Australian Government

Australian Security Intelligence Organisation

ASIO Report to Parliament

2013–2014

www.asio.gov.au

VISION

THE INTELLIGENCE EDGE FOR A SECURE AUSTRALIA

MISSION

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

VALUES

EXCELLENCE

Producing high-quality, relevant, timely advice

Displaying strong leadership and professionalism

Improving through innovation and learning

INTEGRITY

Being ethical and working without bias

Maintaining the confidentiality and security of our work

Respecting others and valuing diversity

RESPECT

We show respect in our dealings with others

ACCOUNTABILITY

Being responsible for what we do and for our outcomes

Being accountable to the Australian community through the government and the parliament

COOPERATION

Building a common sense of purpose and mutual support

Using appropriate communication in all our relationships

Fostering and maintaining productive partnerships

ASIO Report to Parliament

2013–2014

ISSN 0815-4562

Commonwealth Coat of Arms

The Commonwealth Coat of Arms is used in accordance with *Commonwealth Coat of Arms: information and guidelines,* November 2012, provided by the Department of the Prime Minister and Cabinet (http://www.dpmc.gov.au/guidelines/docs/CCoA_guidelines.pdf, viewed 9 May 2013)

Australian Government
Australian Security Intelligence Organisation

Director-General of Security

12 September 2014

A8589256

Senator the Hon George Brandis QC
Attorney-General
Parliament House
CANBERRA ACT 2600

Dear Attorney,

In accordance with section 94 of the *Australian Security Organisation Act 1979* (the ASIO Act), I am pleased to present to you ASIO's Annual Report for the year ending 30 June 2014.

As required by the ASIO Act, a copy of the *Report to Parliament 2013-14* – with deletions authorised by you to protect national security – is to be laid before each House of 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

Table of Contents

Part 5

Part 6

Part 7

Director-General's review

ASIO's mission is to identify and investigate threats to security and provide advice to protect Australia, its people and its interests in Australia and overseas.

The security environment

Australia currently faces a concerning, challenging and volatile security environment. This is ASIO's assessment based on intelligence ASIO collects, intelligence ASIO receives from others, and all other available information. It takes into account a spread of international tensions, an increase in the range and intensity of threats, and the difficulties Australia faces in responding to them. Australia is subject to significant and increasing threats simultaneously from both terrorism and clandestine or deceptive activity by foreign powers, occurring against a backdrop of significant geopolitical uncertainty.

Terrorism

The increased terrorist threat has a range of drivers, but chief among these is the Syrian conflict, which has now spread to Iraq. It has attracted would-be fighters and terrorists from around the world and provided an environment in which extremism, in its most abhorrent form, has both spread and flourished. A substantial number of Australians are in Syria and Iraq training and fighting with anti-government groups. Most of these individuals have gravitated to the most extreme groups, Jabhat al-Nusra and Islamic State of Iraq and the Levant.

At the end of the reporting period, ASIO was aware of 14 Australians who had died in Syria and Iraq during this conflict. This included the first known Australian suicide bomber in Syria, in September 2013. (In July 2014, shortly after the reporting period, another Australian conducted a suicide bombing near a Shia mosque in Iraq.) These events demonstrate one of ASIO's primary concerns with Australians travelling overseas to train and fight with extremist groups—that these individuals will undertake activities overseas causing death and injury.

ASIO is also concerned that individuals in Australia will be inspired by the conflict in Syria to commit terrorism here. Returnees from the conflict are likely to be radicalised and to have the knowledge, experience and networks to conduct a mass casualty attack in Australia or other Western countries. They are also likely to have increased influence over vulnerable youth. We have already seen returnees from Syria and Iraq undertake attacks in Europe. A significant proportion of those returning to Australia from fighting or training in Afghanistan in the early 2000s became involved in terrorist planning here, and recruited and encouraged others who had not travelled to join them in their plots. We are concerned that history will repeat itself in Australia.

It could also affect us overseas. The flood of foreign fighters into Syria comes from many parts of the world, including many from our region. The impact of this on the threat to Australian interests overseas is to increase the potential for terrorist violence from those returning to their home countries or those inspired by events in the Middle-East. Any such violence could be indiscriminate or, in some places, could be specifically directed at Australians or Australian interests.

