ASIO Report to Parliament 2008–09

ISSN 0815-4562

Australian Government
Australian Security
Intelligence Organisation

Director-General of Security

12 October 2009

eA: 1141996

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 2009.

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

The Hon Robert McClelland MP
Attorney-General

Mr David Irvine AO
Director-General of Security

Director-General's Review

This year saw the most intense period of operational activity since 2005. ASIO detected and responded to a new alleged domestic terrorist cell, and the extent of Internet-enabled espionage as a rapidly growing threat to the national interest became more apparent.

The national response to these and other national security threats must be strong and effective. ASIO must continue to enhance its capability to detect and prevent threats from manifesting and to deliver the results expected by the Government and the people of Australia.

Next year will see the final stages of a carefully managed five-year enhancement program, which resulted from the review of ASIO's resourcing by Mr Allan Taylor AM in 2005. The Organisation will need to ensure its capability continues to evolve from 2010, when funding and growth levels stabilise. The security environment in which ASIO operates is a constantly shifting mosaic and the Organisation must be equally agile in response.

New and improved capabilities are one way to derive strength, but effectiveness is derived also from working with partners collaboratively and effectively to form holistic national security responses. The joint Australian Federal Police, Victoria Police, New South Wales Police, ASIO and New South Wales Crime Commission counter-terrorism operation that culminated with arrests on 4 August 2009 is one example of this increased interoperability and coordination.

Similar fusion is taking place in response to electronic espionage. Whereas our focus was once on nation states and their human agents, the threat is now more varied and today's response requires high-technology to be joined with traditional tradecraft. ASIO's counter-espionage expertise is being combined with specialist capability residing in other national security community agencies. Jointly we are working against this increasing threat to the integrity of Australian Government and commercial information systems.

For the foreseeable future, ASIO's first priority will remain preventing a terrorist attack on Australian soil and protecting Australians and Australian interests from terrorism overseas. As we saw in attacks in Mumbai and elsewhere, terrorists continue to adapt their tactics for strategic impact and in response to hardened security measures. For ASIO, these events, and the need again this year for preventive action within Australia, were sobering reminders of the importance of ongoing vigilance. For all Australians, they should be reminders of the danger of complacency when it comes to terrorism.

While an enduring feature of our security landscape, terrorism will not be the only national security challenge requiring ASIO's attention over the coming years. Today's increasingly interconnected world has great benefits, but it also provides new opportunities for state and non-state actors to advantage themselves at Australia's expense. Espionage and foreign interference, for example, threaten not only the

integrity of our national institutions but also our economic competitiveness and community cohesion. Like terrorism, espionage and foreign interference is enabled by technology and the free flow of people, goods and ideas across borders.

ASIO will need to continue to scan the horizon not just for new manifestations of existing threats, but also for new challenges. And we will need to ensure that we are positioned to protect Australia's national security both singly as the nation's security service, and jointly as a crucial component of Australia's overall national security capability.

I have joined an organisation that is capable and underpinned by a highly-dedicated group of officers. I am confident, therefore, that ASIO will not only remain steadfast in its efforts to protect Australia and Australians from today's threats, but also rise to meet the challenges of tomorrow.

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* (the ASIO Act). ASIO's primary function is to collect, analyse and disseminate security intelligence. The ASIO Act defines 'security' as the protection of Australia, its people and interests against:

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

The ASIO Act extends ASIO's responsibility for security intelligence beyond Australia's borders. The ASIO Act also includes, in the definition of security, Australia's security obligations to other 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 ASIO's Minister, the Attorney-General;
- assesses intelligence and provides advice to Government and beyond on security matters;
- investigates and responds to threats to security;
- maintains a national counter-terrorist capability; and
- provides security assessments, including visa entry checks and for access to classified material and designated security controlled areas.

Under the ASIO Act and other legislation, ASIO can be authorised to use special powers under warrant, including powers to intercept telecommunications, enter and search premises, and compel 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 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.

ASIO's Funding

Funding to ASIO in 2008–09 expressed in terms of total price of Outputs was $361.730m, an increase of $57.621m (19 percent) from 2007–08.

Revenue from Government increased $62m (21 percent) to $353m, from $291m in 2007–08 and $227m in 2006–07. The growth continues in 2009–10 with revenue from Government increasing $56m (16 percent) to $409m and total price of Outputs estimated to be $413m. This reflects the final stage of growth in staff and depreciation expense flowing from previous equity injections arising from the *Review of ASIO Resourcing* (the Taylor Review) in 2005.

ASIO received an equity injection of $71m in 2008–09, a reduction from significant equity injections in 2007–08 ($159m) and 2006–07 ($113m). This injection allowed for further substantial investment in ASIO's information technology infrastructure and the state and territory offices network, and the commencement of ASIO's new central office building.

Output	Actual 2007–08 $m	Estimated 2008–09 $m	Actual 2008–09 $m	Actual 2008–09 % of total
Output Group 1: Total	304.109	358.383	361.730	100

Table 1: Price of ASIO's Outputs

Customer Satisfaction

In 2009 ASIO interviewed representatives from key Commonwealth, state and territory and private sector agencies to seek feedback on their engagement with ASIO, the quality of ASIO advice and product, and ASIO's overall performance in meeting their requirements. The survey also looked to identify areas for further engagement or improvement in the relationship and services provided by ASIO.

Commonwealth customers generally considered their relationships with ASIO have improved. ASIO officers were seen to be more willing to assist and more focused on customer needs. Some customers said they would value expanding their existing network of contacts within ASIO. ASIO is facilitating this in response, and as part of a broader effort to ensure the Organisation is seamlessly integrated within Australia's national security architecture. ASIO will continue its successful Partnership Forum series and the program of attachments, which enable direct interaction between partner agencies and ASIO.

The Australian Federal Police and state and territory law enforcement agencies reported a highly satisfactory level of engagement with ASIO. In the last twelve months, these relationships have strengthened and are considered even more positive, useful and cooperative than previously reported. There has also been an improvement in engagement at the senior officer level. These agencies consider ASIO product and advice is valuable and relevant to their requirements. Continuing to develop ASIO's relationship with law enforcement agencies will remain a high priority for ASIO.

Private sector clients reported increasingly positive levels of engagement with ASIO, particularly via the Business Liaison Unit. ASIO is considered responsive and client-focused, which has instilled a high level of trust and confidence. These clients believe their decisions are well informed as a result of ASIO's reporting, which is regarded as timely and relevant.

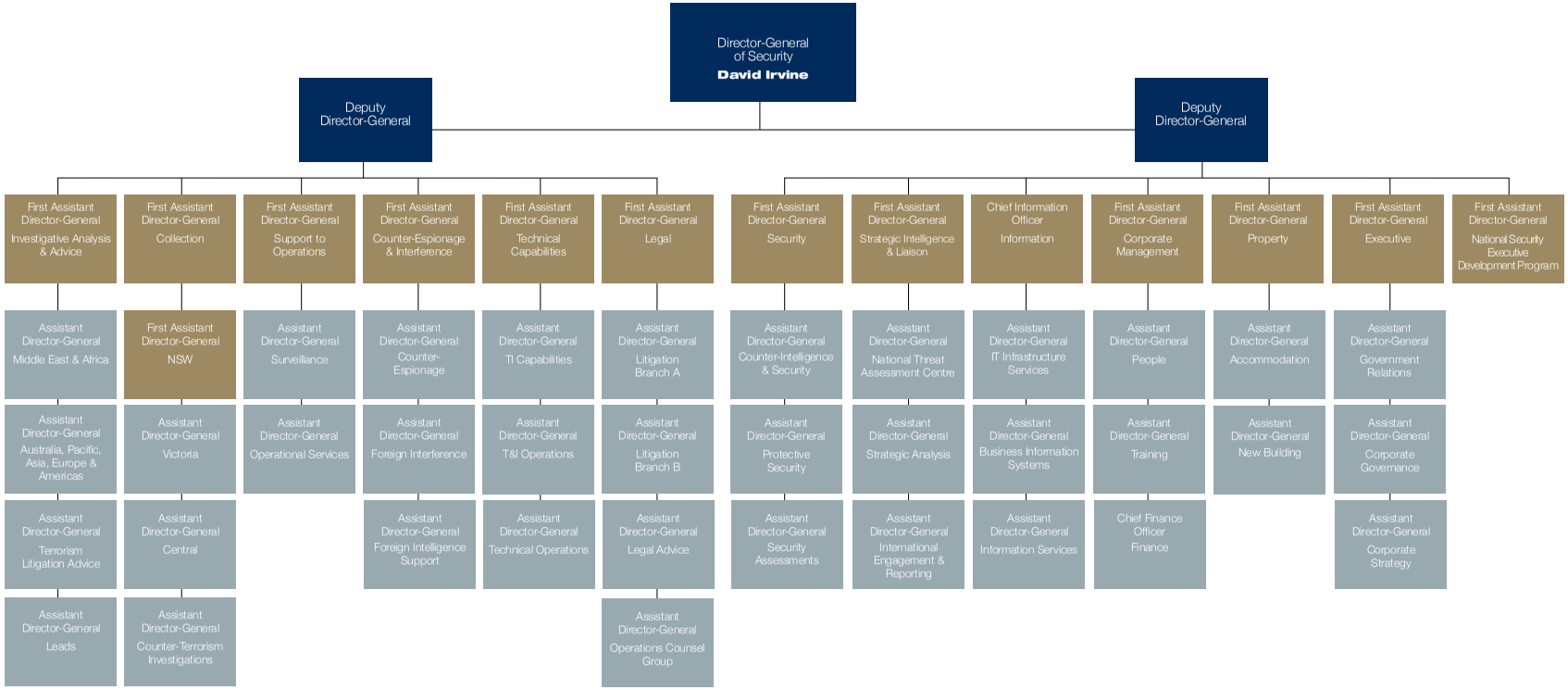

Figure 1: ASIO's Organisational Structure at 30 June 2009

INTRODUCTION

Guide to the Report

ASIO produces a classified and an unclassified Annual Report. Section 94 of the *Australian Security Intelligence Organisation Act 1979* (the 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 the Parliament within 20 sitting days of receipt.

ASIO is the only Australian intelligence agency to produce an unclassified *Report to Parliament*.

Guide to Outcomes and Outputs Structure

In support of the Australian Government's policy aim of 'a secure Australia in a secure region', ASIO contributes to the Government outcome: '*A secure Australia for people and property, Government, business and national infrastructure, and special events of national and international significance.'*

To achieve this outcome ASIO delivers and reports to Government against four identified outputs:

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

Executive Summary

The Security Environment

Australia's security environment evolved further in 2008–09, with new layers of complexity added to the threats from terrorism, espionage and foreign interference.

Within Australia, ASIO identified new extremists and ASIO's intelligence investigations revealed a range of terrorism-related activity – the most serious being alleged planning by a Melbourne-based group of Islamic extremists for an armed suicide assault on an Australian military facility.

The Middle East, South Asia and now East Africa are the primary sources of motivation and capability for extremists in Australia. Small numbers of Australians continue to look to conflict theatres overseas for inspiration and some aspire to participate in the violence or seek to learn from the tactics and techniques employed by extremists there.

Attacks in Islamabad, Mumbai, and Lahore in 2008–09 highlighted the enduring strategic intent of al-Qa'ida-inspired terrorism and the potential for Australians to be victims of attacks overseas.[1] These and other events reinforced ASIO's assessment that terrorism continues to be a persistent threat to Australia and Australian interests, and that the possibility of an attack in Australia remains.

The threat of hostile intelligence services exploiting Australian information systems was brought into sharper focus, with traditional espionage methods supplemented by new high-technology techniques. ASIO found further evidence of hostile intelligence services using the Internet as a means of appropriating confidential Australian Government and business information.

State-sponsored efforts to procure materiel and knowledge for weapons programs – including weapons of mass destruction – continued in 2008–09.

Communal violence within Australia remained, overall, a low level concern, and most protest activity was peaceful.

ASIO's Activities and Outcomes in 2008–09

ASIO made a strong contribution to Australia's national security efforts in 2008–09 through the collection, analysis and reporting of intelligence as well as through security assessment advice, protective security advice and border protection advice.

Counter-terrorism investigations remained ASIO's highest priority in 2008–09. However, counter-espionage, foreign interference and counter-proliferation were also high priorities.

ASIO continued to cooperate and collaborate extensively, both nationally and internationally, with a wide range of policy, security, intelligence and law enforcement agencies.

---

1 In July 2009 (shortly after the close of the reporting period), three Australians – including a senior Australian trade official based at the Australian Embassy in Indonesia – were killed in an attack on the JW Marriott Hotel in Jakarta. Other Australians were injured.

- ASIO provided advice to the National Security Committee of Cabinet and the Secretaries Committee on National Security on a number of security issues including counter-terrorism, counter-radicalisation, counter-espionage and cyber security. ASIO also contributed through the National Intelligence Coordination Committee to the development of the National Intelligence Priorities.
- ASIO strengthened partnerships with intelligence and law enforcement agencies, in particular the Australian Federal Police (AFP).
- ASIO continued to work closely with the other Australian intelligence agencies, particularly the Australian Secret Intelligence Service, the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation.
- ASIO increased its network of overseas representation, and as at 30 June 2009 had 316 approved liaison relationships with authorities in 122 countries.
- The audience for ASIO reporting expanded in 2008–09, and included 80 Commonwealth and state and territory customers within Australia.
- ASIO produced 2,738 reports and assessments in 2008–09, including 1,092 threat assessments and 138 threat analysis papers.
- ASIO continued to deliver high-quality strategic and thematic analysis for Australian decision-makers and policy agencies.
- ASIO increased its liaison with the private sector, with subscribers to the Business Liaison Unit (BLU) increasing by 40 percent in 2008–09. The BLU made over 200 security reports available for business subscribers on its website.

ASIO's border network of aviation and maritime liaison officers worked in close partnership with key aviation and maritime partners including the AFP, the Department of Immigration and Citizenship, the Australian Customs and Border Protection Service and airport and seaport authorities. ASIO continued to contribute to the security of Australia's borders through visa security assessments.

- In 2008–09, ASIO completed 59,884 visa security assessments including 1,466 assessments for protection visa applicants.
- ASIO issued adverse security assessments for two individuals seeking entry to Australia in 2008–09. The visa applicants were assessed to pose a security threat due to links to a terrorist group or a foreign government.

ASIO continued to provide high-quality protective security advice to clients including through protective security risk reviews, vulnerability assessments, ministerial office security reviews and technical surveillance counter-measures testing.

ASIO contributed to the Australian Government's 2008 *Review of E-Security*, working with DSD and the AFP to produce a wide-ranging classified assessment of the electronic threat environment.

ASIO's expertise in major event security planning was used to provide security advice in support of World Youth Day (Sydney), the Beijing Olympic and Paralympic Games, and the Asia-Pacific Economic Cooperation forum, Peru.

ASIO continued its major investment in the development and delivery of technical collection capability and worked closely with domestic and international partners, including industry.

In 2008–09, ASIO continued to build upon its long-standing program of confidential contact with leaders and influential members of various ethnic and religious community groups in Australia.

ASIO continued to operate under a rigorous oversight and accountability framework. The Inspector-General of Intelligence and Security conducted a series of monitoring, inspection and inquiry activities and was satisfied there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or human rights.

In 2008–09, ASIO broadened its engagement outside of government, building links with industry, business and research institutions.

- The Director-General of Security addressed conferences and audiences from business, government and academia. Nine of these speeches are available on the ASIO website.
- ASIO's BLU gave briefings to relevant industry forums, and coordinated an 'Executive Program' for the Director-General of Security to brief chief executives of Australia's largest corporations.

Recruitment remained a high priority in 2008–09.

- ASIO's net staffing increased by 13 percent to 1,690 – ASIO is on track to achieve staffing levels of approximately 1,800 by 2010–11, consistent with recommendations made in the *Review of ASIO Resourcing* (the Taylor Review) in 2005.
- ASIO increased its investment in training in 2008–09, to support the needs of a growing workforce with a focus on the development of management and leadership skills, language training and specialist training for ASIO's investigative work.

Construction work commenced on ASIO's new special-purpose, high-security central office. The new building is being designed and constructed in partnership with the Department of Finance and Deregulation. It is expected to be completed by 2012.

Part One THREATS AND THE SECURITY ENVIRONMENT 2008–09

Threats and the Security Environment 2008–09

Security threats to Australia and Australian interests evolved further in 2008–09. As in previous years, the new dimensions of threats built on – rather than replaced – existing elements, adding new layers of complexity to the challenges of terrorism, espionage and foreign interference.

Terrorism

Global Terrorism Environment

Terrorism remains a serious and immediate threat to Australia, Australian citizens and Australian interests globally. Terrorist intent is typically strategic, its targets tactical and the destruction indiscriminate. Terrorism is expected to be a destabilising force for the foreseeable future and a persistent feature of the global threat environment.

The greatest terrorism threat is from the violent jihadist movement comprising core al-Qa'ida in Pakistan and Afghanistan, Sunni Islamic extremist groups allied or associated with al-Qa'ida, and individuals or groups motivated by the violent jihadist ideology. In recent years, this violent jihadist movement has suffered setbacks through the death or imprisonment of many of al-Qa'ida's leading figures. But core al-Qa'ida remains resilient and committed to achieving its political goals through extreme violence. Of particular concern are safe havens, such as in the Federally Administered Tribal Areas of Pakistan and potentially now also in Somalia. These allow violent jihadist groups to recruit, incite, train, and prepare for terrorist attacks internationally. The strategic importance of defeating al-Qa'ida in Pakistan and Afghanistan is central to strategic success against terrorism.

Al-Qa'ida-inspired terrorism is not, however, the only terrorism concern with international implications. Shi'a extremism, in particular that affiliated with Lebanese Hizballah's External Security Organisation (ESO), also has global reach and – to a lesser extent – influence.

In terms of terrorist tactics and capability, improvised explosive devices continue to be the weapon of choice, followed by firearms and incendiaries. Small, person-carried bombs, vehicle-bombs and armed assault are favoured tactics. The attackers in Mumbai in November 2008 employed explosives – including grenades – and small arms in tactical assaults, indiscriminate killings and siege-hostage situations. These tactics are not new, but the scale and operational complexity of the Mumbai attacks were notable and had not been seen previously in India.

Terrorist groups such as al-Qa'ida continue to maintain an interest in chemical, biological, radiological or nuclear weapons.

Terrorists will continue to target places where population is concentrated, including mass gatherings, and critical infrastructure.

Terrorism and Australia

In 2008–09, Islamic extremists again identified Australia as a target for terrorism. In October 2008, an audio interview with the leader of al-Qa'ida in Iraq, Abu Hamzah al-Muhajir, contained a thinly veiled threat against the United Kingdom, United States and Australia 'about what's coming' on their home 'turf'. In November 2008, a Taliban video statement warned the United States, Australia and several other countries with military deployments in Afghanistan of future attacks unless they withdrew their forces.

Major Incidents and Impact on Australians

Two significant terrorist attacks overseas in 2008–09 involved Australian civilians. In November 2008, two Australians were among the over 165 people killed in attacks in Mumbai and Australians were among the more than 300 injured. On 3 March 2009, five Australians were travelling in the Sri Lankan cricket team convoy in Lahore, Pakistan, when it was attacked by assailants using small arms, rocket launchers and hand grenades.[2]

Local Terrorism

The number of known Islamic extremists – those willing to use violence in pursuit of political objectives – in Australia is very small but significant and did not change substantially in 2008–09. Local extremists can be particularly difficult to detect and their potential for harm is disproportionate to their small number. Overseas experience demonstrates that small groups with relatively unsophisticated methods can cause substantial destruction and disruption. Successful attacks can also embolden others.

New extremists were identified in Australia in 2008–09. Their alleged intent to participate in terrorism in Australia or overseas – and for some allegedly to contemplate suicide – underscores the enduring propensity for al-Qa'ida-inspired ideology to resonate strongly within larger but still small groups in Australia.

2 In July 2009 (shortly after the close of the reporting period), three Australians – including a senior Australian trade official based at the Australian Embassy in Indonesia – were killed in an attack on the JW Marriott Hotel in Jakarta. Other Australians were injured.

Mumbai attacks

The 26–29 November 2008 attacks in Mumbai were the most significant terrorist incident in 2008–09 in scale, complexity and diversity of targets. At least 165 people, including two Australians, were killed in the attacks and more than 300 were injured. Planned and executed by Pakistan-based Islamic extremist group Lashkar-e-Tayyiba (LeT), the incident lasted some 60 hours. It paralysed India's usually vibrant commercial and entertainment capital, and played out under the intense gaze of the international media. The terrorists combined a range of relatively simple but highly effective tactics, including armed assault, grenades and explosives, indiscriminate killing, and hostage sieges.

The attacks were intended to damage the Indian Government and undermine investor confidence in the Indian economy, and possibly precipitate a hostile response by India to derail the Kashmir peace process.

