements, determinations, common law contracts and AWAs	Suggested	70

Part of Report	Description	Requirement	Page
	Training and development undertaken and its impact	Suggested	66
	Occupational health and safety performance	Suggested	71
	Productivity gains	Suggested	xiii
	Statistics on staffing	Mandatory	63, 137
	Enterprise or collective agreements, determinations, common law contracts and AWAs	Mandatory	70
	Performance pay	Mandatory	72
Assets Management	Assessment of effectiveness of assets management	If applicable, mandatory	80, 85
Purchasing	Assessment of purchasing against core policies and principles	Mandatory	85
Consultants	A summary statement detailing the number of new consultancy services contracts let during the year; the total actual expenditure on all new consultancy contracts let during the year (inclusive of GST); the number of ongoing consultancy contracts that were active in the reporting year; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST). A statement noting that information on contracts and consultancies is available through the AusTender website	Mandatory	85
Australian National Audit Office Access Clauses	Absence of provisions in contracts allowing access by the Auditor-General	Mandatory	n/a
Exempt Contracts	Contracts exempt from the AusTender	Mandatory	n/a
Commonwealth Disability Strategy	Report on performance in implementing the Commonwealth Disability Strategy	Mandatory	71
Financial Statements	Financial statements	Mandatory	Part 6
Other Information	Occupational health and safety	Mandatory	71

Part of Report	Description	Requirement	Page
	Freedom of Information	Mandatory	78
	Advertising and Market Research	Mandatory	63
	Ecologically sustainable development and environmental performance	Mandatory	84
Other	Grant programs	Mandatory	n/a
	Correction of material errors in previous annual report	If applicable, mandatory	n/a
	List of Requirements	Mandatory	142

1. Part 3 has been removed in its entirety for the *Report to Parliament*.

Glossary

AAT	Administrative Appeals Tribunal
ACBPS	Australian Customs and Border Protection Service
ACC	Australian Crime Commission
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGS	Australian Government Solicitor
AGSVA	Australian Government Security Vetting Agency
AIC	Australian Intelligence Community
APS	Australian Public Service
AQI	al-Qa'ida in Iraq
AQAP	al-Qa'ida in the Arabian Peninsula
ASIO	Australian Security Intelligence Organisation
ASIC	Aviation Security Identification Card
ASIS	Australian Secret Intelligence Service
BLU	Business Liaison Unit
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive weaponry
CDPP	Commonwealth Director of Public Prosecutions
CSOC	Cyber Security Operations Centre
CTCC	Counter Terrorism Control Centre
DBCDE	Department of Broadband, Communications and the Digital Economy
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
DSA	Defence Security Authority
IGIS	Inspector-General of Intelligence and Security
IMA	Irregular Maritime Arrival

JAT	Jamaah Ansharut Tauhid
JI	Jemaah Islamiyah
LeT	Lashkar-e-Tayyiba
LTTE	Liberation Tigers of Tamil Eelam
MSIC	Maritime Security Identification Card
NAA	National Archives of Australia
NERE	National Extremist and Racist Extremist
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
OTS	Office of Transport Security
PIJ	Palestinian Islamic Jihad
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PKK	Kurdistan Workers Party
PM&C	Department of the Prime Minister and Cabinet
SCNS	Secretaries Committee on National Security
SES	Senior Executive Service
WMD	Weapons of Mass Destruction

General Index