Events in Syria and Iraq have also contributed to increased tensions between communities in Australia with links to those countries. This has led to occasional instances of communal violence. ASIO has worked in cooperation with communities and with other Australian Government agencies to try to mitigate these tensions.

It is important to recognise that Syria is only one part of the picture. Terrorist threats emanating from elsewhere persist, from the Middle-East to Africa to South and South-East Asia. Australia must remain alert to moves by organisations such as al-Qa'ida and its many franchises to undertake attacks in the West or against Western interests, including Australian interests, in other parts of the world. Other jihadist organisations not affiliated with al-Qa'ida but sharing its willingness to use violence to achieve their objectives are also active and have links into Australia. And politically motivated violence from sources other than jihadists also persists, from time to time involving Australians or touching on Australia's interests.

To protect Australia from these threats, ASIO has worked closely with law enforcement, intelligence and other partners to identify and disrupt extremist activity in Australia and to discourage and prevent Australians from travelling overseas to train and fight with extremist groups. The reporting period saw a substantial increase in the number of adverse security assessments ASIO issued in relation to Australian passports; this increase is almost entirely attributable to the Syrian conflict. ASIO works closely with the community in addressing the issue of home-grown terrorism. ASIO also contributed to the government's countering violent extremism strategy by identifying and diverting people at risk of violent extremism.

Espionage and clandestine foreign interference

ASIO's understanding of the threat from clandestine activity by foreign powers directed against Australia has increased over the past year, and the situation here is worse than previously thought. Harmful acts of clandestine or deceptive foreign activity against Australian interests continued throughout the reporting period. These utilised both 'traditional' methods of spying and foreign interference, and 'cyber' means. The scale and complexity of the challenge posed by this activity demand sustained attention from both government and industry. The compromise of sensitive Australian Government and business information has adverse consequences for Australia's national security. ASIO worked closely with business, government and key intelligence partners to counter the threat posed by these insidious attacks.

Appropriate and effective disclosure laws are important to ensure that improper conduct within government—including within intelligence agencies—is investigated and dealt with. ASIO welcomes the enactment of the *Public Interest Disclosure Act 2013*, which came into effect in January 2014 and provides appropriate protection against the unauthorised disclosure of intelligence information.

But continued unauthorised disclosures of sensitive information during the reporting period have highlighted the threat posed by self-motivated malicious insiders. Governments are entitled to hold secrets and individuals with privileged access to those secrets have obligations to protect them. In addition to its investigative response to unauthorised disclosures, ASIO works with partners to identify and address personnel security policy issues arising from such events.

Outlook

The challenges Australia faces from terrorism and clandestine foreign activity will persist. The impact of the conflicts in Syria and Iraq will be felt in Australia for many years to come, including through instances of communal violence and in the potential for Australians—including lone actors—inspired by the conflicts to engage in terrorism here or against Australia's interests overseas.

Foreign clandestine targeting of Australian government and business information will also persist, as will the threat from the actions of malicious insiders. Australia's defence will be multidimensional and will include raising awareness of the consequences for individuals who betray the trust associated with access to highly sensitive government information.

A security service in a democracy

The role of a security intelligence organisation is to identify and assess possible threats to national security or to the lives and safety of Australians in sufficient time and with sufficient accuracy to prevent such threats eventuating. Our work is predictive and advisory—an exercise in informing risk management and enabling government to take preventative actions. We also provide assessments, drawing on our understanding of the security environment, that help inform decision making, policy setting and the taking of action by others to ensure they are based on the best possible foundation of knowledge.

ASIO necessarily conducts most of its work in the background, away from public attention. However, as a result of developments in the security environment during the reporting period, ASIO's work has been subject to particularly sustained public commentary and speculation. ASIO has increased its public engagement to match the current level of public interest in its activities. ASIO's public commentary aims to explain the Organisation's role and to clarify misconceptions about the Organisation's activities and its legislated powers. That said, it is not appropriate for ASIO to comment on each and every item of public speculation or sometimes fanciful conspiracy theory relating to its work. ASIO adheres to the rule of law and operates under not just a strict legislative regime, but also comprehensive oversight and accountability regimes. It engages transparently with those oversight and accountability mechanisms established to provide public reassurance of the legality and propriety of ASIO's actions.