Arriving by sea in southern Mumbai, a group of ten heavily armed militants separated into five pairs and proceeded via taxi or on foot to a range of pre-selected targets, in some cases killing while in transit. The five main targets of the attacks were all located within a three mile radius in southern Mumbai and included two hotels, a café, a train station and a Jewish centre. The inclusion of the Taj Mahal and Oberoi hotels and the Nariman House as targets was a departure from the LeT's previous attacks in India, which have primarily focused on public spaces or places of religious or political significance. Killing was indiscriminate and included locals and foreigners.

The mobile-unit style of small-arms attack used in Mumbai was not new. However, the combination of elements on such a scale and against such a range of targets in a single attack had not been seen before. The protracted spectacle of the attacks and their highly disruptive nature are likely to inspire others.

ASIO deployed officers to New Delhi immediately after the attacks. Working closely with Indian authorities, these officers facilitated the flow of information to the National Threat Assessment Centre and other customers in Australia.

Mumbai 2008 *(photo courtesy of AAP)*

Radicalisation and Extremism in Australia

Radicalisation is the process by which a person's beliefs or ideas move from those held by the majority towards a more extreme world view, often striving for far-reaching societal change. Extremism is one possible end point of radicalisation and includes the acceptance and willingness to use violence.

There is no single path to becoming an extremist. However, in most cases, the driver for individuals to transition from retaining grievances and holding beliefs to taking action lies in the dynamics of small, isolated groups.

Violent jihadist extremists in Australia – like those elsewhere in the world – possess an identifiable 'mindset' composed of a particular world view, including an historical narrative that the West has been hostile to Muslims since the emergence of Islam, and an underlying rejection of secular, Western society. Despite being factually incorrect, the single historical narrative is particularly important because to them it proves Islam and Muslims are persecuted by the West.

ASIO is conducting a variety of activities to help identify individuals and groups intent on acting on extremist beliefs. These range from constructive long-term engagement with influential community and religious figures and associations, through to investigations relating to specific extremists or extremist threats.

Overseas Links and Influences

Australia's security environment is heavily influenced by international events. Overseas links and events can provide the source of inspiration or motivation for activity in Australia. Some of the links are more direct and can include overseas extremists in contact with Australians or Australians seeking to gain terrorism training or other capability for use in Australia or overseas.

The Middle East, South Asia and now East Africa are the primary sources of motivation and capability for extremists in Australia. Small numbers of Australians continue to look to theatres of conflict overseas for inspiration; some aspire to participate in the violence or seek to learn from the tactics and techniques employed by extremists overseas.

There has been no reinvigoration of coordinated support from Australia for Jemaah Islamiyah (JI) – or any other extremist group – in South-East Asia.

The pattern of Australians wishing to travel overseas for terrorism-related activity was similar to previous years, with a small number acting on their intent. Some participated in combat overseas.

LET and Links to Australia

Lashkar-e-Tayyiba (LeT) – the group responsible for the November 2008 Mumbai attacks – was originally established to oppose India's control of the disputed Kashmir region. LeT aligned itself ideologically and operationally with al-Qa'ida, particularly after 11 September 2001. The Mumbai attacks were the most recent – and most destructive – demonstration of LeT's commitment to al-Qa'ida's global jihad objectives.

Australian links to LeT were evident in October 2003 when ASIO became aware of a group in the early stages of planning a terrorist attack in Australia.

The central figures were Faheem Khalid Lodhi – an Australian citizen who had held a leadership position in an LeT training camp in Pakistan – and Willy Brigitte, a French national and LeT-trained explosives expert sent to Australia to work with Lodhi. Lodhi and Brigitte were consequently convicted of terrorism offences, the latter in France.

Regional Trends and Developments

Afghanistan and the Subcontinent

The threat environment in much of South Asia remains grim.

In Afghanistan, suicide bombings against Afghan Government interests and international forces are a key militant tactic. Foreign civilians are at constant threat from kidnapping and assassination.

A number of militant groups operate in Afghanistan, all of which seek to undermine the Afghan Government and reject Western influence. Afghanistan has also attracted individual Islamic militants from around the world, including Australians.

Islamic militants in Pakistan continue to conduct major attacks in urban areas. The 20 September 2008 attack on Islamabad's Marriott Hotel underlines the threat to Western interests and the determination of extremists to destabilise the government of Pakistan. The Marriott Hotel attack used the largest ever bomb in a suicide vehicle bombing. It killed some 60 people of various nationalities, injured around 260 more and destroyed much of the hotel.

Politically motivated violence is a routine feature of the Indian security environment, with frequent violence from separatists, Maoists and Islamic militants. Four attacks in July and September 2008 were claimed by Indian Mujahidin (IM). IM's near-simultaneous bombings in urban centres have focused on Indian interests, but it also targets sites popular with tourists and expatriates. There is an increased potential for Westerners to be targeted in terrorist attacks in India, as evidenced by the 26–29 November 2008 attacks in Mumbai in which two Australians were killed and three injured.

In late May 2009, Velupillai Prabhakran and most of the senior members of the Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka were killed, signifying military defeat for the group. The last surviving senior figure, Selverasa Pathmanathan, was appointed leader and publicly called for the group to renounce violence.

The deaths of its core leadership in Sri Lanka, and Pathmanathan's intention to adopt a political path to its goals, leaves the LTTE without adequate direction or motivation to mount a coordinated or effective armed offensive. But some survivors of the military campaign may revert to terror tactics in an effort to pursue the LTTE's separatist agenda.

Middle East and Africa

Somalia emerged as an area of major terrorism concern in 2008–09. The volatile security environment there is conducive to the growth of Islamic extremist groups and its profile as a battle front for al-Qa'ida's offensive has increased significantly. Al-Shabaab – a loose alliance of clan-based militias formerly aligned with the Union of Islamic Courts – conducted coordinated suicide-vehicle bombings in northern Somalia on 29 October 2008. At least 28 people were killed and 30 others wounded. The simultaneous suicide attacks occurred in areas of northern Somalia which had previously been considered safe for aid workers. One of the suicide bombings took place inside the United Nations Development Program compound. The attacks were aimed at destabilising transitional governing bodies and repelling foreign involvement in Somalia.

Al-Shabaab expanded its influence in Somalia during the first half of 2009 and, together with other Islamic militant groups, engaged in a violent insurgency against the Transitional Federal Government of Somalia and African Union peacekeeping forces. The group's objectives of repelling foreign forces and establishing an Islamic state have resonated with elements of the Somali diaspora, including in Australia, as well as with Sunni Islamic extremists around the world, including al-Qa'ida. Some al-Shabaab members subscribe to al-Qa'ida's global jihad agenda and maintain the intent to conduct terrorist attacks in, and outside, Somalia.

The Middle East threat environment remains highly volatile. Sunni Islamic extremists, particularly those affiliated with al-Qa'ida, planned or prepared for a range of attacks across the region – many of which were disrupted. Militants continued to attempt to undermine the effective governance of countries in the region and to attack Western interests directly.

The security environment in Yemen deteriorated considerably in 2008–09. The al-Qa'ida-affiliated group, al-Qa'ida in the Arabian Peninsula (AQAP), which relocated to Yemen as a result of disruption by Saudi authorities, is increasingly active.

On 17 September 2008, AQAP conducted a sophisticated attack against the United States Embassy in the Yemeni capital of Sana'a using vehicle-borne improvised explosive devices, suicide bombers and small arms. The attack demonstrated the group was capable of attacking high-profile, hardened Western targets. The group also claimed responsibility for the March 2009 suicide attack against South Korean tourists in Yemen. A second suicide attack against a South Korean delegation was attempted three days later.

Extremists remain active in Syria and Lebanon; many of them have participated in the jihadist insurgency in Iraq.

Despite the failure of the Lebanese Hizballah-led coalition to gain a majority at the 7 June 2009 parliamentary elections, Lebanese Hizballah remains the strongest political organisation and armed group in Lebanon.

South-East Asia

Extremists linked to key JI operative, Noordin Mohammad Top, remained the most significant threat to Western interests in Indonesia. Mention of the Bali bombers' martyrdom in a 1 December 2008 statement by al-Qa'ida's second in command, Ayman al-Zawahiri, would have provided encouragement to South-East Asian extremists keen to have their efforts recognised on the global stage.

JI more broadly remains in a consolidation and rebuilding phase but has not abandoned its intent to achieve political and social change through violence. It remains, therefore, a serious terrorism concern.[3]

Terrorism in Thailand is mostly limited to a violent separatist insurgency in the Muslim-dominated southern provinces. Australian and other Western interests have not been targeted specifically in the violence.

There are ongoing hostilities in the Philippines between the Moro Islamic Liberation Front and the Philippines Government.

Espionage and Foreign Interference

Espionage is not defined in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), but criminal offences relating to espionage are set out in Division 91 of the *Criminal Code Act 1995* (Cth) and in the *Crimes Act 1914* (Cth).

Some espionage can arise from foreign interference activity, where a country's foreign intelligence service finds opportunity to cajole or coerce into cooperation one of its former nationals with access to sensitive Australian Government information. The original purpose of their targeting may not have been directed at espionage, but intelligence services are opportunistic and will often try to turn such opportunities to their advantage.

In other cases, espionage arises from deliberate efforts by foreign intelligence services to penetrate governments, their intelligence services, their departments and agencies, and strategic sectors of industry in pursuit of secret intelligence or commercial and economic advantage.

Australia remained a target for espionage in 2008–09.

3 The 17 July 2009 near-simultaneous bombings of the JW Marriott and Ritz Carlton hotels in Jakarta carried all the operational signatures of Noordin Mohammad Top. ASIO had consistently assessed that Top would attempt another anti-Western attack in Indonesia when he – or a trusted associate – considered it operationally feasible to do so, but there was no intelligence to forewarn of the attacks. Top and three of his associates were killed during an Indonesian National Police counter-terrorism operation in Solo, Central Java, on 17 September 2009.

Acts of foreign interference are defined in section 4 of the ASIO Act. Most acts of foreign interference investigated by ASIO are activities carried out by a foreign government or one of its instrumentalities, are clandestine or deceptive, and are carried out for intelligence purposes, in order to affect political or governmental processes, or are otherwise detrimental to Australia's interests. Some acts of foreign interference involve threats to a person and do not need to be clandestine or deceptive to fall within ASIO's mandate.

Australia has a significant history of foreign diplomats and officials collecting information on, and sometimes actively targeting, individuals in Australia who are perceived as dissident, disloyal, or otherwise likely to act in ways unwelcome to their country's government. Some of this activity is conducted quite overtly in the course of regular consular or community liaison by foreign officials. Other activity is covert and carried out by foreign intelligence officers or their contacts, co-optees and agents in the community. Some genuine diplomats undertake intelligence tasks on behalf of their government.

Promotion of Communal Violence

No information came to ASIO's attention in 2008–09 to indicate significant ongoing tensions between any community groups within Australia. ASIO was alert to the potential for communal violence as police investigated criminal activity against Indian students in Australia. Specific incidents outside or within Australia have the potential to cause short-term tensions resulting in some violence between communities. Usually the communities engage in lawful and peaceful protest action to demonstrate their concerns.

Nationalist extremist and racist extremist groups did not undertake organised or premeditated violence in Australia towards ethnic or religious communities in 2008–09.

Violent Protest

Most protest activity in Australia is peaceful and lawful and therefore not of concern to ASIO. Section 17A of the ASIO Act mandates that the Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent. However, a small number of individuals consider the promotion and use of violent protest tactics are justified in order to influence government policy or to achieve other political ends. This activity can fall within the definition of politically motivated violence in the ASIO Act and, therefore, be of interest to ASIO.

No significant violent protest occurred in Australia in 2008–09.

Proliferation

ASIO's counter-proliferation work focuses on detecting and preventing attempts to exploit Australia's industrial, technological and educational resources for the illicit development of weapons of mass destruction (WMD).

Australia has continued to increase its legislated obligations to ensure compliance with various United Nations Security Council Resolutions aimed at preventing the spread of WMD, with particular emphasis on Iran.

Outlook for the Security Environment

Terrorism

Australia will remain a terrorist target for the foreseeable future. Within Australia, terrorism-related activity will continue. Extremist ideology will continue to resonate with a small but dangerous minority, so there is a high likelihood of local terrorist groups emerging from time-to-time. Some Australians will continue to support extremism financially, logistically or by involving themselves in terrorist operations in Australia, or overseas.

Overseas terrorist groups might seek to conduct operations in Australia, either unilaterally or by seeking support locally. Overseas groups targeting Australia are more likely, however, to attack in their home country – as has been the case in Indonesia.

Australians and Australian interests overseas will continue to be among those indiscriminately targeted by terrorists – as in Mumbai and Indonesia.

The Middle East is likely to remain the global origin of terrorism threats and extremism. It will continue to provide the major focus and inspiration for extremists in Australia. Concerns about Israel-Palestinian conflict and United States influence in the Middle East will continue to sustain the ideology of extremists.

Continued instability and extremism in East Africa, mainly Somalia, is a growing concern to Australia. It is likely the continued instability will see an increased threat of terrorist attacks against Western interests in some East African countries.

Despite counter-terrorism successes, extremists with the desire to plan and conduct terrorist attacks, and an ability to build bombs, pose a continuing threat in Indonesia. JI is currently in a consolidation and rebuilding phase but has not abandoned its violent Islamist goals. JI has never been the only player in terrorism in Indonesia and even attacks ascribed to JI involved individuals drawn from a variety of extremist organisations. The terrorism environment in Indonesia remains fluid, and provides new avenues for Australia-based sympathisers to support Islamic extremism in South-East Asia.

Ongoing instability in Pakistan's tribal areas creates a fertile operating environment for extremist groups who pose a threat to Western interests in Pakistan and internationally. Lashkar-e-Tayyiba (LeT) – particularly given its previous links to Australia – will remain a particular concern. LeT remains focused on destabilising the Pakistan and India peace process and the Mumbai attacks demonstrated a willingness to target Western interests in India to achieve this goal. This is particularly noteworthy in light of the Commonwealth Games to be held in New Delhi, India in 2010.

ASIO expects fundraising for the LTTE to continue, but at a much reduced level. At this time it is unlikely LTTE members will target Sri Lankan interests in Australia for acts of violence. Some LTTE members may seek to enter Australia to escape Sri Lankan Government scrutiny.

Espionage and Foreign Interference

Espionage and foreign interference directed against Australia and Australian interests will continue. New technologies will allow new and different forms of undeclared intelligence activity, but the tried and true methods of cultivating, recruiting and running human sources with access to confidential information, secrets and sensitive technology will continue.

Australia will remain an important target as a source of intelligence not least because we are a close United States ally; active in the Asian region; suppliers of energy, mineral resources and technology; a potential source of commercial information and influence; and home to people who may be viewed by foreign governments as dissidents or separatists. Global commercial and economic competition – for resources, energy, technologies and competitive advantage – will blur the boundaries between nation-state and commercially driven espionage and require ASIO to broaden its role outside traditional counter-espionage boundaries.

Electronic attacks via the Internet occur frequently, originate from a range of sources and will persist.

Violent Protest and Communal Violence

Most issue motivated groups will continue to use peaceful and non-violent disruptive protest tactics. A very small proportion of activists continue to believe violent protest tactics are an effective means of influencing government and business decision-makers. These individuals are likely to plan for violent protest activity at selective anti-war and anti-globalisation protests.

Proliferation

Countries of proliferation concern will continue to adapt and evolve their procurement activities to thwart WMD control efforts. Australia will remain of interest to them, including because of our technologically advanced industry and military, strategic alliances and world class educational facilities. ASIO expects the need for counter-proliferation intelligence support for regulatory and enforcement agencies to increase. ASIO also expects an increase in the need for its advice on WMD matters in general.

Part Two OUTPUT PERFORMANCE

PART TWO

Output 1: Security Intelligence Analysis and Advice

Parts of this performance report have been excluded from the unclassified *Report to Parliament* for reasons of national security.

Analysis in ASIO

As both a collection and assessment agency, ASIO's analytical capability is crucial to its ability to investigate, report and advise on national security matters.

Some ASIO analysis is strategic and thematic, for example, on Australia's security environment or extremism and radicalisation in Australia. Other analysis is highly tactical and aims to reveal the significance of specific detail, relationships and linkages. In either case, the intelligence being analysed is often disparate and incomplete, providing only partial insight into complex intelligence questions.

ASIO's analytical capability is supported by a range of information and analysis systems and techniques. Expert knowledge and sound reasoning along with an ability to express findings clearly are the keys to good analysis. ASIO draws from a long history of examining threats to Australia, particularly from terrorism and other forms of politically motivated violence, and espionage and foreign interference. ASIO places a significant premium on advanced training for analysts in order to develop and maintain their skills and knowledge.

Some ASIO analysis forms the basis of ASIO intelligence advice. It is provided to Commonwealth and state and territory governments – and increasingly the private sector. Other analysis supports and drives ASIO – and partners' – intelligence investigations and operations. It might reveal a new lead, provide operational insight or be crucial to the planning or implementation of an intelligence operation.

ASIO analysts and collectors work together closely with regular feedback and evaluation on the extent to which collection is meeting analysis and assessment requirements. This helps ensure collection efforts are focused, carefully prioritised and their value maximised. It also produces an effective cycle whereby assessment priorities drive collection, collection is supported and informed by analysis, and collection and analysis are combined to provide reporting and advice that contributes to Australia's national security.

ASIO's international liaison relationships and domestic partnerships contribute substantially to ASIO's analytical capability. As well as being an important source of intelligence and information, these partnerships enable assessment, analytical techniques and tools to be exchanged, ideas shared and judgments tested. International liaison arrangements are particularly important for threat assessment, as they provide information on specific threats that would be otherwise unavailable. Analytical exchange is also an important driver and facilitator for greater operational and diplomatic exchange between Australia and other countries.

Intelligence Reporting

ASIO produced 2,738 reports and assessments in 2008–09. The audience for ASIO reporting is diverse and expanded in 2008–09. It now includes some 80 Commonwealth and state and territory agencies and departments within Australia, as well as additional foreign liaison partners in 60 countries.

Some security intelligence reporting is strategic and assists primarily Ministers and policy-makers. Other reporting is tactical and critical to calibrating operational threat responses, including by law enforcement and agencies such as the Department of Foreign Affairs and Trade (DFAT). ASIO's classified threat assessments form the basis of the terrorism section of DFAT's Travel Advisories.

In May 2009, ASIO launched a new product, the *ASIO Brief*, designed specifically to bring key security intelligence assessments and operational developments to the attention of the highest level decision-makers.

ASIO produced double the number of *Insight* reports compared with the previous year, a reflection of increased demand for this focused executive level product that provides strategic context on issues of current or emerging security concern.

ASIO also continued to deliver high-quality strategic and thematic analysis for Australian decision-makers and policy agencies.

ASIO's National Threat Assessment Centre (NTAC) is responsible for 24/7 coordination and analysis of threat-related intelligence. Threat assessments report on threats to Australia's domestic and overseas national security interests, threats to the interests of foreign countries in Australia, the threat from foreign intelligence services and threats to major events. Threat assessments are also used by Commonwealth and state and territory authorities to determine appropriate levels of protective security resourcing and response. In 2008–09, NTAC produced 1,594 reports, including 1,092 threat assessments and 138 threat analysis papers.

Intelligence Advice

In addition to regular intelligence reporting, ASIO draws from its intelligence sources and expertise to provide a range of advice that contributes to Australia's national security efforts. Some advice contributes to official processes – such as visa and other security checks – and other advice is in response to issues of current or emerging concern.

National Security and Intelligence Policy Advice

At the strategic level, ASIO provides intelligence advice to the Australian Government through a range of high-level national security policy and coordination forums, including the National Security Committee of Cabinet (NSC), the Secretaries Committee on National Security (SCNS), the National Intelligence Coordination Committee (NICC), and the Homeland and Border Security Policy Coordination Group (HPCG).

In 2008–09, ASIO provided advice to NSC and SCNS on a number of security issues including counter-terrorism, counter-radicalisation, counter-espionage, and cyber security.

The Director-General of Security participates in NSC meetings and is a member of SCNS.

The Director-General of Security is also a member of the NICC, which was established following Prime Minister Rudd's 4 December 2008 National Security Statement. In early 2009, ASIO contributed through the NICC to the development of National Intelligence Priorities, which provide an intelligence collection management framework incorporating foreign, defence, security and transnational law enforcement intelligence issues.

ASIO also supported the development and coordination of policy on homeland and border security issues through participation in the HPCG.

Proscription-Related Advice

The *Criminal Code Act 1995* allows the proscription of a terrorist group 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 it is directly or indirectly engaged in preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not the 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).