ASIO fulfils an essential role in our system of government, helping protect Australians and Australian interests from attempts to do us harm or cause us disadvantage. In doing so, it contributes to a safe and secure environment in which the nation, individuals and our democratic institutions can operate freely and prosper. Such a security service, operating under not just a strict legislative regime but also comprehensive oversight and accountability frameworks, helps us maintain a society in which, as Justice Hope said, '*public safety and individual liberty sustain each other*'.

Funding and financial performance

Over the last several years, ASIO has absorbed a number of additional functions and activities, while funding has remained steady. To accommodate this, ASIO has undertaken a range of efficiency measures—including cessation or reduction of a number of security functions, an organisational restructure, a reduction in ASIO's overseas presence and a reduction in the number of Senior Executive Level and Executive Level staff—in an effort to maximise the use of its appropriation. But the increased complexity and severity of security threats facing Australia, as well as their persistence into the medium and long-term, mean ASIO has now sought additional resourcing to provide a level of assurance to government that it can continue to respond adequately to these threats.

In early August 2014 the Prime Minister, the Hon. Tony Abbott MP, announced additional funding for ASIO and other counter-terrorism agencies as part of the government's response to the increased terrorism threat facing Australia.
The additional resources will increase intelligence officer, analyst and technical specialist numbers, strengthening the Organisation's human intelligence collection, technical collection, surveillance, investigation and assessment capabilities, as well as liaison with Australia's national security community and ASIO's counterpart security agencies overseas. While no amount of resourcing can provide the government with absolute certainty that all future terrorist attacks will be identified and prevented, the proposed additional resourcing will allow ASIO to build and sustain the capabilities required to give government a considerably greater level of assurance in relation to the long-term terrorism threat facing Australia. However, resourcing pressures will remain in relation to the Organisation's non-counter-terrorism focused areas.

Challenges to capability

The complexity and diversity of threats faced led to a heightened operational tempo over the reporting period and increased demands on ASIO's capabilities. The demands were further compounded by the challenges of the increasingly complex technical environment in which ASIO operates, and of legislation that has not kept pace with significant technological change.

The legislative framework under which ASIO operates was largely enacted more than 30 years ago; it is in the process of being modernised to maintain pace with the exponential increase in technological change since that time. Amendments such as streamlining ASIO's warrant-based intelligence collection powers, introducing a special intelligence operations scheme and requiring the retention of data by telecommunications providers are critical for ASIO to maintain its ability to provide an appropriate level of security assurance for Australia. The *National Security Legislation Amendment Bill (No. 1) 2014*, introduced into parliament outside the reporting period, proposes to put in place some of these mechanisms; it has been referred to the Parliamentary Joint Committee on Intelligence and Security for inquiry and report.

With the support of the Parliament of Australia in giving ASIO the capabilities it needs, I believe ASIO will be well placed to protect Australia from current and future threats.

I trust this report will provide some insight into the work of the nameless people of ASIO, who are to be commended for their conscientious professionalism in the support of national security and the safety and lives of their fellow Australians. This is my final annual report as Director-General of Security. I should like to express my gratitude and appreciation to the staff of ASIO, and to all others who have helped and supported me in my time with the Organisation.

David Irvine
Director-General of Security

The year at a glance

OUTCOMES AND ACHIEVEMENTS

During the reporting period, ASIO:

- initiated and continued security investigations into terrorism, espionage, foreign interference, communal violence and border integrity threats
- issued adverse security assessments in relation to 45 passports (compared to 18 in 2012–13)
- completed the following security assessments:
  - 27 149 visa security assessments
  - 159 288 counter-terrorism security assessments
  - 23 522 personnel security assessments
- provided assistance and advice in relation to over 50 litigation matters
- increased the security awareness of the private sector through briefings, publicly accessible reports and bilateral meetings
- implemented an internal framework for current and former public officials to make a public interest disclosure regarding ASIO, consistent with the *Public Interest Disclosure Act 2013*
- reviewed proposed draft legislation and subordinate rules and regulations to ensure a smooth transition from the previous accountability regime (under the *Financial Management and Accountability Act 1997*) to the new regime under the Public Governance, Performance and Accountability legislation
- completed 532 requests for ASIO records, requiring 56 261 pages to be examined
- reviewed and redeveloped ASIO's employment relations framework
- implemented the ASIO Professional Conduct and Behaviour Strategy and reviewed the Organisation's Values and Code of Conduct to ensure ASIO maintains a professional, ethical and high-performing workforce.