ASIO provides the Attorney-General with a 'statement of reasons' that details why a group should be listed under the regulations. ASIO assesses a range of factors when considering organisations for proscription, including – but not limited to – ideology, engagement in terrorism, links to other terrorist networks, threats to Australian interests, proscription by the United Nations or other countries and whether the group has been engaged in some form of peace process. The statement is drafted from unclassified and publicly available information but is informed by all information available to ASIO, including classified reporting.

ASIO provided statements of reasons on 13 groups that were re-proscribed in the reporting period. Also in 2008–09, and following review of all proscribed groups, the Attorney-General deemed that two groups – the Armed Islamic Group (GIA) and the Egyptian Islamic Jihad (EIJ) – no longer met the statutory test for proscription. At the end of the reporting period there were 17 groups proscribed in Australia (see Appendix A).

Advice on Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Weaponry

Demand for ASIO advice on CBRNE-related issues increased in 2008–09. Typically produced in close cooperation with the Australian Federal Police (AFP) and the Defence Intelligence Organisation, ASIO provided reports to counter-terrorism forums and external agencies, which assisted the implementation of both operational and policy measures to reduce the risk posed to Australia by CBRNE terrorism.

Advice to Business

ASIO's Business Liaison Unit (BLU) provides an interface between ASIO and Australia's private sector. The BLU distributes unclassified security reporting to businesses in

Australia to enable them to understand better the security environment and the threats they face, and assist them with security planning.

The BLU draws from the full range of ASIO's information holdings and expertise, including the NTAC, ASIO's Critical Infrastructure Protection area, and international liaison reporting. It distributes unclassified *Business Security Reports* covering a variety of domestic and international security topics. The BLU also provides information intended to help develop businesses' security management capability. Such reporting covers physical, personnel and information security strategies.

BLU reports are available via a secure website offered free to businesses on a subscription basis. Subscribers also receive a quarterly *BLU Bulletin*, which provides news and updates about ASIO's work.

The number of subscribers to the BLU website continued to grow steadily during 2008–09, with 680 subscribers compared with 398 in 2007–08. There was significant interest from the transport sector (aviation, maritime, freight, and mass-transit), the energy and resources sector (exploration, production, consulting engineering), banking and finance, telecommunications, stadium operators, shopping centres, property management and utilities. The BLU increased the number of security reports available for business subscribers on the website to over 200, compared with 140 in 2007–08.

BLU representatives liaise with industry associations to identify speaking opportunities and to contribute to trade publications and journals. These engagements cover all designated critical infrastructure sectors and specialist sectors such as the Plastics and Chemicals Industry Association and the Australian Hotels Association. The BLU also coordinates an 'Executive Program' where the Director-General of Security briefs chief executives of Australia's largest corporations. This program is intended to raise security awareness at the most senior levels of industry.

Australian Government
Australian Security Intelligence Organisation
Business Liaison Unit

ASIO

BLU BULLETIN

INFORMING THE PRIVATE SECTOR SINCE 2006 – ISSUE 9 QUARTER 1 2009–10

In this issue:

ASIO Director-General's foreword

It is my pleasure to introduce this latest version of the BLU Bulletin; the first for the new financial year 2009/10. It is encouraging to find ASIO's collaboration with business is well established and indeed growing.

The recent completion of the Report into Homeland and Border Security, followed by the Prime Minister's inaugural National Security Statement, highlighted the importance of building the intelligence community's relationship with business. ASIO's Business Liaison Unit will continue to help business stay abreast of trends in Australia's national security environment, using the combined resources of ASIO and our close partner agencies overseas. In addition to domestic and international threat reporting, BLU website subscribers should also see a continued emphasis on tactical security reporting. This information is intended to help business build its own capability to counter particular security threats, drawing on ASIO's own experiences.

...continue to help business stay abreast of trends...

As a security organisation with 60 years of expertise in areas such as information, protective and personnel security, ASIO is in a good position to translate its risk management principles into a workable business context.

The BLU of course welcomes ideas from our website subscribers on new reporting topics and ways that we can improve the BLU service. ■

Australian Government
Australian Security Intelligence Organisation
Business Liaison Unit

ASIO

BLU BULLETIN

INFORMING THE PRIVATE SECTOR SINCE 2006 – ISSUE 8 QUARTER 4 2008–09

In this issue:

Foreword

On 27 February 2009, Paul O'Sullivan completed his term as Director-General of Security having accepted the role of High Commissioner to New Zealand. Paul has been replaced by David Irvine, most recently Director-General, Australian Secret Intelligence Service (ASIS) who commenced with ASIO on 30 March 2009.

David Irvine had been Director-General of ASIS since early 2003. He is a career diplomat who joined the Australian Foreign Service in 1970. David's postings included Rome, Jakarta (twice), Beijing and Port Moresby. He served as Australia's Ambassador to the People's Republic of China, and concurrently to Mongolia and the Democratic People's Republic of Korea.

Given his long-standing and productive engagement with ASIO in his capacity as Director-General of ASIS, David is well-placed to take on the position of Director-General of Security. He will bring a depth and breadth of experience directly relevant to ASIO. ■

WEBSITE UPDATE

During 2009 the Business Liaison Unit will be upgrading our website. This will be more than just a fresh coat of paint – we are aiming to increase the usability and functionality of the website. For example, the BLU will look to add new features, such as automatic email notifications when new information or reporting is added to the website.

To ensure that the website remains relevant and useful we are seeking your input. Feel free to email us at blu@asio.gov.au and tell us what you like or don't like about the existing website and any new additions you wish to see built into the redesigned website.

Stay posted for further updates on the new BLU website as 2009 progresses.

BLU Bulletin

The Register of Australian Interests Overseas

The Business Liaison Unit (BLU) recently launched the Register of Australian Interests Overseas in conjunction with the National Threat Assessment Centre (NTAC). The Register allows businesses to provide ASIO with details of their interests overseas. Information held on the Register includes the type of facility, number of staff (including Australian nationals), location, and emergency contact details.

The information is collated in ASIO's secure network, together with details of the Australian Government's own overseas interests. The information allows NTAC analysts to match Australian interests to emerging threats overseas.

The BLU is encouraging participation now; around 800 facilities have been registered covering 64 countries.

Border Security Advice

ASIO's network of aviation liaison officers (ALOs) and maritime liaison officers (MLOs) was established in 2003 to provide an immediate representation and response capability for ASIO across the aviation and maritime sectors. In 2008–09, through regular participation in border security community meetings and via informal channels, ASIO's border network provided direct connectivity with key aviation and maritime partners including the AFP, the Department of Immigration and Citizenship (DIAC), the Australian Customs and Border Protection Service, and airport and seaport authorities.

ALOs are based at key airports around Australia and have established linkages with most regional airports nationally. MLOs are connected with maritime authorities across all states.

In 2008–09, in partnership with state-based police agencies and the Department of Infrastructure, Transport, Regional Development and Local Government (Office of Transport Security), ALOs contributed to the *Securing our Regional Skies* program in Western Australia, Northern Territory, Queensland and New South Wales. The program enhances security and security awareness at regional airports.

Visa Security Assessments

ASIO contributes to the security of Australia's borders through visa security assessments. Any person applying for a visa to travel to, and remain in, Australia may have the application referred by DIAC to ASIO for a security assessment – an assessment of the threat that the person's presence in Australia would pose to security (as defined in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act)).

In conducting a security assessment, ASIO draws on classified and unclassified information to evaluate activities, associates, attitudes, background and character, taking into account the credibility and reliability of information available. Where inconsistencies or doubts persist, ASIO may seek to interview the person.

ASIO limits its consideration in security assessments to factors related to 'security' as it is defined in the ASIO Act. Where ASIO determines that a person's presence in Australia would pose a direct or indirect threat to security, ASIO may recommend against the issue of a visa.

ASIO processed visa security checks in order of referral from DIAC, taking into account any agreed priority cases (with particular emphasis on refugee, humanitarian and protection cases, and genuine compassionate or compelling cases).

ASIO has continued to improve client service timeframes. The Next Generation Border Security initiative has improved the effectiveness and efficiency of security checking processes conducted by ASIO for applicants for Australian visas. Direct connectivity between DIAC and ASIO for the electronic transfer of security referrals and responses is now in place. This new system has improved the tracking and reporting of security referrals.

ASIO contributes entries to DIAC's Movement Alert List to detect known persons of security interest who are attempting to obtain an Australian visa. ASIO completed 59,884 visa security assessments in 2008–09 (see Table 2). These comprised 12,988 assessments for permanent visa holders and 46,896 assessments for temporary visa holders.

In 2008–09, ASIO issued adverse security assessments for two individuals seeking entry to Australia. The visa applicants were assessed to pose a security threat due to links to a terrorist group or a foreign government.

ASIO conducts security assessments for protection visa applicants, including offshore applicants, unauthorised arrivals (those who travel by boat or air without relevant documentation or using false documentation), and applicants who arrive legally in Australia on a valid visa and who subsequently claim protection.

The *Migration Act 1958* requires the Minister for Immigration and Citizenship to make a decision on protection visa applications within 90 days. In 2008–09, 64 percent of protection visa applications assessed by ASIO were completed within the 90-day timeframe, an increase from 62 percent in 2007–08. Compliance against the 90-day requirement is measured through reports submitted to Parliament by DIAC. These reports are prepared in consultation with ASIO. Where delays are attributable to ASIO, cases exceeding 90 days are typically complex and require further investigation. ASIO continues to work closely with DIAC to resolve cases that exceed the 90-day timeframe.

In 2008–09, ASIO completed 1,466 assessments for protection visa applicants. This included 372 assessments for temporary protection visa holders applying for resolution of status visas, as a result of the Government's abolition of temporary protection visas in August 2008. Protection visa assessments increased more than eleven percent from 2007–08.

There were no adverse or qualified assessments in the protection visa category in 2008–09.

Type of entry	2003–04	2004–05*	2005–06*	2006–07*	2007–08*	2008–09*	% decrease from 2007–08
Temporary	30,841	39,015	39,973	44,197	56,126	46,896	16
Permanent	13,881	13,402	13,174	9,190	16,562	12,988	22
Total	**44,722**	**52,417**	**53,147**	**53,387**	**72,688**	**59,884**	**18**

Table 2 Visa security assessments 2003–04 to 2008–09

*From 2004–05, figures include protection visas

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 significantly impact on Australia's social or economic well-being, or affect Australia's defence or national security capabilities.

ASIO's role in critical infrastructure protection involves identifying and ranking national critical infrastructure, and providing threat assessment advice. That advice is used by Commonwealth and state and territory governments – as well as private industry – to make decisions about risk and, on that basis, allocation of protective security resources.

ASIO engages closely with both Commonwealth and state and territory governments and private sector owners and operators throughout the threat assessment cycle. Engagement with owners and operators in the preparation of threat assessments is essential to gain an understanding of the characteristics and operations of critical infrastructure. In addition to distributing critical infrastructure protection threat assessments to a wide range of both Commonwealth and state and territory government departments, agencies and authorities, ASIO provides briefings to critical infrastructure stakeholders, including owners and operators from private sector business and industry. In 2008–09, ASIO briefed private sector representatives from 14 major financial sector companies, and 16 ports and shipping companies.

In 2008–09, ASIO produced seven sectoral and 17 vital asset threat assessments and provided 42 briefings to critical infrastructure owners and operators.

Advice for Special Events

ASIO has considerable expertise in providing intelligence advice and operational support to special events. ASIO's role in supporting special events may include:

- threat assessments to inform security planning;
- security assessments to inform venue access control;
- security assessments for individuals applying to travel to Australia to participate in or attend special events;
- physical security and risk management training and advice; and
- operational and technical support.

In 2008–09, ASIO provided security advice in support of three key international events – World Youth Day (WYD08) (Sydney, July 2008), the Beijing Olympic and Paralympic Games (August–September 2008), and the Asia-Pacific Economic Cooperation (APEC) forum (Lima, November 2008).

WYD08 was held without incident in Sydney between 15 and 20 July 2008. WYD08 was attended by close to half a million participants, including 130,000 international visitors. Along with His Holiness Pope Benedict XVI, numerous cardinals and bishops from around the world attended.

In support of this event ASIO prepared threat assessments and security intelligence reports, including 27 event-specific security intelligence reports. ASIO provided WYD08-related security intelligence reports to the New South Wales Police and relevant Australian Government and New South Wales State Government agencies.

The 2008 Olympic Games were held in Beijing, China between 8 and 24 August 2008, followed by the Paralympic Games between 6 and 17 September 2008. There were no security incidents of concern to Australia. ASIO was a member of the Security and Intelligence Specialists for 2008 Beijing Olympic Games (SISBOG), the official body for security and intelligence liaison. As a member of SISBOG, ASIO provided advice on intelligence gathering and assessment. ASIO worked closely with key Australian Government security stakeholders including DFAT, the AFP, and the Attorney-General's Department. ASIO produced 64 Beijing Olympic Games-related reports.

Beijing Olympic Games venues

Peru was the APEC forum host in 2008, which culminated in the APEC Economic Leaders Meeting in Lima on 22 and 23 November 2008. Prime Minister Rudd attended for Australia, along with the Minister for Foreign Affairs. ASIO produced 13 APEC 2008-related reports for Australian Government customers.

ASIO will provide support for ten forthcoming significant events, including the 2009 Pacific Islands Forum (Cairns), the 2009 Parliament of World Religions (Melbourne), the Vancouver 2010 Winter Olympic Games, the New Delhi 2010 Commonwealth Games, and ANZAC Day 2010 commemorations in Gallipoli.

Analysis Support to Investigations

Leads Development and Analysis

ASIO investigates thousands of new leads annually. The sources of ASIO's leads include human and technical sources from intelligence operations, overseas liaison services, government agencies and police services, open sources, the public, and the National Security Hotline (NSH). A dedicated leads branch triages and assesses primarily counter-terrorism leads, including those received through the NSH.

In 2008–09, ASIO continued to work closely with Commonwealth, state and territory law enforcement authorities to investigate and resolve intelligence leads. ASIO strengthened partnerships with Australian intelligence and law enforcement agencies, in particular the AFP. This involved close coordination and cooperation at the national and regional level.

Complex Technical and Tactical Analysis

ASIO's complex analysis capability continued to provide crucial support to investigations in 2008–09. ASIO enhanced its capability to apply financial intelligence to security investigations, including through engagement with partner agencies and through participation in national and international working groups.

Involvement in Litigation

ASIO provides information in response to, and as a contribution to, Commonwealth efforts in criminal, civil and administrative legal proceedings. Demand for such material, both from other government agencies and from defendants and applicants, has continued to increase. ASIO 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 2008–09, ASIO was involved in over 60 litigation matters. These ranged from support to prosecutions (in particular, terrorism prosecutions) to judicial and administrative review of security assessments, to civil actions. While the overall litigation volume remained comparable with that of the previous year, it is considerably higher than during any period preceding 2005. This high volume and the diversity and complexity of matters generated a significant work load. ASIO also responded to numerous requests for a broad range of material for use in litigation.

2008–09 saw verdicts in the Melbourne Pendennis terrorism trial. The prosecutions included ASIO intelligence as material in the form of documents, witnesses, and audio and video material. Supported and represented by barristers and external solicitors, ASIO's in-house lawyers, intelligence and technical officers worked with support staff to identify, retrieve, review, collate and, where necessary, redact tens of thousands of documents and hundreds of hours of audio and video material.

In the Melbourne Pendennis proceedings in 2008–09, some of the defendants were convicted of membership of a terrorist organisation and other terrorism-related charges, and sentenced to periods of imprisonment ranging from six to 15 years.

Three defendants were acquitted. One pleaded guilty before retrial to membership of a terrorist organisation and recklessly making a document connected with preparation for a terrorist act and was sentenced to five years' imprisonment.[4]

ASIO was directly involved in two legal matters initiated by Mr Mamdouh Habib: appeals to the Full Federal Court and High Court against the November 2007 decision of the Administrative Appeals Tribunal upholding an adverse security assessment and denying him an Australian passport;[5] and a Federal Court compensation claim alleging the Commonwealth defamed him and aided and abetted his alleged mistreatment during his detention overseas. In March 2009, the Federal Court struck out a number of Mr Habib's compensation claims on the grounds they had no reasonable prospects of success. ASIO provided instructions, material and documents in support of the defence of Mr Habib's claims for compensation.[6]

Mr Belal Khazaal was found guilty in the New South Wales Supreme Court of making a document in connection with assistance in a terrorist act.[7]

The re-trial of former ASIO officer Mr James Seivers for unauthorised communication of national security intelligence, and of Mr Matthew Francis O'Ryan for aiding and abetting Mr Seivers, resulted in guilty verdicts and sentences of periods of weekend imprisonment. Mr Seivers lodged an appeal against his conviction on 26 June 2009.

To ensure support to Commonwealth litigation, and to manage legal issues across the Organisation, ASIO continued to invest in its legal team throughout 2008–09, and has established legal teams in Sydney and Melbourne. ASIO has continued to integrate lessons learned from prosecutions and other legal proceedings into policies and procedures.

4 A further defendant pleaded guilty in 2007.

5 On 4 September 2009 Mr Habib was granted special leave to appeal to the High Court against the Full Federal Court decision, which had dismissed his appeal relating to the decision to issue an adverse security assessment and refuse to grant him an Australian passport.

6 A further application by the Commonwealth to strike out Mr Habib's claims of misfeasance in public office and harassment was heard on 14 and 15 September 2009 by the Full Federal Court. Judgment is reserved.

7 On 25 September 2009, Mr Khazaal was convicted and sentenced to twelve years' imprisonment, with a non-parole period of nine years. Mr Khazaal will not be eligible for parole until 31 August 2017. Mr Khazaal has filed a notice of intention to appeal his conviction and sentence.

Output 2: Protective Security Advice

Parts of this performance report have been excluded from the unclassified *Report to Parliament* for reasons of national security.

Protective Security

ASIO provides protective security advice to the Australian Government, and with approval from the Attorney-General, to state and territory governments and private sector companies. Within ASIO, T4 is the primary area that provides protective security advice. T4's advice typically includes recommendations on procedural, personnel and information security, along with physical security. T4 works with a wide range of organisations in Australia and internationally.

In 2008–09, ASIO recovered $1.68m of costs from providing protective security advice to clients. This advice included:

- protective security risk reviews;
- vulnerability assessments;
- certification and advice in relation to top secret facilities;
- ministerial office security reviews;
- evaluation of security equipment and consultants, locksmiths, couriers and classified waste services (on behalf of the Security Construction and Equipment Committee);
- protective security and risk management training and information circulars; and
- technical surveillance counter-measures testing.

In 2008–09, ASIO conducted security vulnerabilities assessments at ten airports, and additional assessments on several regional airports and maritime passenger terminals. This major body of work was commissioned by the Department of Infrastructure, Transport, Regional Development and Local Government and fed into its regulatory decision-making processes. It also assisted a review of airport protective security arrangements following the death of a man at Sydney Airport in March 2009.

During the term of each Parliament, ASIO conducts two reviews of the adequacy of ministerial security arrangements. ASIO completed the first round of ministerial office security reviews in 2008–09. The second round of reviews will commence early in 2009–10.

ASIO certifies all Australian top secret facilities. Recertification of these sites is required every five years. ASIO certified 27 new sites in 2008–09, and an additional nine sites were inspected and will be considered for certification after completion of physical security improvements.

ASIO provides a Technical Surveillance Counter-Measures (TSCM) capability (including electronic surveys, monitoring of premises for possible hostile electronic activity, and physical security inspections) to the Australian Government to protect discussions at a

national security or sensitive level. Throughout 2008–09, there continued to be a high demand for ASIO's TSCM services.

ASIO contributed to the Australian Government's 2008 *Review of E-Security*, including working with the Defence Signals Directorate and the Australian Federal Police (AFP) to produce a wide-ranging classified assessment of the electronic threat environment.

Policy Advice on Protective Security

ASIO provides the chair and secretariat for the Inter-Agency Security Forum (IASF), a consultative forum on government security issues. In 2008–09, the IASF, through a whole-of-government approach to protective security, continued to develop security policy, provided advice on the handling of highly sensitive information and reported to Government on the security status of agencies.

ASIO continues to drive a more strategic agenda for the IASF. In 2008–09, the IASF's work program included:

- documenting emergent issues challenging government protective security regimes;
- streamlining the Top Secret (positive vetting) security clearance process;
- comprehensively revising the *Classified Supplement to the Australian Government Protective Security Manual*;
- auditing safehand and overnight courier companies endorsed by the Security Construction and Equipment Committee (SCEC); and
- reviewing SCEC's endorsement criteria for safehand and overnight courier companies.

As IASF chair, ASIO produces an annual review on the protective security status of IASF agencies.

Personnel Security Assessments

ASIO provides personnel security assessments to assist government departments and agencies in deciding whether to grant access to national security classified information.

Applicants for security clearances must provide detailed background information to their sponsoring agency and ASIO. ASIO's personnel security assessments take into account intelligence information held by ASIO, as well as known risk factors. ASIO completed 21,699 personnel security assessments in 2008–09, consistent with a long-term trend of growth in the overall personnel security assessment workload (see Figure 2).

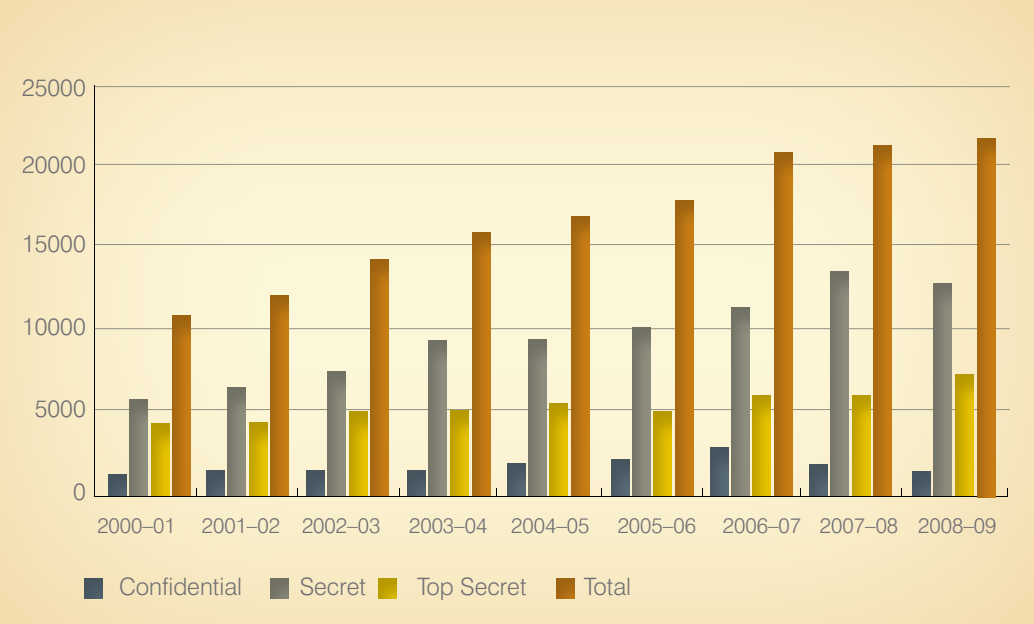

Figure 2: Personnel Security Assessments 2000–09

Adverse and Qualified Assessments

One qualified personnel security assessment was issued in 2008–09.

Adverse or qualified personnel security assessments issued by ASIO may be appealed to the Administrative Appeals Tribunal. There were no appeals in 2008–09.

Counter-Terrorism Security Assessments

ASIO's counter-terrorism security assessments are carried out at the request of government authorities who are responsible for accreditations, usually the AFP and AusCheck. In 2009, ASIO established direct connectivity with AusCheck for the electronic transfer of the information required to undertake counter-terrorism checks. This has provided greater efficiencies, and improved the tracking and reporting of security referrals.

ASIO completed 65,119 counter-terrorism checks in 2008–09 (see Table 3), 98 percent of which were completed within ten days. These included:

- 56,266 checks for Aviation and Maritime Security Identity Cards for pilots, trainee pilots, air and sea vessel crew, and persons requiring access to controlled areas at air and seaports;
- 7,948 checks for persons requiring licences to access ammonium nitrate; and
- 905 checks for staff and visitors to the Australian Nuclear Science and Technology Organisation (ANSTO) facility at Lucas Heights, Sydney.

Adverse and Qualified Assessments

No adverse or qualified counter-terrorism security assessments were issued as a result of counter-terrorism security assessments conducted during 2008–09.

Type of check	2003–04	2004–05	2005–06	2006–07	2007–08	2008–09
Aviation/Maritime Security Identity Cards	58,147	38,466	71,733	118,118	70,084	56,266
Ammonium Nitrate	-	1,634	7,428	6,419	4,502	7,948
ANSTO	-	-	-	1,027	1,251	905
Commonwealth Games	-	-	56,149	-	-	-
G20 Finance Ministers' Meeting	-	-	-	1,580	-	-
Asia-Pacific Economic Cooperation forum and World Youth Day	-	-	-	7,837	13,453	-
Total	**58,147**	**40,100**	**135,310**	**134,981**	**89,290**	**65,119**

Table 3: Counter-terrorism checks

Contact Reporting Scheme

The *Australian Government Protective Security Manual* requires Australian Government employees to report suspicious, unusual, or persistent contact with foreign nationals as part of the Australian Government Contact Reporting Scheme. This reporting scheme is a valuable component of ASIO's efforts to identify attempts to gain unauthorised access to sensitive information.

In 2008–09, ASIO promoted the scheme with over 90 presentations, including to state and territory agencies. Thirty-six government agencies provided contact reports to ASIO in 2008–09. There are a number of agencies that would be expected to have considerable contact with foreign nationals but that have relatively low reporting rates. ASIO has an active program of liaison with agencies to promote the reporting scheme and to encourage a culture of contact reporting within agencies.

Output 3: Security Intelligence Investigations and Capabilities

Parts of this performance report have been excluded from the unclassified *Report to Parliament* for reasons of national security.

ASIO's Collection Capability

ASIO's work necessarily has a strong focus on investigation in order to determine the relevance to security of particular activities, the threat posed by the activities of persons and groups of security concern as well as the harm done to national security interest through those activities. ASIO's collection capabilities are focused on high-tempo operational engagement with a wide range of national and international security and intelligence partners with a focus on human source operations.

ASIO draws on information from a variety of sources, ranging from publicly available information to covert and highly sensitive human source and warrant operations. Decisions to use intrusive techniques are made balancing the severity and immediacy of the threat and degree of intrusion into individual privacy.

Most of ASIO's investigations require a variety of techniques. In 2008–09, ASIO strengthened its operational planning capability to ensure maximum utility was obtained from the deployment of ASIO resources.

Investigations and Operations

ASIO's investigative and operational effort is directed primarily at countering terrorism. However, counter-espionage, foreign interference and counter-proliferation are also high priorities. ASIO provides intelligence on the activities of individuals and groups assessed to represent a security threat to Australia or Australian interests.

Counter-Terrorism

Counter-terrorism investigations remained ASIO's highest priority in 2008–09, and this will continue for the foreseeable future. While other threats continue to grow and develop, few of these carry the immediate public safety threats and consequences.

Counter-Terrorism Response

ASIO's contribution to national counter-terrorism response arrangements is an important element of Australia's overall counter-terrorism capability. Counter-terrorism response arrangements centre on the National Counter-Terrorism Committee (NCTC). The NCTC – established in 2002 under the Inter-Governmental Agreement on Australia's National Counter-Terrorism Arrangements – is responsible for whole-of-government counter-terrorism policy coordination and national counter-terrorism arrangements, including Australia's National Counter-Terrorism Plan (NCTP).

The NCTC is supported nationally by several other bodies including the Australian Government Counter-Terrorism Policy Committee, the Australian Government Counter-Terrorism Committee, and the Homeland and Border Security Policy Working Group.

The NCTC coordinates training courses and exercises which bring together Commonwealth and state and territory law enforcement and emergency management agencies to test and improve response arrangements across jurisdictions and organisations. In 2008–09, ASIO provided support to a range of NCTC exercise and training activities.

The NCTP identifies four key components of counter-terrorism activity – prevention, preparation, response and recovery. Under the NCTP, ASIO is responsible for:

- the National Intelligence Group, which coordinates and disseminates intelligence to support operational commanders and senior government decision-makers in the event of a major terrorist incident, or in support of Inter-departmental Emergency Taskforce arrangements;
- leading a multi-agency Forward Intelligence Analysis Team that would be deployed overseas in response to a terrorist incident in another country;
- maintaining a capability to deploy intelligence support overseas; and
- ongoing assistance for the conduct of investigations as part of the Joint Counter-Terrorism Team arrangements.

ASIO's Technical Support Unit (TSU) is a rapid response capability which can be deployed under the NCTP framework to assist Commonwealth or state or territory authorities in the event of a terrorist incident. The TSU was not deployed operationally during 2008–09.

Special Powers Under Warrant

The *Australian Security Intelligence Organisation Act 1979* (the ASIO Act) and the *Telecommunications (Interception and Access) Act 1979* (the 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 2008–09, no questioning or questioning and detention warrants were issued.

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.

Capabilities

ASIO continues to develop its investigative capability and build partnerships within Australia and internationally to meet the operational needs of an increasingly complex security environment. ASIO's collection methods include open sources, human sources, physical surveillance, technical collection and special powers operations under warrant.

Open Source Intelligence

Open sources provide a wealth of information. International news services provide continuous, near real-time monitoring of global events. Publications, the Internet and databases can provide valuable input to ASIO's analytical and investigative work. Managing the volume of publicly available information can, however, be challenging, and the veracity of information in the public domain must often be tested against other sources.

ASIO's Research and Monitoring Unit provides specialised open-source support to analysis and operational activity and conducts 24/7 monitoring of the global and domestic security environment through classified and unclassified sources.

Physical Surveillance

ASIO's physical surveillance capability is a vital component of the Organisation's intelligence collection effort.

In 2008–09, ASIO continued the enhancement of its physical surveillance capability. ASIO recruited and trained additional surveillance teams.

Human Intelligence Collection

Human intelligence sources – from community contacts, interviewees and members of the public who volunteer information through to covert, fully recruited ASIO sources who report against priority targets – enable ASIO to provide accurate and timely information on continuing and new sources of security threat. They are a valuable and flexible method of acquiring intelligence on the activities of those who pose a security threat. Human sources can provide unique access and context and can be tasked and developed over time to be deployed in a variety of roles.

In 2008–09, ASIO continued to build upon its long-standing program of confidential contact with leaders and influential members of various ethnic and religious community groups in Australia. This program provides ASIO with ready access to community members and an ability to contextualise information in response to specific developments or government information requirements.

Language Capability

ASIO maintains foreign language capabilities to assist counter-terrorism, counter-espionage and foreign interference investigations. ASIO is implementing several projects and initiatives to augment its foreign language translation capability and capacity, and to maximise efficiencies in the processing and dissemination of foreign language product.

Technical Collection

Technically-derived intelligence, such as data from telecommunications intercept, makes an important and often unique contribution to ASIO's investigations and assessments. In 2008–09, ASIO continued its major investment in the development and delivery of technical collection capabilities. ASIO works closely with domestic and international partners – including industry – to maximise the benefit and efficiency of the complex development work which often underpins technical collection activity.

ASIO has technical capability to collect intelligence, as part of a special powers operation such as telecommunications interception. These capabilities, like all ASIO's collection activities, are exercised in strict observance of the principle of proportionality – the means for obtaining information must be proportionate to the gravity of the threat. This is required by the *Attorney-General's Guidelines* (see also pp. 60–61).

Telecommunications Interception

ASIO is designated by the Attorney-General to be the lead Commonwealth agency in managing the development of interception and delivery capabilities for use by Commonwealth and state and territory intercepting agencies. In this role, ASIO works with the telecommunications industry to ensure comprehensive interception capabilities are in place. Under the TIA Act, carriers and carriage service providers are required, unless specifically exempted, to develop, install and maintain capabilities to provide interception to authorities. As a part of its 'lead house' role, ASIO provides technical advice to the responsible policy departments, the Attorney-General's Department (AGD) and Department of Broadband Communications and the Digital Economy (DBCDE).

In 2008–09, ASIO, with the Australian Federal Police (AFP), contributed to work led by AGD and the DBCDE to develop an improved strategic dialogue with the Australian telecommunications industry. A new strategic forum has been established to consider national security and law enforcement issues relevant to the telecommunications sector. This will augment ASIO's existing industry contacts for telecommunications interception and critical infrastructure protection.

Information and Communication Technology Capability and Connectivity

While ASIO continues the development of its information and communication systems in line with the recommendations arising from the *Review of ASIO Resourcing* (the Taylor Review) in 2005, ASIO systems remain under pressure.

Challenges include the increasing tempo of work; the need to share relevant information

quickly with an increasing range of government, business, community and international partners; and the requirement for ASIO to identify what is, and what is not, of intelligence relevance in much larger volumes of information. Similarly, ASIO's growing involvement in judicial processes and the Organisation's need to meet the requirements set by courts and tribunals in a timely manner are creating new challenges.

To meet these challenges during 2008–09, ASIO reviewed its information and communication technology (ICT) strategic plan; refined internal governance frameworks and processes supporting ICT business alignment; continued focus on the development and training of staff; and completed a range of ICT projects. The ICT strategic plan incorporates the Government-adopted recommendations from Sir Peter Gershon's 2008 *Review of the Australian Government's Use of Information and Communication Technology*.

To assist in analysing greater volumes of information ASIO introduced several analytical visualisation tools in 2008–09. One ASIO-developed tool provides for automated mapping and manipulation of data. The visual representation allows analysts to rapidly understand the nature of links between entities and better identify linkages of potential concern.

In 2008–09, ASIO enhanced its ability to undertake analysis of data with a geospatial element. This will also assist analysts in the identification of previously unknown links or associations.

The maintenance and development of ASIO's supporting infrastructure remains a significant body of work. In 2008–09, this included the programmed replacement of server infrastructure and, where possible, the virtualisation of servers to reduce power and space requirements while reducing hardware costs. This is an important 'greening' initiative.

Major initiatives for 2009–10 will include commencement of a three-year redevelopment of ASIO electronic information management systems; updating ASIO's electronic information storage infrastructure; the introduction of a new ASIO-wide Top Secret desktop and standard operating environment; the development of a new intranet for corporate information; and a new ASIO Internet site.

Protecting Capabilities and Information

ASIO's priority investigations often occur in uncertain and rapidly evolving environments. They rely frequently on highly sensitive collection capabilities, including human sources and technical operations.

In recent years extremists have acquired broad knowledge of intelligence methodologies. Drawing upon this knowledge, they have adopted more sophisticated methods, making it more difficult for ASIO to monitor them.

ASIO carefully considers police and Commonwealth Director of Public Prosecutions requests to use its material as evidence, and in most cases is able to assist. Some of this material must, because of its sensitivity, retain a national security classification. It is generally provided in closed court and may be judicially determined to not form part of the publicly available record of the trial.

In 2008–09, ASIO worked closely with the legal community to ensure suitable arrangements for protecting the identity of ASIO witnesses.

Cover and Assumed Identities

ASIO has cover arrangements to protect the identities of ASIO officers. Knowledge of the real identities of ASIO officers could be used to compromise the Organisation's work, and the safety of staff.

Assumed identities can be used for intelligence collection, operational support, intelligence training, surveillance duties, and administrative support.

All use of assumed identities in ASIO is authorised under the *Crimes Act 1914* (Cth), and in accordance with the *Law Enforcement and National Security (Assumed Identities) Act 1998* (NSW).

The Commonwealth legislation allows the Director-General of Security, and delegates, to authorise the use of assumed identities and the acquisition of supporting documents from Commonwealth, state (except New South Wales) and territory and non-government agencies.

New South Wales legislation is used by ASIO in addition to the Commonwealth scheme where assumed identities are required in New South Wales.

Two audits of assumed identity records were conducted in 2008–09. There were no discrepancies or breaches detected for either the Commonwealth or New South Wales schemes.

Operational and Investigative Cooperation

ASIO liaises with Commonwealth, state and local government partners, the private sector and with overseas partners for assistance on inquiries, investigations and in support of operations. Joint counter-terrorism work by intelligence and policing agencies requires cooperation and management of resources at the strategic, operational and tactical levels to avoid duplication or confusion, and to maximise outcomes of coordinated ASIO and police activity.

Increased cooperation with the Australian Federal Police following the Street Review

In 2007, the Australian Federal Police (AFP) initiated a review into the AFP's national security operations and the effect of interaction between the AFP and its partner agencies. The Review Committee, Chaired by the Hon. Sir Laurence Street, included retired New South Wales Police Commissioner, Mr Ken Moroney, and former Director of the Defence Signals Directorate, Mr Martin Brady. The Terms of Reference for the Review included an examination of the adequacy of existing practices, policies and inter-agency governance and frameworks.

The Review identified ten recommendations covering four broad areas – operational decision-making processes, joint taskforce arrangements, information sharing, and training and education. All ten recommendations relate directly to the AFP, with six significantly affecting ASIO and four recommendations affecting the Commonwealth Director of Public Prosecutions (CDPP).

A regular forum has been established for the heads of ASIO, the AFP and the CDPP to review strategic priorities and interoperability issues – the Chief Executive Interoperability Forum. Heads of Commonwealth, state or territory agencies attend meetings where matters affecting their jurisdictions or responsibilities will be discussed.

ASIO and the AFP have developed a National Counter-Terrorism Protocol that provides a framework for efficient and effective interaction and information exchange between the agencies. The Protocol sets out a clear process of consultation between ASIO and the AFP to strengthen Australia's counter-terrorism arrangements, to ensure both agencies work concurrently to meet their separate but related legislative mandates when engaging in counter-terrorism operations. The Protocol establishes a process for the regular and accountable provision of information between ASIO and the AFP and how that information may be communicated.

A Counter-Terrorism Operations Oversight Committee (CTOOC) has been created, co-chaired by one of ASIO's Deputy Directors-General and the AFP's Deputy Commissioner National Security. Senior officials from the CDPP and the Attorney-General's Department attend, and representatives from other agencies participate as required. The CTOOC maintains strategic oversight of significant counter-terrorism operations and agrees which operation will have primacy – either an ASIO security intelligence operation or a criminal investigation.

Multi-Agency Cooperation

In early 2009, a joint ASIO-AFP team was established in ASIO's Leads Branch to evaluate leads received from the National Security Hotline (NSH). The team has centralised and coordinated the evaluation of new leads across Australian Government agencies, reduced duplication of analytic and investigative effort, and streamlined and enhanced investigative responses. An out-posted AFP officer is embedded in the team, and new processes are in place to develop combined ASIO-AFP assessment of each NSH report. The establishment of the team has resulted in significant resource efficiencies for both ASIO and the AFP, as well as a more comprehensive and timely response to new information. The AFP's extensive criminal information holdings and ASIO's intelligence holdings and access to Australian intelligence community resources are brought to bear simultaneously for each case, providing quicker and better assessments of lead information, reducing duplication for both ASIO and the AFP and ensuring appropriate priority is given to investigations. This is of particular value during high operational tempo.

Cooperation with Overseas Partners

ASIO's International Engagement

Most security threats to Australia have origins or linkages outside Australia. The international threat environment is complex and dynamic. Developments in areas which previously have not been a source of security concern may very quickly become directly relevant to ASIO's work. Globalisation, particularly the transnational nature of international terrorism, as well as espionage and foreign interference, means that security matters with links to Australia may be uncovered anywhere in the world. In addition, security intelligence investigations in Australia often contain links to countries and overseas groups and individuals. This requires ASIO to have an effective, well-established and strategic international liaison network to provide the global reach necessary to pursue threats wherever they may be.

In 2008–09, visits to and from Australia continued to provide ASIO with opportunities to reinforce Australian interests and enhance areas of common interest.

Liaison Statistics

- At 30 June 2009, ASIO had 316 approved liaison relationships with authorities in 122 countries.
- In 2008–09, ASIO received approximately 135 visits from foreign intelligence and security services.
- In 2008–09, the Director-General of Security visited 13 heads of overseas intelligence services.

Counter-Terrorism Intelligence Training Cooperation

ASIO provides training to overseas intelligence and security agencies. The Counter-Terrorism Intelligence Training Program (CTITP) delivers counter-terrorism training and capacity-building to enhance counter-terrorism cooperation with and between partner agencies.

CTITP programs were presented by ASIO officers, supported as appropriate by members of Australian Government and state government agencies, and external consultants with expertise in counter-terrorism. Programs were conducted in Australia and overseas.

CTITP continues to assist the AFP in delivering intelligence training at the Jakarta Centre for Law Enforcement Cooperation in Indonesia.

CTITP's flagship program is the annual International Counter-Terrorism Seminar. In 2009, 27 intelligence and security agencies from 15 countries were represented. The seminar encourages information exchange and fosters the concept of counter-terrorism success through interaction and cooperation.

Research and Development

ASIO's research and development efforts have increased the capability of its people and systems. The Science Adviser contributes to the pursuit of innovation in all areas of ASIO through in-house research and development; collaboration with international and domestic partners; engagement with industry and academia; and human resource development. ASIO collaborates with government-funded research agencies such as the Defence Science and Technology Organisation (DSTO). A senior DSTO officer is a full member of ASIO's Research & Development Committee (see also pp. 59–60).

Through the Science Adviser and its Research & Development Committee, ASIO engaged with the Department of the Prime Minister and Cabinet and other stakeholders to focus on advancing broader national security interest in research and development. ASIO is contributing to the development of the *National Security Science and Innovation Strategy*.

In 2008–09, the Science Adviser developed a framework for ASIO to capture innovative ideas and facilitate their development.