Guide to the report

The Director-General of Security provides an annual report to the Attorney-General on the activities of ASIO in accordance with section 94(1) of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). As stipulated in section 94(3) of the ASIO Act, the Attorney-General is required to table an unclassified version of that report, in each House of the Parliament of Australia, within 20 sitting days of receipt. That unclassified version is the Report to Parliament.

The Report to Parliament is an essential component of ASIO's accountability framework. Importantly, it allows ASIO to communicate information regarding its work to its partners and the Australian public.

Part

The Overview provides the Director-General of Security's review of the 2013–14 security environment, describes the role and functions of ASIO and illustrates the organisational structure.

1 **Part 1** summarises the current state of the security environment and how ASIO expects the environment to evolve.

2 **Part 2** reports on ASIO's performance in protecting Australia, its people and its interests from threats to security, through intelligence collection, assessment and advice to government. The report informs parliament about the performance of ASIO against the outcomes and deliverables set out in the Portfolio Budget Statements 2013–14.

3 **Part 3** is a detailed report of ASIO's performance and operations against the outcome of protecting Australia, its people and its interests from threats to security. This part carries a national security classification of Top Secret and is excised by the Attorney-General in its entirety from the unclassified version of the report, as unauthorised disclosure could reasonably be expected to cause exceptionally grave damage to the security of the Australian Government.

4 **Part 4** explains ASIO's ministerial, parliamentary, independent and legislative oversight provisions and describes ASIO's accountability mechanisms, providing information on a range of audits and reviews to which ASIO has contributed.

5 **Part 5** provides information regarding ASIO's corporate strategy and governance arrangements, including the key highlights of the corporate services within ASIO.

6 **Part 6** details ASIO's audited financial statements for the 2013–14 financial year.

7 **Part 7** is a set of appendices and indices regarding ASIO's finances, resources and activities, as required by a range of legislation.

ASIO's role and functions

ASIO is responsible for protecting Australia, its people and its interests from threats to security, through intelligence collection and assessment and by providing advice to ministers, Commonwealth and state authorities and other approved entities.

The ASIO Act defines 'security' as the protection of Australia and its citizens from:

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

The ASIO Act also defines 'security' as including the carrying out of Australia's responsibilities to any foreign country in relation to the above matters.

As authorised by the ASIO Act, ASIO is responsible for providing security assessments regarding:

- people seeking entry to Australia
- people seeking access to classified material and designated security-controlled areas.

Section 17E of the ASIO Act also authorises ASIO to obtain foreign intelligence within Australia, under warrant, on matters related to national security, at the request of the Minister for Defence or the Minister for Foreign Affairs.

In investigating and responding to threats to security, ASIO works closely with a range of stakeholders, including members of the Australian Intelligence Community, law enforcement agencies, government departments, industry and members of the public. This engagement includes providing protective security advice to industry and communicating and cooperating with relevant authorities of foreign countries, as approved by the Attorney-General.

Organisational structure

ASIO has maintained a structure of eight divisions, following a close to a quarter reduction in the Senior Executive Service during the previous reporting period. ASIO further refined its organisational structure in this reporting period by combining its operational and support functions into two groups under each Deputy Director-General.