Output 4: Foreign Intelligence Collection

ASIO collects foreign intelligence in Australia under warrant and through human sources at the request of the Minister for Defence or the Minister for Foreign Affairs. Foreign intelligence deals broadly with the capabilities, intentions or activities of a foreign power. It covers political, economic, and diplomatic matters and also threats against the security of Australia. ASIO works closely with the other Australian agencies dedicated to foreign intelligence, namely the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation.

The work performed by ASIO varies considerably according to the nature of the target and the means of collection and information processing employed. In some cases, ASIO performs much or all of the operational work and makes the collected intelligence available for processing and reporting by DSD or ASIS. In other instances, ASIO's role is largely limited to preparing and coordinating the warrants required for the work and the tasks of collecting, processing and reporting the intelligence fall to the foreign intelligence community. In all instances, ASIO reports to the Attorney-General on the information collected under foreign intelligence warrants and its intelligence value.

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

Part Three CORPORATE MANAGEMENT AND ACCOUNTABILITY

People

Recruitment

ASIO's success depends on the commitment and calibre of its staff. Recruitment is, therefore, a high priority, particularly as ASIO is in the final stages of a substantial growth program. In 2008–09, ASIO's net staffing increased by 198, exceeding the growth forecast of 170 additional staff and taking the total staff number to 1,690. ASIO is on a growth program, set to achieve staffing levels of around 1,800 by 2010–11, consistent with recommendations made in the *Review of ASIO Resourcing* (the Taylor Review) in 2005 (see Figure 3).

In 2008–09, ASIO's exposure to the employment market was enhanced through the use of innovative and diverse recruitment advertising. Employment market research in 2008–09 resulted in a new recruitment brand for ASIO – '*ASIO something more*…'. ASIO expanded its use of on-line, electronic, outdoor and radio advertising and industry-specific publications. ASIO was represented at university career fairs around Australia to promote it as an employer of choice.

There was a strong response to ASIO's advertisements with 12,550 applications in 2008–09, compared with 9,567 applications received in 2007–08. Recruitment strategies were successful in attracting appropriately skilled applicants. They were also more cost effective as ASIO spent less on recruitment advertising – $1.962m in 2008–09, down from $2.192m in 2007–08.

ASIO employees require a Top Secret (Positive Vetting) (TSPV) national security clearance. ASIO initiated over 564 TSPV security clearances from recruitment activity in 2008–09. A further 297 national security clearances were initiated, at varying security clearance levels, for a range of contractors and consultants engaged by ASIO.

In 2008–09, ASIO implemented a number of practices which resulted in, on average, an efficiency saving of around 20 working days for security clearance processing.

Recruitment

Staffing Profile and Workplace Diversity

ASIO staff are employed under conditions of service similar to the *Public Service Act 1999*. ASIO uses the annual Australian Public Service (APS) *State of the Service* as a comparison benchmark.

ASIO staffing was 1,690 at 30 June 2009, up from 1,492 as at 30 June 2008.

At 30 June 2009, 88 percent of ASIO's total staffing was working on a full-time basis which equates to a full-time staff equivalent (FTE) of 1,599.

Only eight percent (or 135) of ASIO's staff were employed on a part-time basis compared with around 12.2 percent in the APS in 2007–08. Most of these part-time staff (86 percent, or 116) were women with nearly half being in the 35-44 year age group.

ASIO's attrition rate for 2008–09 decreased to 4.5 percent compared with 7.6 percent in 2007–08. This compares favourably with 8.2 percent across the APS in 2007–08 and provides an acceptable level of turnover while retaining skilled and experienced staff.

While two thirds of ASIO's staff have been with the Organisation for less than five years, recruitment of new staff from the public and private sector has boosted the diversity of skills and experience within the Organisation.

The median age of ASIO's workforce is now 36 years (compared with the APS median of 42 years in 2007–08). The median age has continued to decrease with the growth of the Organisation. Only 28 percent of ASIO's workforce is aged 45 years or older compared with 42 percent in the APS in 2007–08.

Women represent 45 percent of ASIO's workforce. However, they remain under-represented in the senior officer ranks (37 percent) and Senior Executive Service (SES) (18 percent) ranks compared with the APS levels of 45 percent and 37 percent respectively in 2007–08.

ASIO officers from non-English speaking backgrounds now comprise 17.1 percent of staff, an increase from 16.4 percent in 2007–08.

Workforce statistics are at Appendix C.

ASIO increased resources for workforce planning and reporting in 2008–09 to meet the continuing demands of growth in a changing labour market, and to focus on longer-term issues such as succession planning during and beyond the period of growth.

Staff Survey

ASIO conducts a staff survey every two years. The 2009 staff survey measured perceptions, attitudes, concerns and areas of satisfaction across a range of key cultural, security and people management performance dimensions. The response rate was 78.3 percent, similar to response rates in 2005 and 2007 (76 percent and 79 percent respectively).

Responses in 2009 were more positive than in 2007, with the exception of 'opportunities for promotion'. Key findings included:

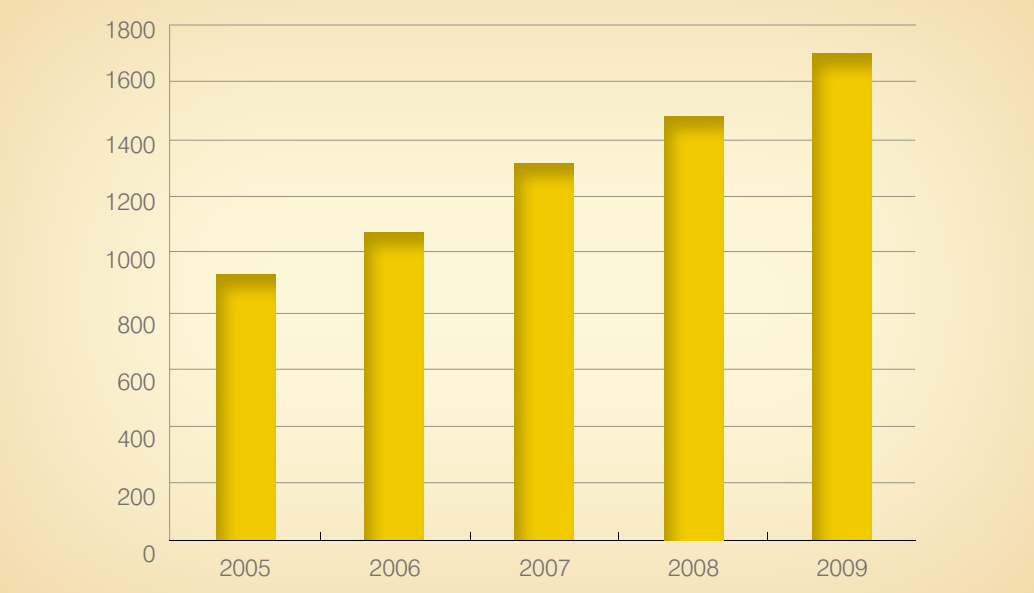

Figure 3: Staffing growth, 2005–09

- staff are satisfied with the Organisation and their jobs and they support the Organisation's mission and objectives;
- staff believe the Organisation has a clear set of values and that their colleagues act in accordance with these values;
- staff have the skills and knowledge to do their job well, and sufficient resilience to cope with challenge;
- staff support and understand the Organisation's security procedures; and
- staff understand the interdependencies between the Organisation and other agencies.

Overall, the survey demonstrated staff are very committed to ASIO, and strongly support its mission, goals and objectives.

Human Resource Policies

ASIO undertook a significant project during 2008–09 to review and refresh the Organisation's Human Resource policy framework. Policies are more user-friendly and staff find them easier to interpret.

Staff Training and Development

ASIO staff are capable and well-trained to operate in today's challenging security environment. In 2008–09, ASIO invested over 40 percent more in training ($10.3m compared with $6.4m in 2007–08). This additional investment supported the needs of a growing workforce, and reflects a commitment to ensuring staff are adequately skilled. Training staff numbers were increased to facilitate training of a greater number of Intelligence Officers (IOs).

Training is ongoing, and investment is set against the skills and knowledge that employees require to carry out their duties to the highest-level. ASIO's *Learning and Development Strategy* informs training course development and delivery is targeted to business needs. Throughout 2008–09 there was a continuing focus on technical skill development, complemented by training in interpersonal skills to support management and leadership practices, including relationship management.

Leadership and Management Skills

ASIO continues to place a strong emphasis on the development of its SES and Senior Officers. The development of its leaders during 2008–09 included a range of learning activities, with over 200 senior staff trained in management and leadership.

Three SES forums were held, which focused on managing growth, corporate planning, whole-of-government operations and legal challenges. Leading academics and practitioners in a range of fields addressed these forums. Two combined SES and Senior Officer forums considered issues such as legal matters, priorities and plans, and upgrades to technical capabilities.

ASIO's suite of leadership programs was evaluated and reviewed in 2008–09. This led to short workshops on specific management skill-sets, and a new internal management development program for high-potential ASIO officers who may be promoted to the Senior Officer level.

Corporate Training

Corporate training activities include an induction program for all new starters, wide-ranging administrative training, information technology training, ethics and accountability training, and discipline-specific courses covering areas such as the political and social drivers of terrorism.

Staff who undertake tertiary study can receive financial and other support through the Studies Assistance Program. ASIO has expanded its Studies Assistance Program and now has over 114 staff members undertaking part-time study at the graduate and postgraduate level. Staff who achieve outstanding results in their studies while maintaining high levels of work performance may receive a study bursary.

In 2008–09, ASIO implemented a study initiative allowing up to 13 high-potential staff full-time postgraduate study for up to a year, fully funded by ASIO. This initiative is an investment in ASIO's future and provides high-calibre staff with an avenue to undertake advanced career and personal development activities.

ASIO conducts a monthly series of internal seminars on topics of professional interest to staff. It seeks to foster a sense of teamwork and a shared culture, through broadening knowledge of work areas across the Organisation.

eLearning in ASIO

ASIO introduced an eLearning program in 2009. Staff are able to undertake training in a variety of disciplines through an online interactive program. Training is available at any time, which is particularly beneficial to shift-workers and for distance education. The eLearning program is also used to provide pre-course material prior to traditional face-to-face training workshops. It also allows a wide range of in-house customised topics to be delivered.

ASIO has a dedicated team of eLearning professionals who can design, create and publish customised eLearning to meet ASIO's needs.

Screen shot of eLearning

Intelligence Training

ASIO provides specialised in-house training to its IOs and Intelligence Analysts (IAs). These training courses include theory and practical components and cover interviewing skills, management of human source operations, operational tradecraft, analytical techniques, and the preparation of ASIO security intelligence and other reports. ASIO engages with both domestic and international partners to source high-quality training programs that broaden ASIO officers' experience.

The demand for training for IOs and IAs during 2008–09 was at its highest level in more than a decade, and is a reflection of the continued growth in staff numbers. These demands will continue into and beyond 2009–10. All programs undergo continual and rigorous evaluation with particular focus on enhancing tradecraft and human source recruitment and management skills to ensure ASIO's staff are best prepared for their respective roles.

Response to Recommendations of the Street Review

In response to the Street Review of *Interoperability between the Australian Federal Police (AFP) and its National Security Partners*, a number of training programs were developed, refined and implemented during 2008–09. These include modules to provide IOs with an enhanced understanding of evidentiary, prosecutorial methodology – and how it applies in the ASIO context – and knowledge of the AFP and Commonwealth Director of Public

Prosecutions. AFP training modules were also delivered on handling and protection of classified and sensitive information and intelligence and on ASIO's structure, role, responsibilities and methodology. All IO trainees now undertake a workshop on the roles and functions of the AFP and all new recruits of the AFP are given an understanding of the role and functions of ASIO.

Course	Host Organisation	Participants
AFP Counter-Terrorism Workshop	Joint ASIO-AFP	149
ASIO Role and Functions Seminar	ASIO	252
AFP Role and Functions Seminar	AFP	25
Overt Search and Evidentiary Procedures Course	AFP	75

Table 4: Joint ASIO-AFP training 2008–09

Language Training

ASIO invests in language skills to support its operations, and to enable it to engage effectively with foreign liaison partners. ASIO's commitment in 2008–09 included:

- full-time training in languages relevant to ASIO's investigative work;
- full-time language training for ASIO overseas-posted officers, provided by the Department of Foreign Affairs and Trade;
- training for linguist staff to refine and enhance their skills; and
- a Language Skills Allowance (up to $12,000 per year) for staff with language proficiencies.

Support to New Staff

The New Employee Support Officer (NESO) program, introduced in 2007–08, provides support and guidance to new staff members. New starters are allocated an experienced staff member from a different workgroup to assist their transition to ASIO. A review of the NESO program has commenced with preliminary findings that the program has been positive and beneficial in providing support and assisting the integration of new starters into the Organisation.

Staff Placements

In 2008–09, ASIO introduced an innovative approach to the management of appointments, promotions and transfers through a Recruitment Framework strategically aligned with a Promotions and Transfer sequencing framework. The Recruitment Framework provides a concise and convenient approach to balancing the Organisation's strategic staffing requirements with the day-to-day activities of advertising, interviewing and vetting applicants. The Promotions and Transfer sequencing framework was introduced in March 2009. This framework is supported by revised human resource policies.

Attachments

ASIO has a well-developed attachment program with staff posted both from and to ASIO as outlined in Table 5. This has improved cooperation and interoperability with a range of other agencies and encourages the sharing of skills, capability, knowledge and information.

Agency	Staff to ASIO	Staff from ASIO
Attorney-General's Department		✓
Australian Transaction Reports and Analysis Centre (AUSTRAC)	✓	
Australian Federal Police (AFP)	✓	✓
Australian Secret Intelligence Service (ASIS)	✓	✓
Defence Imagery and Geospatial Organisation (DIGO)	✓	
Defence Intelligence Organisation (DIO)	✓	
Defence Signals Directorate (DSD)	✓	✓
Department of Defence (DoD)	✓	
Defence Security Authority (DSA)	✓	✓
Department of Foreign Affairs and Trade (DFAT)	✓	✓
Department of Infrastructure, Transport, Regional Development and Local Government (DITRDLG)	✓	
Office of National Assessments (ONA)	✓	✓
Department of the Prime Minister and Cabinet (PM&C)		✓

Table 5: ASIO attachments

Workplace Agreement

ASIO's *Seventh Workplace Agreement* will expire on 31 December 2009. The final salary increase of 4.8 percent was effective from 1 January 2009. Negotiations on the *Eighth Workplace Agreement* commenced in mid–2009.

Performance Management

Performance management remains a priority focus. Training in the performance management system was delivered across ASIO.

Senior Executive Service Performance Pay

Sixty substantive SES members received a performance bonus and three staff members acting in an SES capacity for greater than three months received a pro-rata amount dependent on their period of acting in an SES position. The individual range of performance pay was $1,372 - $13,606 with the average payment being $6,789. The total amount of performance pay for the SES was $434,522.

Harassment Free Workplace

In 2008–09, ASIO released a new policy – *Maintaining a Harassment Free Work Environment and Valuing Diversity.* ASIO maintains an Harassment Contact Officer Network to provide ongoing support to counter any instances of bullying, harassment and discrimination.

Occupational Health and Safety

During 2008–09, ASIO undertook a number of initiatives to prevent workplace injuries, including development of *Occupational Health and Safety Management Arrangements*. A risk management framework was implemented to assess and control health and safety risks, and prevent workplace injuries. Assessments for work areas that perform operational, mechanical and building maintenance work resulted in recommendations being implemented including:

- developing systems for hazard management;
- writing and reviewing procedures;
- implementing training and maintenance schedules;
- providing equipment and signage to provide and maintain a safe work environment; and
- undertaking further specialised assessments.

A corporate procedures framework was established to provide policy advice on Occupational Health and Safety issues of concern to staff. A number of first-aid risk assessments were completed, ensuring work area safety provisions are adequate and appropriate. The findings of the assessments indicated that by tailoring first-aid provisions to meet ASIO's specific risk profile, work area safety provisions exceeded the requirements of the *Occupational Health and Safety Code of Practice 2008*.

ASIO's Health and Wellbeing program delivered free health appraisals, skin checks and a range of health activities and seminars, with over 50 percent of staff members reporting that this program had encouraged them to make positive lifestyle changes. Influenza vaccinations were also provided.

In 2008–09, five incidents were notified to Comcare compared with nil in 2007–08. The injuries sustained in these incidents, although relatively minor, resulted in the affected staff members needing emergency treatment by a doctor or to be treated within a hospital casualty unit, thus necessitating notification to Comcare under section 68 of the *Occupational Health and Safety Act 1991*.

There were no investigations conducted under section 41, or any notices issued under sections 46 and 47, of the *Occupational Health and Safety Act 1991*.

During 2008–09, ASIO actively managed injuries sustained by staff to mitigate the direct and indirect costs of these injuries to the staff member and their families, their work area, and the Organisation. There were 29 staff members with compensable injuries, eight fewer than 2007–08.

ASIO has reviewed and developed a new *Corporate Procedure on Injury Management, Rehabilitation and Graduated Return to Work* program and engaged the services of additional approved rehabilitation providers to support timely and active rehabilitation. ASIO continues to actively manage workers' compensation cases to facilitate a timely and durable return-to-work outcome.

Disability Strategy

ASIO's *Disability Action Plan 2005–2009* demonstrates ASIO's commitment to improving conditions and accessibility for people with disabilities. The plan ensures that all employment policies and practices incorporate the needs of disabled staff. It promotes an awareness of disability discrimination issues and is forefront in any necessary amendment to ASIO's facilities.

The Plan has ensured all employment policies and procedures comply with the requirements of the *Disability Discrimination Act 1992*. Through training and development, awareness of disability discrimination issues in the workplace has been established and maintained. The Organisation's *Disability Action Plan 2005–2009* has ensured premises and facilities are accessible and usable by people with disabilities.

Financial Services

Purchasing

ASIO procurement activity occurs in accordance with the *Chief Executive Instructions* which require officers to comply with *Commonwealth Procurement Guidelines*, subject to authorised exemptions for the protection of national security. ASIO adheres to the Australian Government's core procurement policy framework, and ensures that value for money is achieved through competitive procurement processes wherever practicable.

Details of ASIO agreements, contracts and standing offers may be made available to

Members of Parliament as a confidential briefing or to the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

In 2008–09, ASIO's investment in capability continued with procurement activity focused on key business areas, including technical capabilities, information technology infrastructure and protective security.

Consultants

During 2008–09, ASIO let four consultancy contracts, up from two in 2007–08. The total expenditure during the year on consultancy contracts valued at $10,000 or more (including contracts let during the previous year) totalled $0.575m, down from $0.942m in 2007–08.

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, and one open request for tender during 2008–09. The restricted requests for tender were not advertised publicly for national security reasons – rather a restricted set of suppliers was invited to tender. The open request for tender was for an *Official History of ASIO.*

ASIO uses procurement panels – which are guided by Australian Government procurement policy – to engage providers of goods and services.

Information Services

Release of ASIO Records

ASIO is an exempt agency under the *Freedom of Information Act 1982*, but is subject to release of its records under the *Archives Act 1983* which allows for public access to all Commonwealth records over 30 years old.

Requests to access ASIO records that are at least 30 years old and not publicly released 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 between public access and the need to protect sensitive information. In most cases, the information is released and is available for public access.

During 2008–09, ASIO received 454 applications for access to records, a decrease from 530 in 2007–08. A total of 497 requests were completed in 2008–09 – including some requests carried over from 2007–08. The total number of pages examined during 2008–09 was 74,039 – an increase from the 63,932 folios assessed in 2007–08.

ASIO gives greater priority to requests from those seeking records on themselves or family members. There were 169 such requests completed in 2008–09 compared with 136 in

2007–08. Eighty-six percent of these were completed within the benchmark of 90 days in 2008–09 – slightly less than the percentage for 2007–08. The completion of 82 percent of all requests within the 90 days in 2008–09 from 90 percent in 2007–08 reflects the impact of assessing a number of very large and complex requests and also assessing in priority order, where multiple requests are lodged by one applicant.

Applicants dissatisfied with exemptions by ASIO can request a reconsideration of the decision. In 2008–09, there were 17 reconsiderations. In 15 cases, the NAA upheld the ASIO exemptions. For the remaining two cases, ASIO released further material. Applicants may also appeal to the Administrative Appeals Tribunal if their request is not completed within 90 days. One appeal of this nature was lodged in 2008–09. The hearing on this matter led to some reprioritisation.

The Inspector-General of Intelligence and Security (IGIS) investigated a complaint about the timeliness of processing applications in 2008–09. The IGIS focused primarily on ASIO's past archival practices for storage and copying of film. The IGIS noted that some of the practices had not been appropriate for the long-term retention of film. The IGIS recommended ASIO consult with the NAA on the suitablity of future storage practices. This has since occurred.

Table 6 illustrates ASIO's commitment to making archival information available.

Official History of ASIO

ASIO has commissioned Professor David Horner and the Australian National University to produce an unclassified history of ASIO for the period 1949 to 1978. This five-year project commenced in 2008–09.

Subject of Assessment	2003–04	2004–05	2005–06	2006–07	2007–08	2008–09
Percentage of Folios released without exemption	35%	48%	45%	53.6%	63%	62%
Percentage of Folios released with part of text claimed as exempt	58%	46%	53%	43.8%	33%	37%
Percentage of Folios claimed as totally exempt	7%	6%	2%	2.6%	4%	1%
Percentage of Folios completed within the 90 days	–	84%	79%	92%	90%	82%
Total folio assessed	**32,708**	**41,181**	**45,454**	**52,234**	**63,932***	**74,039**

Table 6: Folios released by ASIO 2004–2009
*Included records of the Royal Commission on Intelligence and Security – 26,587 folios

Property

New Central Office

ASIO's central office is located in Russell in the Australian Capital Territory. It is the only publicly declared ASIO office, although ASIO occupies premises in every Australian state and territory.

In 2007–08, the Government approved a new special-purpose, high-security building for ASIO. In 2008–09, the Government approved a budget of $606m. The new building is being designed and constructed in partnership with the Department of Finance and Deregulation.

Site establishment works commenced in March 2009 and excavation works were scheduled to commence in July 2009. Occupation of the building is expected in late 2012. The location is Section 49, Parkes, within the Parliamentary Triangle and in close proximity to the Russell precinct.

The building will be in keeping with the National Capital Plan and the Griffin Legacy (under guidance of the National Capital Authority) and includes elements of environmentally sustainable design. The building will meet ASIO's future needs, with a design concept that integrates form and function.

It will accommodate up to 1,800 people and will operate 24 hours per day, with a level of security commensurate with ASIO's intelligence functions. The new central office work environment encompasses open plan work areas, purpose designed technical workspaces, a data centre, training areas and staff amenities. Incorporated into the design will be natural light and other amenities to enhance its appeal as an attractive workplace.

In October 2008, the planning phase was completed which included the development of the functional design brief, concept design and cost plan. On 24 November 2008, the delivery phase commenced and Bovis Lend Lease, the managing contractor, entered into the delivery phase contract with the Commonwealth. The delivery phase encompasses the detailed design documentation and construction of the building. GHD, the project consultant, continues to provide construction program oversight on behalf of the Commonwealth.

In December 2008, ASIO and the Department of Finance and Deregulation provided a confidential briefing to the Public Works Committee that gave the Committee an overview of the building design. ASIO will ensure the Committee receives regular confidential briefings on progress.

During 2009, local residents raised a number of concerns including whether the relevant planning processes had been followed. In response, the National Capital Authority publicly confirmed that approvals had been given in accordance with the National Capital Plan.

Project Location Map – Section 49 Parkes, ACT Insert right – View from Mount Ainslie

Left – Artist impression looking toward entrance to the Central Office from Constitution Avenue, Parkes, ACT.

Right – Artist impression of the building looking at the southern facade from Anzac Park East on Parkes Way, Parkes, ACT.

ASIO's New Central Office: Planning Approvals

ASIO and the Department of Finance and Deregulation are committed to ensuring that all relevant planning and building controls are in place, and no works are undertaken on the site without approval from the relevant authorities.

The Griffin Legacy Plan envisaged a number of smaller buildings along Constitution Avenue to foster the creation of a 'vibrant community'. The new central office design is accommodating the Griffin Legacy Plan in a number of ways, including the height of the building and main exterior finishes.

In 2008–09, the new central office received in-principle support from the National Capital Authority. Consultation with the National Capital Authority is actively maintained to ensure the appropriate works approvals are gained for all stages.

On 20 March 2009, a referral was lodged for the new central office under the *Environmental Protection and Biodiversity Conservation (EPBC) Act*. The referral, which included a Heritage Impact Assessment, was subsequently confirmed by the Department of the Environment, Water, Heritage and the Arts (DEWHA) as a 'non – controlled action'. This means that additional assessment by DEWHA is not required.

Green Design for ASIO's New Central Office

The new ASIO central office will achieve a 5 Star National Australian Built Environment Rating System and 4.5 Star Australian Greenhouse Building Rating to meet or exceed Commonwealth guidelines on energy efficiency.

Environmental design features include:

- solar panels on the roof to generate electricity for use within the building;
- energy efficient lighting;
- an 'active ventilation system' which will provide venting of heat during summer and further insulation in winter;
- air conditioning with 100 percent fresh air at floor level for a healthier work environment;
- harvesting of storm water for use in landscaping, irrigation and toilet flushing; and
- opportunity for the adoption of improved waste minimisation and recycling practices.

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

State and Territory Offices

New and refurbished offices provide secure, flexible and multi-functional environments that can be converted rapidly to accommodate operational task force units in response to emerging issues. The need to accommodate additional staff, undertake increased operational activities and refresh ageing facilities, has led to the establishment of an integrated property upgrade program.

During 2008–09, and in response to pressure from staffing growth, significant progress was made in upgrading accommodation as a result of funding received in 2006–07 and 2007–08. Reconfiguration and relocation of a number of ASIO offices also occurred. In 2009, the reconfiguration of the current ASIO central office was completed.

During 2008–09, the relocation of staff to new facilities in several states was finalised and ASIO is on track to finalise the current funded reconfiguration and relocation program by the end of 2009–10.

Environmental Performance

ASIO's demand for energy continues due to advances in technology, increases in staff numbers and the further expansion of ASIO's 24/7 operations.

While ASIO recognises that it is a large consumer of electrical energy, considerable effort is being placed on adopting practical new technologies to reduce consumption. All new or refurbished office fit-outs conform to an Australian Greenhouse Building Rating of at least 4 Stars.

The design and age of the ASIO central office in Canberra hinders significant improvements and restricts opportunities for long-term energy efficiencies. However, considerable improvement occurred during 2008–09 with the installation of power factor correction units and the upgrading of uninterrupted power supplies. ASIO has also progressively upgraded energy inefficient lighting.

At ASIO's new state offices, energy efficiency has been integrated into the design and encompasses the use of efficient lighting (incorporating daylight sensors, motion detectors and dimming capabilities) as well as water saving tapware. In addition, ASIO's New South Wales office power is supplied by a trigeneration plant which is equivalent to purchasing 50 percent green energy.

ASIO continues to recycle cardboard waste, computer packaging including polystyrene components, toner cartridges, unclassified information technology equipment and fluorescent tubes. The protection of national security material prevents ASIO from recycling classified waste or classified information technology equipment, with the exception of pulped paper waste. In addition, all ASIO contracts incorporate clauses that require contractors and sub-contractors to make the best use of recycled materials and remove fixtures and fittings for recycling wherever possible.

Corporate Governance

ASIO has a strong corporate governance framework and culture that takes into account the particular needs of an intelligence agency and the importance that the public and the Government place on ensuring ASIO is accountable, professional and impartial.

ASIO's corporate governance arrangements reflect the Organisation's sustained focus on risk management, accountability, performance measurement, building capability and managing growth.

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 4).

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.

The Director-General's Meeting comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. It manages the day-to-day business of ASIO, including areas of ongoing corporate priority and urgent or emerging issues requiring consideration by the Executive.

The Corporate Executive comprises the Director-General, Deputy Directors-General and First Assistant Directors-General. Several Assistant Directors-General on rotation and the Staff Association President attend as observers. It sets ASIO's strategic direction and oversees resource management, providing the main forum for managing strategic corporate priorities and resource issues. It also conducts detailed quarterly reviews of performance across the Organisation. The Corporate Executive files are reviewed by the Australian National Audit Office (ANAO) on a regular basis.

The Director-General's Meeting and the Corporate Executive provide oversight to eight ongoing and one non-ongoing corporate committees.

The Intelligence Coordination Committee, chaired by a Deputy Director-General, includes senior managers involved in the intelligence process. The Committee establishes security intelligence investigative priorities and allocates broad resources on a risk management basis. It also performs quarterly reviews against strategic objectives and approves arrangements for ensuring the legality and propriety of ASIO's intelligence collection, analysis and advice.

The Audit and Evaluation Committee, chaired by a Deputy Director-General, includes a senior executive officer from the ANAO. The Committee facilitates the internal audit of ASIO in accordance with the Internal Audit Charter, by setting priorities for audit, fraud control and evaluation planning. It considers the findings of the internal audits and evaluations, and ensures management-endorsed recommendations are implemented.

Figure 4: Corporate Governance

The Organisational Development Committee, chaired by the head of Corporate Management Division and including the Staff Association President, provides strategic guidance on ASIO's growth with particular regard to growing the capabilities of ASIO's staff, shaping an appropriate culture and managing change.

The Staff Placements Committee, comprising the two Deputy Directors-General, manages the strategic placement of staff across ASIO, addressing existing and longer-term priorities and capability gaps.

The Security Committee, chaired by the head of Security Division and including the Staff Association President, reviews and addresses key issues relevant to the security of ASIO's people, property and Information Technology systems. The Committee also drives development of security policies and practices.

The Research and Development Committee is chaired by the head of Technical

Capabilities Division and includes ASIO's Science Adviser and a representative from the Defence Science and Technology Organisation. It provides strategic oversight and direction to technical collection and analysis capability.

The Information Management Committee, chaired by the Chief Information Officer, provides strategic oversight and direction to ASIO's Information and Communication Technology (ICT) work program. Five program boards oversee ICT projects on a thematic basis, and report to the Committee.

The ASIO Consultative Council, co-chaired by the head of the Corporate Management Division and the Staff Association President, comprises representatives from management and the Staff Association. The committee is an advisory board which makes recommendations to the Director-General on human resource policies and practices. It facilitates management and staff discussion and resolution of issues of mutual interest and concern.

The New Building Committee (non-ongoing) provides strategic guidance on the new building project, including direction on significant design milestones, review of significant risk issues and oversight of project budget and program.

Accountability

ASIO operates under a rigorous oversight and accountability framework, which results in comprehensive scrutiny of ASIO's activities, and recognises that much of ASIO's work necessarily occurs outside the public view. This framework – including Ministerial and Parliamentary oversight and the IGIS – ensures that ASIO operates professionally and with propriety, and that the appropriate balance is struck between the requirements of security and the individual rights of Australians.

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 resources. 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.

Attorney-General

ASIO falls within the Attorney-General's portfolio. ASIO keeps the Attorney-General informed of its operations, investigations, and other matters relevant to its functions through written submissions, the presentation of special powers warrant requests, and oral briefings as required.

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

The *Attorney-General's Guidelines*:

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

The Guidelines, which are available on ASIO's website, do not broaden ASIO's powers beyond what the ASIO Act allows.

In 2008–09, ASIO provided 230 written submissions to the Attorney-General, compared with 249 in 2007–08.

Parliamentary Joint Committee on Intelligence and Security

The PJCIS reviews ASIO's (and the other intelligence agencies') 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.

Specifically, with regard to ASIO, the PJCIS is also responsible for:

- reviewing the listing of an organisation as a terrorist organisation under the *Criminal Code Act 1995*; 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.

Parliamentary Oversight

ASIO appears before the Senate Standing Committee on Legal and Constitutional Affairs as part of the Budget Estimates process. The Director-General of Security appeared before the Committee on 26 May 2009. ASIO also responded to six Questions on Notice from Parliament.

Inspector-General of Intelligence and Security

The role of the IGIS is to ensure ASIO and the five other agencies that comprise the Australian intelligence community (AIC) act legally and with propriety, comply with ministerial guidelines and show due regard for human rights. The IGIS may, in respect of ASIO, initiate inquiries, respond to requests by the Prime Minister or the Attorney-General, or investigate complaints from members of the public.

The IGIS conducts regular reviews of various aspects of ASIO's work including:

- use of special powers under warrant;
- access to and use of Australian Transaction Reports and Analysis Centre and Australian Taxation Office information;
- compliance with the *Archives Act 1983*;
- liaison with, and provision of information to, law enforcement agencies;
- provision of information on Australian persons to foreign liaison partners;
- inspections of ASIO's internal approvals of investigations;
- inspections of ASIO's interception management systems;
- authorisations for access to prospective telecommunications data; and
- retrospective inspections of selected ASIO operations.

Based on the various monitoring, inspection and inquiry activities undertaken by the Office of the IGIS in 2008–09, the IGIS was satisfied that there was no evidence of enduring, systemic deficiencies that would lead to breaches of propriety, the law or human rights. Further details can be found in the IGIS's *Annual Report* at www.igis.gov.au.

Public Accountability

Much of ASIO's work necessarily occurs outside the public view. Nevertheless, ASIO strives to provide public information on ASIO and its activities. Beyond ASIO's public statements through parliamentary accountability processes, the primary means by which ASIO provides information to the public are:

- ASIO's *Report to Parliament*;
- the ASIO website;
- responses to media enquiries; and
- public statements by the Director-General of Security.

ASIO produces a classified *Annual Report* which covers ASIO's operational and corporate activities in some detail. ASIO also produces an unclassified annual *Report to Parliament*, which provides a publicly available source of information on ASIO's activities. ASIO is the only agency within the AIC that produces a publicly available annual report.

The ASIO website is the primary source of public information about ASIO. It was updated

frequently throughout 2008–09, including with transcripts of the Director-General of Security's speeches, and job vacancies. The website also provides publications such as ASIO's *Reports to Parliament* and its *Corporate Plan 2007–2011*.

For recent recruitment rounds around 70 percent of all applicants became aware of the job vacancies via ASIO's or another website.

ASIO does not comment to the media on sensitive national security matters. It does, however, respond to general media enquiries through ASIO's Media Liaison Officer. In 2008–09, ASIO expanded its contact with journalists and the media, including through interviews on recruitment matters.

In 2008–09, the Director-General of Security addressed conferences and audiences from business, government and academia. Nine of these speeches are available on the ASIO website.

Internal Audits and Fraud Control

The Audit and Evaluation Committee maintains oversight of internal audit activity and fraud control within the Organisation, reporting to the Director-General of Security.

ASIO has an active program of internal audits and evaluations. During 2008–09, ASIO undertook an extensive review of risk management. This resulted in a draft *Strategic Risk Management Plan*, a risk-based *Annual Work Plan for 2009–10*, a *Strategic Audit Plan 2009–11*, a Risk Management Toolkit and Risk Management Policy and Framework.

In 2008–09, one evaluation was completed which reviewed the National Threat Assessment Centre (NTAC) to:

- determine the extent and efficacy of NTAC's internal and external consultation;
- assess the extent of key client satisfaction with NTAC product and services and with the quality of NTAC's assessments;
- assess the extent to which NTAC is delivering on its objective – 'to identify, analyse and issue assessments about threats to security' – especially the timeliness, quality and accuracy of its reporting;
- determine if NTAC is accessing all threat-related material available to the Australian Government; and
- assess the effectiveness of agency attachments to NTAC.

In 2008–09, nine internal audits were completed and were the subject of (classified) reporting to ASIO's Audit and Evaluation Committee. No loss of public monies was reported in these audits. Recommendations for improvements to administrative or procedural anomalies have been reviewed and accepted through the Committee and responsible work areas.

Fraud control in ASIO is a collective responsibility. Staff have two prime responsibilities – to not commit fraud and to report suspected instances of fraud. Investigation of one case of suspected fraud was completed, which found there was no case to answer, and no further cases were reported in 2008–09.

A new *Fraud Control Plan (2008–2010)* was implemented in December 2008 based on the 2008 Fraud Risk Assessment.

ASIO also completed the *Commonwealth Fraud Control Guidelines Annual Questionnaire* and holds data as required under the Guidelines. In accordance with the Guidelines, the AFP has been advised of ASIO's major fraud risks.

One of ASIO's main strategies in minimising fraud is an ethics and accountability program that all members of staff must attend at least once every three years. The Office of the IGIS contributes to this program.

In addition, all new staff, Senior Officers and relevant external providers and clients are provided with a user-friendly *Guide to Fraud Prevention, Detection and Reporting Procedures in ASIO*. Briefings are provided for all staff every five years through the newly-introduced Security Workshop and for all newly appointed Senior Officers on a Senior Officer Orientation Workshop.

Audit of Assumed Identities

All use of assumed identities by ASIO officers must be authorised by the Director-General of Security or an approved delegate under Part IAC of the *Crimes Act 1914 (Assumed Identities)*. Where evidence of an assumed identity is required from a New South Wales State Government agency, this will be authorised under the *Law Enforcement and National Security (Assumed Identities) Act 1998 (NSW).*

An assumed identity may be used to protect the true identity of an ASIO officer undertaking official duties. An assumed identity is only to be used by the person to whom it has been issued and for the purpose approved.

As required under both the Commonwealth and New South Wales assumed identity schemes, audits were conducted in January and July 2009 on records of authorisations, variations and revocations approved under the schemes in 2008–09. No discrepancies were detected.

As required by the legislation, a report for 2008–09 on the number of authorisations, the general activity undertaken with the use of assumed identities, and relevant audit results was provided to the IGIS.

Reviews and Inquiries

Report of the Inquiry into the Case of Dr Mohamed Haneef

Former New South Wales Supreme Court Justice John Clarke QC conducted an inquiry into the handling of the Dr Haneef case.

Mr Clarke was asked to examine and report on:

a. the arrest, detention, charging, prosecution and release of Dr Haneef, the cancellation of his Australian visa and the issuing of a criminal justice stay certificate;

b. the administrative and operational procedures and arrangements of the

Commonwealth and its agencies relevant to these matters;

c. the effectiveness of cooperation, coordination and interoperability between the Commonwealth agencies with state law enforcement agencies relating to these matters; and

d. having regard to (a), (b) and (c), any deficiencies in the relevant laws or administrative and operational procedures and arrangements of the Commonwealth and its agencies, including agency and interagency communication protocols and guidelines.

ASIO cooperated fully with Mr Clarke's inquiry and provided unlimited access to information and personnel. Mr Clarke completed his inquiry on 21 November 2008 and presented two reports (an unclassified volume and a volume of confidential attachments) to the Attorney-General. On 23 December 2008, the unclassified volume, titled *Report of the Inquiry into the Case of Dr Mohamed Haneef*, was tabled in Parliament. A copy of this report can be accessed at www.haneefcaseinquiry.gov.au. The Government's response to the Report can also be accessed at www.ag.gov.au.

Report of Inquiry into the Actions Taken by ASIO in 2003 in Respect of Mr Izhar Ul-Haque and Related Matters

Justice Adams of the New South Wales Supreme Court made negative comments in respect of ASIO during the 2007 trial of Izhar Ul-Haque, who was facing a charge arising from his purported training with Lashkar-e-Tayyiba. The IGIS commenced an 'own motion' inquiry into the matter. Specifically, he inquired into the actions taken by ASIO in respect of Mr Izhar Ul-Haque throughout 2003, and ASIO's policy, procedures and general practices on the interviewing of persons of security interest as they stood in November 2003 and currently, if different.

In November 2008, the IGIS completed his inquiry and presented a report to the Attorney-General (available from www.igis.gov.au). The IGIS concluded that ASIO's conduct was not ill-motivated or criminal.

The IGIS made recommendations concerning ASIO's training, policies and procedures, which have been, or are being, implemented.

Security of ASIO

ASIO collects and stores sensitive information, sometimes provided by international partners and often relating to Australian citizens and residents. Compromise of ASIO information or operations can cause harm to Australia's national security. It is crucial that ASIO information is protected from unauthorised disclosure, misuse, or inappropriate handling.

ASIO's Security Division is responsible for ensuring ASIO's security integrity. Best practice security is ultimately, however, reliant upon staff. ASIO staff undergo stringent vetting processes that include extensive background and suitability checking. ASIO has a strong security culture supported by comprehensive policies, and a regime to ensure

compliance. ASIO conducts regular security audits to ensure adherence to security standards and to identify areas where improvement is required.

ASIO security policies and practices meet or exceed the standards laid down in the *Australian Government Protective Security Manual* and its classified supplement, and the *Australian Government Information and Communications Technology Security Manual*. ASIO's security policies are consistent with Inter-Agency Security Forum security best practice guidelines.

Psychologists and other security professionals provide counselling and advice as part of ASIO's Employee Assistance Program. The program enhances ASIO's security and contributes favourably towards the health and well-being of staff.

In 2008–09, ASIO extensively revised the *ASIO Security Plan 2009–12* which provides strategies to mitigate security risks. It provides a framework for staff to ensure sound security is practised in daily business.

Counter-Intelligence

Counter-intelligence incorporates measures taken to counter security threats to ASIO and its staff. Counter-intelligence measures include the identification and investigation of threats to ASIO operations, security briefings to staff and contractors, management of the Contact Reporting Scheme (see also p. 28), and investigation of suspicious incidents. ASIO staff are encouraged to report suspicious incidents and these are investigated accordingly. The most enduring trends are reports of people impersonating ASIO officers, and people acting suspiciously around ASIO premises, for example, filming staff or ASIO premises.