ASIO's organisational structure as at 30 June 2014

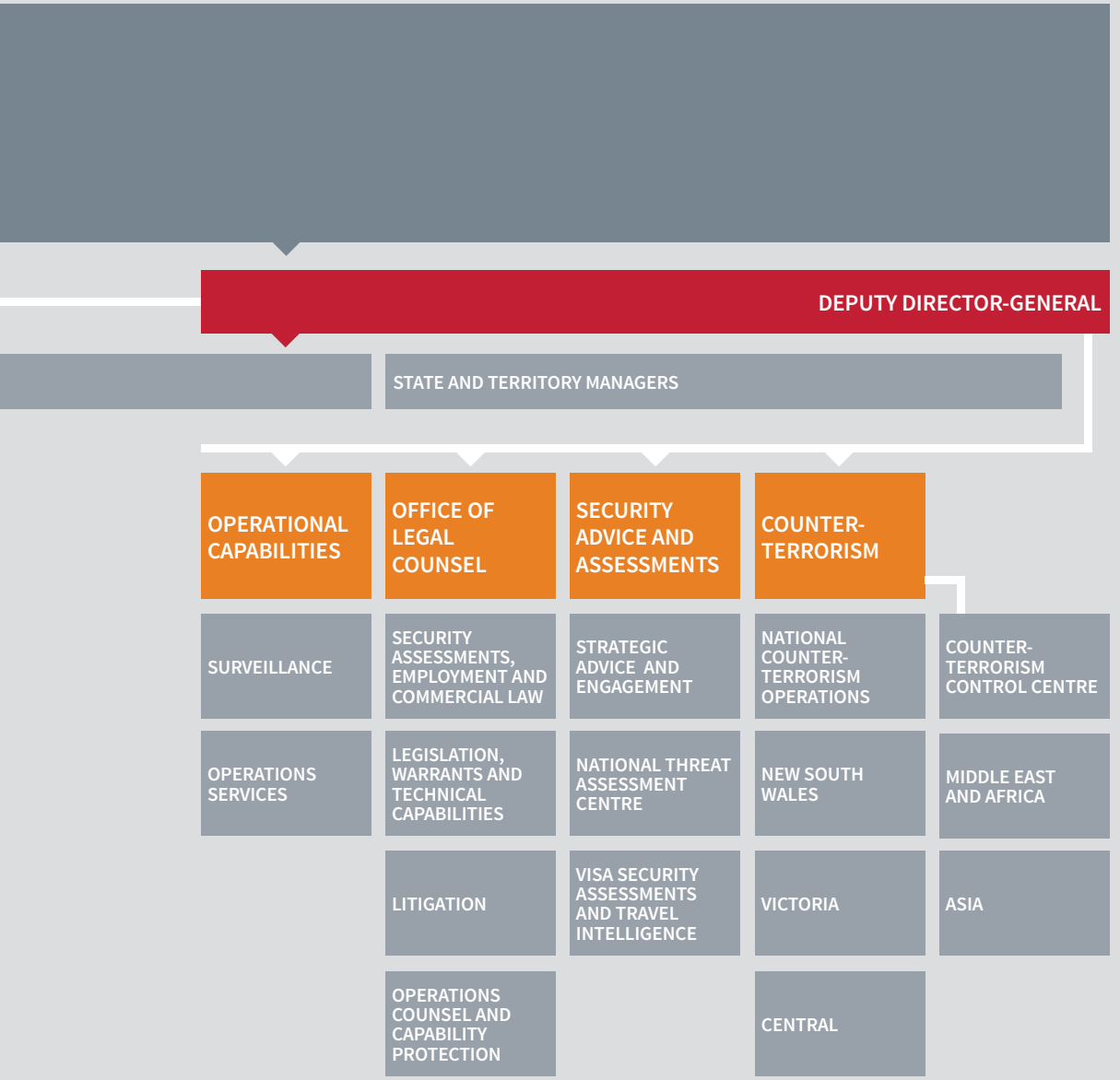
David Irvine

DIRECTOR-GENERAL OF SECURITY

DEPUTY DIRECTOR-GENERAL

- INTERNAL AUDIT
- OFFICE OF THE SENIOR EXECUTIVE

First Assistant Director-General	COUNTER-ESPIONAGE AND INTERFERENCE	INFORMATION	TECHNICAL CAPABILITIES	CORPORATE AND SECURITY
Assistant Director-General	COUNTER-ESPIONAGE AND INTERFERENCE A	IT INFRASTRUCTURE SERVICES	TELE-COMMUNICATIONS INTERCEPTION CAPABILITIES	INTERNAL SECURITY
	COUNTER-ESPIONAGE AND INTERFERENCE B	BUSINESS INFORMATION SERVICES	TELE-COMMUNICATIONS AND INFORMATION OPERATIONS	RESOURCE MANAGEMENT
	COUNTER-ESPIONAGE AND INTERFERENCE C	INFORMATION SERVICES	TECHNICAL OPERATIONS	HUMAN RESOURCES
	CYBER ESPIONAGE		TELE-COMMUNICATION SECTOR SECURITY	PROPERTY
			DATA EXPLOITATION CAPABILITIES	


DEPUTY DIRECTOR-GENERAL
STATE AND TERRITORY MANAGERS
OPERATIONAL CAPABILITIES
OFFICE OF LEGAL COUNSEL
SECURITY ADVICE AND ASSESSMENTS
COUNTER-TERRORISM
SURVEILLANCE
SECURITY ASSESSMENTS, EMPLOYMENT AND COMMERCIAL LAW
STRATEGIC ADVICE AND ENGAGEMENT
NATIONAL COUNTER-TERRORISM OPERATIONS
COUNTER-TERRORISM CONTROL CENTRE
OPERATIONS SERVICES
LEGISLATION, WARRANTS AND TECHNICAL CAPABILITIES
NATIONAL THREAT ASSESSMENT CENTRE
NEW SOUTH WALES
MIDDLE EAST AND AFRICA
LITIGATION
VISA SECURITY ASSESSMENTS AND TRAVEL INTELLIGENCE
VICTORIA
ASIA
OPERATIONS COUNSEL AND CAPABILITY PROTECTION
CENTRAL

Part 1

THE SECURITY ENVIRONMENT AND OUTLOOK

'The role of a security intelligence organisation is to identify and assess possible threats to national security or to the lives and safety of Australians in sufficient time and with sufficient accuracy to prevent such threats eventuating.'

David Irvine, Director-General of Security
2013 Sir Zelman Cowen Oration, Australian Institute of Public Affairs, 1 October 2013

Terrorism

The principal terrorist threat to Australia, Australians and Australian interests comes from those who adhere to a violent jihadist ideology and who view Australia and Australian interests as legitimate targets for attack. The jihadist movement is a worldwide phenomenon involving a range of groups and doctrines that are sometimes in conflict but are united in having an ultimate objective of driving 'apostates' and non-Muslims from Muslim lands and establishing an Islamic state ruled by extremists in accordance with their deviant interpretation of Islam. They are also in agreement on the need to use terrorist and other violence to achieve that objective. The threat comes from al-Qa'ida, its affiliates and like-minded groups and from organisations, such as the Islamic State of Iraq and the Levant (ISIL), that are separate to and sometimes in conflict with the al-Qa'ida axis. All share the view that Western countries, including Australia, are enemies of Islam and that terrorist attacks in Australia are not only legitimate and necessary but also obligatory. So the threat is multidimensional and complex.

Overseas influences and events continue to shape the Australian security environment. Australians have travelled overseas to fight in a number of jihadist theatres or to receive terrorist training, while others who remained in Australia have provided support and encouragement to overseas extremists and recruited new supporters to the jihadist cause.

Of these jihad theatres, by far the most significant over the past year has been Syria. Some Australians who have responded to the conflict share familial or personal links with Lebanon and Syria. Others without such personal links nevertheless see this conflict as a critical and defining moment in the jihadist struggle, particularly given the identification of al-Sham (Greater Syria) in Islamic prophecy as the location of apocalyptical struggles preceding the establishment of the final caliphate. During June 2014 the conflict expanded dramatically with an offensive by ISIL forces in northern and western Iraq. On 29 June 2014 ISIL declared the establishment of a caliphate and changed its name to the Islamic State.

The number of Australians training and fighting with, or otherwise assisting, groups involved in the conflicts in Syria and Iraq increased across the reporting period and is at an unprecedented level. At the end of the reporting period, ASIO was aware of approximately 60 Australians who were training or fighting in Syria or Iraq—most of these individuals had gravitated towards the most violent and extreme jihadist groups, including Jabhat al-Nusra and ISIL. Recruiters for these jihadist groups view fighters with English language skills and Western backgrounds—such as Australians—as valuable, particularly in the context of aspirations to undertake attacks in the West.