Personnel Security

All ASIO permanent staff are security cleared to Top Secret level. In 2008–09, ASIO reviewed and authorised 526 new security clearances, 314 probation revalidations, 152 thirty-month mid-cycle revalidations, and 179 full re-evaluations. All ASIO staff responded to the annual revalidation process.

Reforms in the clearance revalidation process in 2008–09 included mechanisms to better identify potential security concerns early in an employee's tenure.

Physical Security

Ensuring that ASIO facilities are physically secure allows ASIO staff to have confidence in their work environment and protects classified information. ASIO's physical security arrangements are reviewed and upgraded continuously in line with advances in physical security technologies (including access control, camera and alarm systems, blast mitigation strategies and vehicle barriers) and changes to threat levels.

The relocation and renovation of ASIO offices through the year created a high demand for physical security advice.

Information Security

ASIO's information security policies were consolidated into the comprehensive (classified) *ASIO Information Security Policy*.

Emergency Management

Staff safety is the paramount concern in ASIO's emergency management policies and procedures. ASIO's key emergency management documents were reviewed, with significant effort directed towards practices and promoting procedures.

Part Four FINANCIAL STATEMENTS

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2009 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.

(acting) Director-General of Security

30 September 2009

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 2009, which comprise: a Statement by the Director-General of Security; Income Statement; Balance Sheet; Statement of Changes in Equity; Cash Flow Statement; Schedule of Commitments; Schedule of Contingencies; and Notes to and forming part of the Financial Statements, including a Summary of Significant Accounting Policies.

The Responsibility of 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 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, 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 2009 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
30 September 2009

INCOME STATEMENT

for the period ended 30 June 2009

	Notes	2009 $ '000	2008 $ '000
INCOME			
Revenue			
Revenue from Government	3A	**352,653**	291,460
Sale of goods and rendering of services	3B	**5,230**	4,556
Total Revenue		**357,883**	296,016
Gains			
Other gains	3C	**3,847**	8,093
Total Gains		**3,847**	8,093
Total Income		**361,730**	304,109
EXPENSES			
Employee benefits	4A	**158,508**	139,614
Suppliers	4B	**133,457**	120,722
Depreciation and amortisation	4C	**52,090**	42,399
Finance costs	4D	**626**	283
Write-down and impairment of assets	4E	**7,238**	714
Foreign exchange losses	4F	**2**	6
Net losses from sale of assets	4G	**242**	40
Total Expenses		**352,163**	303,778
Surplus attributable to the Australian Government		**9,567**	331

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

BALANCE SHEET

as at 30 June 2009

	Notes	2009 $ '000	2008 $ '000
ASSETS			
Financial Assets			
Cash and cash equivalents	5A	**10,246**	29,168
Trade and other receivables	5B	**283,286**	207,373
Other financial assets	5C	**1,061**	1
Total financial assets		**294,593**	236,542
Non-Financial Assets			
Land and buildings	6A,D	**89,019**	59,264
Infrastructure, plant and equipment	6B,D	**102,317**	95,144
Intangibles	6C,E	**21,247**	26,369
Other non-financial assets	6F	**12,254**	12,582
Total non-financial assets		**224,836**	193,359
Total Assets		**519,429**	429,901
LIABILITIES			
Payables			
Suppliers	7A	**13,673**	16,022
Other payables	7B	**3,918**	2,270
Total payables		**17,591**	18,292
Interest Bearing Liabilities			
Lease incentives	8	**3,989**	2,589
Total interest bearing liabilities		**3,989**	2,589
Provisions			
Employee provisions	9A	**43,132**	36,457
Other provisions	9B	**7,764**	5,987
Total provisions		**50,896**	42,444
Total Liabilities		**72,476**	63,325
Net Assets		**446,953**	366,576
EQUITY			
Contributed equity		**424,780**	353,970
Reserves		**8,894**	8,894
Retained surplus		**13,279**	3,712
Total Equity		**446,953**	366,576
Current assets		**306,847**	249,124
Non-current assets		**212,582**	180,777
Current liabilities		**44,493**	50,015
Non-current liabilities		**27,983**	13,310

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

STATEMENT OF CHANGES IN EQUITY

as at 30 June 2009

	Retained Earnings		Asset Revaluation Reserve		Contributed Equity/Capital		Total Equity	
	2009	2008	**2009**	2008	**2009**	2008	**2009**	2008
	$'000	$'000	**$'000**	$'000	**$'000**	$'000	**$'000**	$'000
Opening Balance	**3,712**	3,381	**8,894**	8,894	**353,970**	195,309	**366,576**	207,584
Income & Expenses								
Surplus (Deficit) for the period	**9,567**	331	**-**	-	**-**	-	**9,567**	331
Transactions with Owners								
Contributions by Owners								
Appropriation (equity injection)	**-**	-	**-**	-	**70,810**	158,661	**70,810**	158,661
Closing Balance attributable to the Australian Government	**13,279**	3,712	**8,894**	8,894	**424,780**	353,970	**446,953**	366,576

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

CASH FLOW STATEMENT

for the period ended 30 June 2009

	Notes	2009 $ '000	2008 $ '000
OPERATING ACTIVITIES			
Cash received			
Goods and services		**8,066**	3,226
Appropriations		**270,000**	214,623
Net GST received		**19,083**	18,234
Other cash received		**5,722**	6,718
Total cash received		**302,871**	242,800
Cash used			
Employees		**150,928**	135,089
Suppliers		**153,455**	139,469
Total cash used		**304,383**	274,558
Net cash from or (used by) operating activities	**10**	**(1,512)**	(31,758)
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		**542**	1,071
Total cash received		**542**	1,071
Cash used			
Purchase of property, plant and equipment		**82,978**	54,630
Purchase of intangibles		**7,815**	16,755
Total cash used		**90,793**	71,385
Net cash from or (used by) investing activities		**(90,251)**	(70,314)
FINANCING ACTIVITIES			
Cash received			
Appropriations - contributed equity		**72,842**	114,926
Total cash received		**72,842**	114,926
Net cash from or (used by) financing activities		**72,842**	114,926
Net increase or (decrease) in cash held		**(18,922)**	12,854
Cash and cash equivalents at the beginning of the reporting period		**29,168**	16,314
Cash and cash equivalents at the end of the reporting period	**5A**	**10,246**	29,168

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

SCHEDULE OF COMMITMENTS

as at 30 June 2009

	Notes	2009 $ '000	2008 $ '000
BY TYPE			
Commitments receivable			
Sublease rental income		**7,257**	1,877
GST recoverable on commitments		**11,304**	18,024
Total commitments receivable		**18,561**	19,901
Commitments payable			
Capital commitments			
Land & buildings		**165,093**	-
Infrastructure, plant and equipment	A	**295**	32,316
Intangibles		**-**	203
Other capital commitments		**-**	20,452
Total capital commitments		**165,388**	52,971
Other commitments			
Operating leases	B	**233,492**	148,176
Other commitments		**9,354**	-
Total other commitments		**242,846**	148,176
Net commitments by type		**389,673**	181,246
BY MATURITY			
Commitments receivable			
Operating lease income			
One year or less		**1,629**	1,877
From one to five years		**5,628**	-
Total operating lease income		**7,257**	1,877
Other commitments receivable			
One year or less		**2,433**	6,714
From one to five years		**5,663**	6,776
Over five years		**3,208**	4,533
Total other commitments receivable		**11,304**	18,024
Commitments payable			
Capital commitments			
One year or less		**24,764**	52,971
From one to five years		**140,624**	-
Total capital commitments		**165,388**	52,971
Operating lease commitments			
One year or less		**36,943**	23,767
From one to five years		**129,175**	74,541
Over five years		**67,374**	49,868
Total operating lease commitments		**233,492**	148,176
Other commitments			
One year or less		**8,695**	-
From one to five years		**659**	-
Total other commitments		**9,354**	-
Net commitments by maturity		**389,673**	181,246

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:

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.

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

SCHEDULE OF CONTINGENCIES

as at 30 June 2009

	2009	2008
	$ '000	$ '000
	Claims for damages or costs	
Contingent liabilities		
Balance from previous period	**-**	-
New	**27**	
Total contingent liabilities	**27**	-
Net contingent liabilities	**27**	-

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 statement should be read in conjunction with the accompanying notes.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

for the year ended 30 June 2009

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, for Government business and national infrastructure, and for 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 a general purpose financial report. 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 2008 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 2008; 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 is 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 Income Statement 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.

Contributions of assets at no cost of acquisition or for nominal consideration are recognised as gains at their fair value when the asset qualifies for recognition, unless received from another government agency as a consequence of a restructuring of administrative arrangements.

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.

1.8 Employee Benefits

Liabilities for services rendered by employees are recognised at the reporting date to the extent that they have not been settled.

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 2007. The estimate of the present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

During 2008-09 a comprehensive review of all employees' long service leave entitlements as at 30 June 2009 was undertaken. This resulted in an increase to Employee Provisions, of which $8,170,329 was accrued in periods prior to 2008-09. This has been reflected in the Employee Provisions liability, with a corresponding adjustment to Retained Earnings.

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 non-current 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 a non-current 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'. They are included in current assets, except for maturities greater than 12 months after the balance sheet date. These are classified as non-current assets. 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 Income Statement.

1.13 Financial Liabilities

ASIO classifies its financial liabilities as '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, 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 (2008: $2,000), 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
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:

	2009	2008
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 2009. Where indications of impairment exist, the asset's recoverable amount is estimated and an impairment adjustment made if the asset's recoverable amount is less than its carrying amount.

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

1.17 Intangibles

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

Software is amortised on a straight-line basis over its anticipated useful life. The useful lives of ASIO's software is 4-5 years (2007-08: 4-5 years).

All software assets were assessed for indications of impairment as at 30 June 2009.

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 2009 financial statements. (2008: Nil)

Note 3: Income

	2009 $ '000	2008 $ '000
Revenue		
Note 3A: Revenue from Government		
Appropriation - Departmental outputs	**352,653**	291,460
Total revenue from Government	**352,653**	291,460
Note 3B: Sale of goods and rendering of services		
Provision of goods - related entities	**225**	8
Provision of goods - external entities	**5**	19
Rendering of services - related entities	**4,658**	4,302
Rendering of services - external entities	**341**	227
Total sale of goods and rendering of services	**5,230**	4,556
Gains		
Note 3C: Other gains		
Resources received free of charge	**100**	1,375
Rent	**1,512**	2,310
Interest	**7**	-
Repayment of costs shared by other agencies	**1,490**	2,273
Miscellaneous	**738**	2,135
Total other gains	**3,847**	8,093

Note 4: Expenses

Note 4A: Employee benefits		
Wages and salaries	**121,221**	111,612
Superannuation:		
Defined contribution plans	**6,438**	4,257
Defined benefit plans	**17,336**	14,849
Leave and other entitlements	**13,245**	8,587
Separation and redundancies	**268**	309
Total employee benefits	**158,508**	139,614

Note 4B: Suppliers	2009 $ '000	2008 $ '000
Provision of goods - related entities	**1,326**	963
Provision of goods - external entities	**7,606**	16,651
Rendering of services - related entities	**25,677**	23,651
Rendering of services - external entities	**75,416**	62,348
Operating lease rentals - external entities:		
Minimum lease payments	**22,087**	16,336
Workers' compensation premiums	**1,345**	773
Total supplier expenses	**133,457**	120,722

Note 4C: Depreciation and amortisation		
Depreciation		
Infrastructure, plant and equipment	**28,377**	25,047
Buildings	**12,079**	10,097
Total depreciation	**40,456**	35,144
Amortisation		
Intangibles - computer software	**10,501**	6,721
Other intangibles	**1,133**	534
Total amortisation	**11,634**	7,255
Total depreciation and amortisation	**52,090**	42,399

Note 4D: Finance costs		
Unwinding of discount	**626**	283
Total finance costs	**626**	283

Note 4E: Write down and impairment of assets		
Asset write-downs from:		
Impairment of receivables	**1,123**	2
Writedown of land and buildings	**85**	-
Writedown of property, plant and equipment	**4,756**	712
Writedown of intangible assets	**148**	-
Impairment of intangible assets	**1,125**	-
Total write-down and impairment of assets	**7,238**	714

Note 4F: Foreign exchange losses	2009	2008
	$ '000	$ '000
Non-speculative	**2**	6
Total foreign exchange losses	**2**	6

Note 4G: Net losses from asset sales

Land and buildings		
Proceeds from sale	**-**	(541)
Carrying value of assets sold	**-**	533
Infrastructure, plant and equipment		
Proceeds from sale	**(512)**	(530)
Carrying value of assets sold	**754**	578
Intangibles		
Proceeds from sale	**(30)**	-
Carrying value of assets sold	**30**	-
Total losses from asset sales	**242**	40

Note 5: Financial Assets

Note 5A: Cash and cash equivalents

Cash on hand or deposit	**10,246**	29,168
Total cash and cash equivalents	**10,246**	29,168

Note 5B: Trade and other receivables

Goods and services		
Related entities	**1,677**	5,494
External entities	**165**	410
Appropriations Receivable:		
for existing outputs	**278,775**	198,154
GST receivable from the Australian Taxation Office	**2,670**	3,315
Total trade and other receivables (gross)	**283,287**	207,373
Less impairment allowance account:		
Goods and services	**1**	-
Total trade and other receivables (net)	**283,286**	207,373

	2009 $ '000	2008 $ '000
Receivables are aged as follows:		
Not overdue	**282,671**	203,795
Overdue by:		
Less than 30 days	**98**	448
30 to 60 days	**452**	69
61 to 90 days	**25**	69
More than 90 days	**40**	2,992
Total receivables (gross)	**283,286**	207,373

Credit terms were net 30 days (2008: 30 days).

Note 5C: Other financial assets

Accrued Revenue	**1,061**	1
Total other financial assets	**1,061**	1

Note 6: Non-Financial Assets

Note 6A: Land and buildings

Freehold land		
fair value	**1,385**	1,385
Total freehold land	**1,385**	1,385
Buildings on freehold land		
fair value	**8,593**	6,885
accumulated depreciation	**(676)**	(237)
Total buildings on freehold land	**7,917**	6,648
Leasehold improvements		
work in progress	**6,715**	10,131
fair value	**92,898**	52,666
accumulated depreciation	**(19,897)**	(11,566)
Total leasehold improvements	**79,717**	51,231
Total land and buildings (non-current)	**89,019**	59,264

No indicators of impairment were found for land and buildings.

Note 6B: Infrastructure, plant and equipment	2009	2008
	$ '000	$ '000
Infrastructure, plant and equipment		
work in progress	**411**	9,007
fair value	**150,746**	112,741
accumulated depreciation	**(48,840)**	(26,604)
Total Infrastructure, plant and equipment (non-current)	**102,317**	95,144

No amounts were charged to the asset revaluation reserve in the equity section of the balance sheet.

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

Note 6C: Intangibles

Computer Software		
purchased - at cost	**17,882**	19,679
internally developed - in progress	**1,351**	5,009
internally developed - in use	**19,823**	16,689
Accumulated amortisation	**(16,684)**	(16,186)
Accumulated impairment	**(1,125)**	-
Total computer software	**21,247**	25,191
Other Intangibles		
Other Intangibles - at cost	**-**	1,937
Accumulated amortisation	**-**	(759)
Total computer software	**-**	1,178
Total intangibles (non-current)	**21,247**	26,369

Asset impairment testing identified two intangible assets with impairment indicators. Both assets were adjusted accordingly.

Note 6D: Analysis of Property, Plant and Equipment

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

	Land	Buildings	Buildings- Leasehold Improvement	Total Land & Buildings	Infrastructure, Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000	$'000
As at 1 July 2008						
Gross book value	1,385	6,885	62,797	71,067	121,748	192,815
Accumulated depreciation / amortisation and impairment	-	(237)	(11,566)	(11,803)	(26,604)	(38,407)
Net book value 1 July 2008	1,385	6,648	51,231	59,264	95,144	154,408
Adj Gross book value	-	-	(543)	(543)	(3,695)	(4,238)
Accumulated depreciation / amortisation and impairment	-	-	543	543	3,695	4,238
Adjusted Net book value 1 July 2008	1,385	6,648	51,231	59,264	95,144	154,408
Additions:						
by purchase	-	1,707	39,967	41,675	40,592	82,267
Revaluations and impairments through equity	-	-	-	-	-	-
Reclassification	-	-	243	243	469	712
Depreciation / amortisation expense	-	(439)	(11,639)	(12,078)	(28,377)	(40,455)
Disposals:						
Other disposals	-	-	(85)	(85)	(5,511)	(5,597)
Net book value 30 June 2009	1,385	7,917	79,717	89,019	102,317	191,336
Net book value as at 30 June 2009 represented by:						
Gross book value	1,385	8,593	99,613	109,591	151,157	260,748
Accumulated depreciation / amortisation and impairment	-	(676)	(19,897)	(20,573)	(48,840)	(69,413)
	1,385	7,917	79,717	89,019	102,317	191,336

PART FOUR

TABLE B - Reconciliation of the opening and closing balances of property, plant and equipment (2007-08)

	Land	Buildings	Buildings-Leasehold Improvement	Total Land & Buildings	Infrastructure, Plant & Equipment	Total
	$'000	$'000	$'000	$'000	$'000	$'000
As at 1 July 2007						
Gross book value	1,730	3,212	45,226	50,168	93,185	**143,353**
Accumulated depreciation / amortisation and impairment	-	-	(1,711)	(1,711)	(3,185)	**(4,896)**
Net book value 1 July 2008	1,730	3,212	43,515	48,457	90,000	**138,457**
Additions:						
by purchase	-	3,863	17,574	21,437	33,193	**54,630**
Depreciation/ amortisation expense		(239)	(9,858)	(10,097)	(25,047)	**(35,144)**
Reclassifications					(1,712)	**(1,712)**
Revaluations and impairments through equity	-	-	-	-	-	**-**
Disposals:						**-**
other disposals	(345)	(188)	-	(533)	(1,290)	**(1,823)**
Net book value 30 June 2008	**1,385**	**6,648**	**51,231**	**59,263**	**95,144**	**154,408**
Net book value as at 30 June 2008 represented by:						
Gross book value	1,385	6,885	62,797	71,067	121,748	**192,815**
Accumulated depreciation / amortisation and impairment	-	(237)	(11,566)	(11,803)	(26,604)	**(38,407)**
	1,385	**6,648**	**51,231**	**59,264**	**95,144**	**154,408**

Note 6E: Intangibles

TABLE A - 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:				
Other 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**

TABLE B - Reconciliation of the opening and closing balances of intangibles (2007-08)

	Computer software internally developed	Computer software purchased	Other Intangibles	Total
	$'000	$'000	$'000	$'000
As at 1 July 2007				
Gross book value	17,080	9,779	-	**26,859**
Accumulated depreciation / amortisation and impairment	(3,327)	(8,375)	-	**(11,702)**
Net book value 1 July 2007	13,753	1,404	-	**15,157**
Additions:				
by purchase or internally developed	6,762	9,993	-	**16,755**
Reclassification	-	-	1,712	**1,712**
Amortisation expense	(5,282)	(1,439)	(534)	**(7,255)**
Disposals	-	-	-	**-**
Net book value 30 June 2008	**15,233**	**9,958**	**1,178**	**26,369**
Net book value as at 30 June 2008 represented by:				
Gross book value	21,698	19,679	1,937	**43,314**
Accumulated depreciation / amortisation and impairment	(6,465)	(9,721)	(759)	**(16,945)**
	15,233	**9,958**	**1,178**	**26,369**

Note 6F: Other non-financial assets	2009 $ '000	2008 $ '000
Prepayments	**12,254**	12,582
Total other non-financial assets	**12,254**	12,582

All other non-financial assets are current assets.

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

Note 7: Payables

Note 7A: Suppliers

Trade creditors	**6,424**	-
Accrued expenses	**7,151**	16,022
Operating lease rentals	**98**	-
Total supplier payables	**13,673**	16,022

All supplier payables are current liabilities.
Settlement is usually made net 30 days.

Note 7B: Other payables

Salaries and wages	**2,530**	1,763
Superannuation	**365**	228
Unearned income	**613**	-
Other	**410**	279
Total other payables	**3,918**	2,270

All other payables are current liabilities.

Note 8: Interest Bearing Liabilities

Lease incentives	**3,989**	2,589
Total interest bearing liabilities	**3,989**	2,589
Lease incentives are represented by:		
Current	**539**	697
Non-current	**3,450**	1,892
Total interest bearing liabilities	**3,989**	2,589

Note 9: Provisions

	$ '000	$ '000
Note 9A: Employee provisions		
Leave	**43,132**	36,457
Total employee provisions	**43,132**	36,457
Employee provisions are represented by:		
Current	**25,078**	30,384
Non-current	**18,054**	6,073
Total employee provisions	**43,132**	36,457

During 2008-09 a comprehensive review of all employees' long service leave entitlements as at 30 June 2009 was undertaken. This resulted in an increase to Employee Provisions, of which $8,170,329 was accrued in periods prior to 2008-09. This has been reflected in the Employee Provisions liability, with a corresponding adjustment to Retained Earnings.