The extent of direct involvement of Australians in violence has also increased across the reporting period. The first known suicide bombing conducted by an Australian occurred in Syria in September 2013. A second suicide bombing conducted by an Australian was carried out in Iraq in July 2014, just outside the reporting period. Australians are also likely to have been directly involved in the murder of civilians and prisoners in Iraq. ASIO works with local and overseas partners to disrupt the travel of individuals likely to engage in activities prejudicial to national security. Australia has an international obligation not to export terrorism or other forms of political violence—it is an offence for Australians to take part in foreign incursions. The disruption of travel through means such as passport cancellation is one way Australia can meet those obligatons.

The travel of Australians to take part in jihad in Syria and Iraq has attracted much public attention, but it should be seen as part of a broader problem that also involves those who do not travel but are radicalised and support jihadist objectives and methods. Australians who have participated in the Syrian conflict as members of one or other of the extremist groups, and jihadist sympathisers in Australia who have not travelled, will present a threat to Australia's security both domestically and internationally well into the future. The numbers involved both in travel and local support are greater than in previous conflicts, and it is likely the future consequences for Australia will be commensurably greater.

By way of comparison, ASIO identified 30 Australians who travelled to Afghanistan or Pakistan to fight or train with Islamic extremist groups during the 1990s and early 2000s.

Of the 25 of these who returned to Australia, 19 continued to engage in activities of security concern and nine of those were involved in terrorist attack planning in Australia within five years of their return to Australia. The threat to security from such individuals comes from the skills they have acquired that would enable them to mount attacks domestically, the cachet they have in the extremist community and the capacity they possess to attract others to their cause and to motivate them to act. The nine Afghanistan returnees who engaged in attack planning in Australia did so in concert with an even greater number of extremists who had not travelled to fight. And it is not only Australians engaged in or engaged by the conflicts who pose a threat—other Westerners active in conflict areas could also readily pose a threat to Australians here or overseas.

Syria is not the only source of threat. Australian citizens continue to materially support or directly participate in terrorism in other theatres overseas, demonstrating the persistent and enduring appeal of the extremist message that persuades some Australians to join the cause of violent jihadists worldwide. Affected regions include large parts of Somalia, Yemen, Afghanistan and Pakistan. These locations continue to provide havens for al-Qa'ida and its affiliates and environments conducive to radicalisation, training and, potentially, plotting to target Western countries.

Inspire, the English-language magazine of al-Qa'ida in the Arabian Peninsula.

The threat of terrorism in Australia's region endures. Authorities in South-East Asia have had numerous counter-terrorism successes over a number of years, but extremist networks are resilient and will continue to be a threat to Western—including Australian—interests, as well as to local interests. A number of factors point to an increasing threat. The release of terrorist prisoners whose incarceration either has recently concluded or will do so in the year ahead is likely to strengthen these extremist networks. And in South-East Asia, as in other parts of the world, the Syrian conflict has served to energise extremists. Numbers of extremists from South-East Asia are travelling to Syria and training and fighting with the most extreme groups. Given the history of attacks on Australian interests in the South-East Asian region and continued identification of Australia as a specific target by regional extremists, these developments are of significant concern.

Individuals outside established groups may pose a 'lone actor' threat. A lone actor is an individual who plans or conducts violent acts for political or religious motives or to advance some personal cause. The lone actor may have some contact with other extremists but operates independently; may have no contact with other extremists but is inspired by an ideology promulgated by others; or may be completely self-contained. Regardless, their autonomy makes them difficult to detect.

The potential for lone actors to perpetrate terrorist acts has not gone unnoticed by jihadist organisations, and a number of jihadist online publications specifically target young men who might follow this path. The al-Qa'ida in the Arabian Peninsula publication *Inspire* includes a section specifically providing instructions on how to undertake lone actor attacks. An issue published during the reporting period included an interview with now deceased figure Anwar al-Aulaqi which stated, 'Weaken the enemy from within as much as you can. If we have brothers bringing the battle to the US, France, Britain, Germany, Denmark and Australia, that would have much more effect in weakening the enemy than having brothers join us from those countries'.