The classification of current includes amounts for which there is not an unconditional right to defer settlement by one year, hence in the case of employee provisions the above classification does not represent the amount expected to be settled within one year of reporting date. Employee provisions expected to be settled in twelve months from the reporting date is $25,712,622 (2008: $25,245,610), in excess of one year $17,418,986 (2008: $11,211,390).

	$ '000	$ '000
Note 9B: Other provisions		
Restoration obligations	**6,526**	5,987
Rent payable	**1,238**	-
Total other provisions	**7,764**	5,987
Other provisions are represented by:		
Current	**1,285**	641
Non-current	**6,479**	5,345
Total other provisions	**7,764**	5,987

	Restoration Obligations	Rent Payable	Total
Carrying amount 1 July 2008	**5,987**	**-**	**5,987**
Additional provisions made	**580**	**1,238**	**1,818**
Lease expiry	**(667)**	**-**	**(667)**
Unwinding of discount or change in discount rate	**626**	**-**	**626**
Closing balance	**6,526**	**1,238**	**7,764**

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

	2009 $ '000	2008 $ '000
Reconciliation of cash and cash equivalents per Balance Sheet to Cash Flow Statement		
Report cash and cash equivalents as per:		
Cash Flow Statement	**10,246**	29,168
Balance Sheet	**10,246**	29,168
Reconciliation of operating result to net cash from operating activities:		
Operating result	**9,567**	(1,303)
Depreciation/amortisation	**52,090**	42,399
Net write down of non-financial assets	**6,114**	712
Net loss on disposal of assets	**242**	40
(Increase)/decrease in receivables	**(77,945)**	(77,734)
(Increase)/decrease in accrued revenue	**(1,060)**	1,800
(Increase)/decrease in prepayments	**328**	(2,022)
Increase/(decrease) in employee provisions	**6,676**	6,159
Increase/(decrease) in provisions for makegood and rent	**1,777**	1,316
Increase/(decrease) in lease incentives	**1,400**	(575)
Increase/(decrease) in supplier payables	**(2,349)**	(15,994)
Increase/(decrease) in other payables	**1,644**	13,444
Net cash from/(used by) operating activities	**(1,516)**	(31,758)

Note 11: Contingent Liabilities and Assets

Quantifiable contingencies

The Schedule of Contingencies reports contingent liabilities in respect of claims for damages/costs of $27,000 (2008: Nil). This amount represents an estimate of ASIO's liability based on precedent cases. ASIO is defending the claims.

Unquantifiable contingencies

At 30 June 2009, 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. (2008: Nil)

Remote contingencies

ASIO does not have any remote contingencies.

Note 12: Executive Remuneration

The number of executive officers who received or were due to receive a total remuneration of $130,000 or more:	**2009**	2008
$145 000 to $159 999	**-**	5
$160 000 to $174 999	**3**	-
$175 000 to $189 999	**-**	1
$190 000 to $204 999	**4**	6
$205 000 to $219 999	**3**	4
$220 000 to $234 999	**7**	8
$235 000 to $249 999	**3**	6
$250 000 to $264 999	**6**	2
$265 000 to $279 999	**4**	8
$280 000 to $294 999	**6**	1
$295 000 to $309 999	**6**	1
$310 000 to $324 999	**7**	2
$325 000 to $339 999	**1**	4
$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**	1
$400 000 to $414 999	**1**	-
	59	51
The aggregate amount of total remuneration of executive officers shown above.	**$16,330,837**	$12,585,453
The aggregate amount of separation and redundancy/termination benefit payments during the year to executives shown above.	**-**	$104,843

Note 13: Remuneration of Auditors

Financial statement audit services are provided free of charge to ASIO.	**2009**	2008
The fair value of audit services provided was:		
Australian National Audit Office (ANAO)	**$100,000**	$86,980

No other services were provided by the Auditor-General.

Note 14: Financial Instruments

	2009 $'000	2008 $'000
Note 14A: Categories of financial instruments		
Financial Assets		
Loans and receivables		
Cash and cash equivalents	**10,246**	29,168
Trade receivables	**1,842**	5,904
Accrued revenue	**1,061**	1
Carrying amount of financial assets	**13,149**	35,073
Financial Liabilities		
At amortised cost		
Trade creditors	**6,522**	-
Accrued expenses	**7,151**	16,022
Carrying amount of financial liabilities	**13,673**	16,022

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 2009. (2008: Nil). The total expense from financial assets through the profit and loss for the period ending 30 June 2009 was $1,122,666 (2008: Nil).

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 2009 (2008: Nil).

Note 14D: Fair value of financial instruments

	2009 $'000 Carrying amount	2009 $'000 Fair value	2008 $'000 Carrying amount	2008 $'000 Fair value
FINANCIAL ASSETS				
Loans and Receivables				
Cash & cash equivalents	**10,246**	**10,246**	29,168	29,168
Trade receivables (net)	**1,842**	**1,842**	5,904	5,904
Accrued revenue	**1,061**	**1,061**	1	1
Total	**13,149**	**13,149**	35,073	35,073
FINANCIAL LIABILITIES				
At amortised cost				
Trade creditors	**6,522**	**6,522**	-	-
Accrued expenses	**7,151**	**7,151**	16,022	16,022
Total	**13,673**	**13,673**	16,022	16,022

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.

	2009	2008
	$'000	$'000
FINANCIAL ASSETS		
Loans and receivables		
Cash and cash equivalents	**10,246**	29,168
Trade receivables	**1,842**	5,904
Accrued revenue	**1,061**	1
Total	**13,149**	35,073
FINANCIAL LIABILITIES		
At amortised cost		
Trade creditors	**6,522**	-
Accrued expenses	**7,151**	**16,022**
Total	**13,673**	16,022

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

	2009	2008	**2009**	2008
	$'000	$'000	**$'000**	$'000
	Not past due nor impaired		**Past due or impaired**	
Loans and receivables				
Cash and cash equivalents [1]	**10,246**	29,168	**-**	-
Trade receivables [2]	**1,227**	2,326	**615**	3,578
Accrued revenue [3]	**1,061**	1	**-**	-
Total	**12,534**	31,495	**615**	3,578

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 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**
Total	**98**	**452**	**25**	**40**	**615**

Ageing of financial assets that are past due but not impaired for 2008

	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	448	69	69	2,992	3,578
Total	448	69	69	2,992	3,578

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 2007-08.

The following table illustrates the maturities for financial liabilities.

	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	**-**	**6,522**	**-**	**-**	**6,522**
Accrued expenses	**-**	**6,220**	**-**	**-**	**6,220**
Total	**-**	**12,742**	**-**	**-**	**12,742**

	2008 $'000 On demand	2008 $'000 within 1 year	2008 $'000 1 to 5 years	2008 $'000 > 5 years	2008 $'000 Total
At amortised cost					
Trade creditors	-	-	-	-	-
Accrued expenses	-	16,022	-	-	16,022
Total	-	16,022	-	-	16,022

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 2007-08. 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

	2009 $ '000	2008 $ '000
Balance carried from previous period	**160,621**	70,931
Appropriation Act:		
Appropriation Act (No.1) 2008-09 as passed	**352,653**	290,871
Appropriation Act (No.3) 2008-09 as passed	**-**	589
FMA Act:		
Repayments to the Commonwealth (FMA Act s30)	**1,975**	5,741
Appropriations to take account of recoverable GST (FMA Act *s30A*)	**10,499**	11,271
Relevant agency receipts (FMA Act s31)	**12,355**	5,274
Total appropriations available for payments	**538,103**	384,677
Cash payments made during the year (GST inclusive)	**313,751**	224,056
Balance of Authority to draw cash from the Consolidated Revenue Fund for Ordinary Annual Services Appropriations	**224,352**	160,621
Represented by:		
Cash at bank and on hand	**10,246**	29,168
Receivables - departmental appropriations	**214,106**	131,453
Total	**224,352**	160,621

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

Balance carried from previous year	**66,701**	22,965
Appropriation Act:		
Appropriation Act (No.2) 2008-09 as passed	**70,810**	149,616
Appropriation Act (No.4) 2008-09 as passed	**-**	9,045
FMA Act:		
Appropriations to take account of recoverable GST (FMA	**8,584**	6,963
Total appropriations available for payments	**146,095**	188,589
Cash payments made during the year (GST inclusive)	**81,426**	121,888
Balance of Authority to Draw Cash from the Consolidated Revenue Fund for Other than Ordinary Annual Services Appropriations	**64,669**	66,701
Represented by:		
Cash at bank and on hand	**-**	-
Receivables - departmental appropriations	**64,669**	66,701
Total	**64,669**	66,701

Note 16: Compensation and Debt Relief

	2009	2008
One payment was made during the reporting period under the 'Defective Administration Scheme'. (2008: Nil payments made).	**$1,247**	-

Note 17: Reporting of Outcomes

Note 17A: Net Cost of Outcome Delivery	2009	2008
	$'000	$'000
Expenses		
Departmental	**352,163**	303,778
Costs recovered from provision of goods and services to the non-government sector		
Departmental	**2,574**	4,654
Other external revenues		
Departmental	**6,395**	6,620
Net cost of outcome	**343,193**	292,504

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

ASIO does not report its revenue and expenses at output level.

Part Five APPENDICES AND INDICES

Appendix A: List of Proscribed Terrorist Organisations (30 June 2009)

- Abu Sayyaf Group;
- Al-Qa'ida;
- Al-Qa'ida in Iraq, previously known as Tanzim Qa'idat al-Jihad fi Bilad al Rafidayn;
- Al-Qa'ida in the Lands of the Islamic Maghreb (formerly known as Salafist Group for Call and Combat);
- Ansar Al-Sunna (also known as Ansar Al-Islam);
- Asbat al-Ansar;
- Hamas' Izz al-Din al-Qassam Brigades;
- Hizballah External Security Organisation;
- Islamic Army of Aden;
- Islamic Movement of Uzbekistan;
- Jaish-e-Mohammed;
- Jamiat ul-Ansar (formerly known as Harakat Ul-Mujahideen);
- Jemaah Islamiyah;
- Kurdistan Workers Party;
- Lashkar–e Jhangvi;
- Lashkar-e-Tayyiba; and
- Palestinian Islamic Jihad.

Groups that were relisted or proscribed in 2008–09:

- Abu Sayyaf Group;
- Al-Qa'ida;
- Al-Qa'ida in Iraq;
- Al-Qa'ida in the Lands of the Islamic Maghreb;
- Ansar al-Islam;
- Asbat al-Ansar;
- Hizballah External Security Organisation;
- Islamic Army of Aden;
- Islamic Movement of Uzbekistan;
- Jaish e-Mohammed;
- Jamiat ul-Ansar;
- Jemaah Islamiyah; and
- Lashkar-e Jhangvi.

Appendix B: 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	Nil
94(1A)(b)	The total number of warrants issued during the year under that Division	Nil
94(1A)(c)	The total number of warrants issued during the year under section 34E	Nil
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	Nil
94(1A)(e)	The total number of warrants issued during the year under section 34G	Nil
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	Nil
94(A)(f)(ii)	The number of hours each person spent in detention under such a warrant	Nil
94(A)(f)(iii)	The total of all those hours for all those persons	Nil
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	Nil

Appendix C: Workforce Statistics

	2004–05	2005–06	2006–07	2007–08	2008–09
Ongoing Full-time	693	800	1,125	1,263	1,452
Non-ongoing Full time[1]	155	178	55	52	49
Ongoing Part time	43	50	94	108	116
Non-ongoing Part time	22	27	18	12	19
Non-ongoing Casual	42	55	64	57	54
Total	**955**	**1,110**	**1,356**	**1,492**	**1,690**

Table 7: Composition of workforce 2004–05 to 2008–09

[1] Includes atttachments, locally engaged staff and contractors/consultants.

		2004–05	2005–06	200–07	2007–08	2008–09
Band 1	Female	4	5	7	6	7
	Male	10	17	17	29	35
Band 2	Female	1	1	2	2	4
	Male	4	4	8	11	12
Band 3	Male	1	1	1	2	2
Total		**20**	**28**	**35**	**50**	**60**

Table 8: SES equivalent classification and gender 2004–05 to 2008–09 (does not include the Director-General of Security)

Group	Total Staff [1]	Women	Race / Ethnicity [2]	ATSI [3]	PWD [4]	Available EEO Data [5]
SES (excl Director-General of Security)	60	11	2	0	2	56
Senior Officers [6]	418	152	52	0	7	374
AO5 [7]	502	253	100	1	5	425
AO1 – 4 [8]	599	321	87	2	6	555
ITO1 – 2 [9]	101	16	19	0	1	97
ENG1 – 2 [10]	10	0	0	0	0	10
Total	**1,690**	**753**	**260**	**3**	**21**	**1,517**

Table 9: Representation of designated groups within ASIO at 30 June 2009

1 Based on staff salary classifications recorded in ASIO's human resource information system.
2 Previously Non-English speaking background (NESB1 and NESB2).
3 Aboriginal and Torres Strait Islander.
4 People with a disability.
5 Provision of EEO data is voluntary.
6 Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications.
7 ASIO Officer grade 5 group translates to APS Level 6.
8 Translates to span the APS 1 to 5 classification levels.
9 Information Technology Officers Grades 1 and 2.
10 Engineers Grades 1 and 2.

Group	2004–05 %	2005–06 %	2006–07 %	2007–08 %	2008–09 %
Women [1]	43.14	45.9	45.50	45.44	44.56
Race/Ethnicity [2]	14.64	16.16	15.81	16.46	17.14
ATSI [3]	0.45	0.38	0.31	0.31	0.20
PWD [4]	1.59	1.36	1.17	1.38	1.38

Table 10: Percentage of representation of designated groups in ASIO 2004–05 to 2008–09

1 Percentages for women are based on total staff. Percentages for other groups are based on staff for whom EEO data was available.
2 Previously Non-English speaking background.
3 Aboriginal and Torres Strait Islander.
4 People with a disability.

ASIO MANAGERS			
SES Band 3	$194,372		minimum point
SES Band 2	$153,632		minimum point
SES Band 1	$128,855		minimum point
AEO3	$111,962		
AEO2	$101,571	to	$111,962
AEO1	$89,562	to	$96,675
INTELLIGENCE OFFICERS			
IO	$68,388	to	$78,006
ASIO OFFICERS			
ASIO Officer 5	$68,388	to	$78,006
ASIO Officer 4	$56,403	to	$61,569
ASIO Officer 3	$49,186	to	$52,999
ASIO Officer 2	$43,314	to	$47,913
ASIO Officer 1	$38,392	to	$42,321
ASIO ITOs			
SITOA	$111,962		
SITOB	$101,571	to	$111,962
SITOC	$89,562	to	$96,675
ITO2	$68,388	to	$78,006
ITO1	$52,999	to	$61,569
ASIO ENGINEERS			
SIO(E)5	$113,740		
SIO(E)4	$101,571	to	$111,962
SIO(E)3	$89,562	to	$96,675
SIO(E)2	$68,388	to	$78,006
SIO(E)1	$52,999	to	$61,569

Table 11: ASIO salary classification structure at 30 June 2009

Appendix D: Agency Resource Statement 2008–09

	Actual Available Appropriations for 2008-09 $'000	Payments Made 2008-09 $'000	Balance Remaining $'000
Ordinary Annual Services			
Departmental appropriation			
Prior year departmental appropriation	–	–	–
Departmental appropriation	352,653	270,000	82,653
S.31 Relevant agency receipts	5,730	5,230	500
Total	**358,383**	**275,230**	**83,153**
Departmental non-operating			
Equity injections	70,810	72,842	(2,032)
Total	**70,810**	**72,842**	**(2,032)**
Total Resourcing and Payments	**429,193**	**348,072**	**81,121**

Compliance Index

Part of Report	Annual Report requirements	Requirement	Page
	Letter of transmittal	Mandatory	III
	Table of contents	Mandatory	V
	Index	Mandatory	123
	Glossary	Mandatory	121
	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–VIII
	Summary of significant issues and developments	Suggested	XV–XVII
	Overview of department's performance and financial results	Suggested	XI
	Outlook for the following year	Suggested	11–12
	Significant issues and developments - portfolio	Portfolio departments - suggested	n/a
Departmental Overview	Overview description of department	Mandatory	IX–X
	Role and functions	Mandatory	IX–X
	Organisational structure	Mandatory	XIII
	Outcome and output structure	Mandatory	XIV
	Where outcome and output structure differ from PBS format, details of variation and reason for change	Mandatory	n/a
	Portfolio structure	Portfolio departments - mandatory	n/a
Report on Performance	Review of performance during the year in relation to outputs and contribution to outcomes	Mandatory	Part 2 13–40
	Actual performance in relation to performance targets set out in PBS/PAES	Mandatory	Part 2 13–40

	Performance of purchaser/provider arrangements	If applicable, mandatory	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 13–40
	Trend information	Suggested	Throughout
	Factors, events or trends influencing departmental performance	Suggested	Part 1 1–12
	Significant changes in nature of principal functions/services	Suggested	n/a
	Performance against service charter customer service standards, complaints data, and the department's response to complaints	If applicable, mandatory	XII, 62, 52–53
	Social justice and equity impacts	Suggested	n/a
	Discussion and analysis of the department's financial performance	Mandatory	XI
	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	Appendix D, 116
	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
Management Accountability			
Corporate Governance	Statement of the main corporate governance practices in place	Mandatory	Part 3 58–60
	Senior management committees and their roles	Suggested	Part 3 58–60
	Corporate and operational planning and associated performance reporting and review	Suggested	58–60

	Approach adopted to identifying areas of significant financial or operational risk and arrangements in place to manage risks	Suggested	n/a
	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	46, 64
	How nature and amount of remuneration for SES officers is determined	Suggested	n/a
External Scrutiny	Significant developments in external scrutiny	Mandatory	35, 62, 64–65
	Judicial decisions and decisions of administrative tribunals	Mandatory	23–24, 27, 53
	Reports by the Auditor-General, a Parliamentary Committee of the Commonwealth Ombudsman	Mandatory	n/a
Management of Human Resources	Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	Mandatory	Part 3 44–51
	Workforce planning, staff turnover and retention	Suggested	Part 3 43, 44
	Impact and features of collective agreements, determinations, common law contracts and AWAs	Suggested	50
	Training and development undertaken and its impact	Suggested	Part 3 45–48
	Occupational health and safety performance	Suggested	Part 3 50–51
	Productivity gains	Suggested	n/a
	Statistics on staffing	Mandatory	XVII, 43–45, 113–115
	Collective agreements, determinations, common law contracts and AWAs	Mandatory	Part 3 50

	Performance pay	Mandatory	Part 3 50
Assets Management	Assessment of effectiveness of assets management	If applicable, mandatory	n/a
Purchasing	Assessment of purchasing against core policies and principles	Mandatory	51–52
Consultants	A summary of statements detailing the number of new consultancy services contracts; the total actual expenditure on all new consultancy contracts; the number of ongoing consultancy contracts that were active; and the total actual expenditure on the ongoing consultancy contracts (inclusive of GST). Statement noting that information on contracts and consultancies is available through the AusTender website	Mandatory	52
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	52
Commonwealth Disability Strategy	Report on performance in implementing the Commonwealth Disability Strategy	Mandatory	51
Financial Statements	Financial statements	Mandatory	69–108
Other Information	Occupational health and safety	Mandatory	Part 3 50–51
	Freedom of Information	Mandatory	Part 3 52
	Advertising and Market Research	Mandatory	Part 3 43
	Ecologically sustainable development and environmental performance	Mandatory	Part 3 54, 56, 57
Other	Grant programs	Mandatory	n/a
	Correction of material errors in previous annual report	If applicable, mandatory	n/a

Glossary

ACBPS	Australian Customs and Border Protection Service
AFP	Australian Federal Police
AIC	Australian Intelligence Community
APS	Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
ASIS	Australian Secret Intelligence Service
AUSTRAC	Australian Transaction Reports and Analysis Centre
BLU	Business Liaison Unit
CDPP	Commonwealth Director of Public Prosecutions
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
DITRDLG	Department of Infrastructure, Transport, Regional Development and Local Government
DSD	Defence Signals Directorate
DSTO	Defence Science and Technology Organisation
IGIS	Inspector-General of Intelligence and Security
NSH	National Security Hotline
NTAC	National Threat Assessment Centre
ONA	Office of National Assessments
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PM&C	Department of the Prime Minister and Cabinet
PMV	Politically Motivated Violence
SES	Senior Executive Service
TIA Act	*Telecommunications (Interception and Access) Act 1979*

General Index

N

O

P

Q

R

S

T

U

V

W