The internet, particularly video-sharing and social-networking sites, remains pivotal to extremists as a means of communication and networking and as a propaganda vehicle. More material than ever before is promoting and glorifying the ideology and actions of violent jihad. Adroit use of social media and modern communications technologies by Syrian jihadists has been central to the Syrian conflict and the ability of groups to attract Western fighters.

Extremist propaganda on the internet can strengthen and exacerbate extremist views among those who already hold them, and exposure to such material can accelerate a person's radicalisation process. On top of this, the internet's increasingly interactive nature enables radicalised users to engage with ideologues who incite violence and extremists who facilitate travel to jihadist theatres.

Extremism is relevant not only to jihadists. Far-right activity in Australia encompasses a broad range of right-wing groups and activists that operate at the fringes of the Australian political scene. Established far right-wing groups in Australia typically do not advocate violence to advance their nationalist or white supremacist cause, with acts of violence being rare. However, nationalist and ethnic tensions, violence overseas and activists involved in right-wing groups could have a bearing on Australia's security environment in the future.

ASIO takes a leadership role in guiding Australian Government responses to terrorism, including through threat assessments, security intelligence advice, contributions to policy development and legislative reform, active public engagement, and collaboration with Australian and international partners.

Espionage and clandestine foreign interference

Nations use a range of clandestine or deceptive activities, including undertaking espionage and other forms of foreign interference, in order to advantage themselves, to protect or project their national interests or to harm adversaries. Espionage and clandestine foreign interference activity against Australian interests is extensive. Foreign powers use a wide range of techniques and capabilities, including human intelligence, technical collection and exploitation of the internet and information technology, to obtain intelligence or disrupt use (cyber attack).

Competing national interests drive intelligence collection and foreign interference priorities, and nations will refine or expand information requirements and interference priorities in response to changing fortunes and international circumstances. The consequences of espionage and foreign interference are not fixed but will change as circumstances change—as international tensions increase, the stakes tend to become higher. Insofar as Australia can never predict where circumstances might take its relationships, all clandestine foreign activity against Australia must be taken seriously.

Information of interest to foreign intelligence services is not limited to classified or other protected material. Any non-public information that may confer advantage to another country—or protect its interests—is of potential value to a foreign intelligence service. Espionage is potentially detrimental to Australia's defence, intelligence, scientific and technical capabilities; its trade and economy; and its international relations.

The capabilities of foreign intelligence services vary widely, as does the potential for hostile intelligence activity to cause serious harm to Australian interests. In responding to this threat, ASIO pursues a three-part approach: to discover the most harmful clandestine activity; degrade its adverse impact on Australia; and defend against future harmful clandestine activity, including by contributing to resilient security policies and practices.

In 2013–14, the range, scale and sophistication of state actors engaged in hostile cyber espionage activity against Australian Government and private sector systems continued to increase. The potential access to large aggregations of valuable information, the plausible deniability it offers to state actors and the often difficult-to-detect nature of the activity ensure cyber espionage remains—and will continue to be—a widely used and increasingly sophisticated espionage vector. Critical to countering this persistent and highly damaging threat are holistic, well-established and widely adopted security practices and policies.

Working collaboratively with its national security partners, and leveraging the growing body of knowledge and expertise in this sphere, ASIO, together with the Australian Signals Directorate and the Computer Emergency Response Team, is actively promoting awareness of defensive responses to the threat from cyber espionage.

A broad awareness of the persistence, currency and scope of state-sponsored espionage is critical to ensuring Australia's defence against it. Consequently, ASIO continues to allocate substantial resources to defensive outreach and advice—to heighten awareness of the threat environment and to drive and shape appropriate security policy responses.

A range of foreign governments interfere in Australia's affairs in clandestine and deceptive ways designed to support or advance their interests. These acts of foreign interference may be carried out by intelligence services or others and may include the monitoring, coercion, or intimidation of diaspora communities; attempts to influence, or shape, commercial and government thinking to favour foreign interests; or other actions that are detrimental to Australia's interests. Foreign interference in Australia is pervasive and ongoing; it spans community groups, business and social associations, academic institutions and many other areas of civil society and is directed against all levels of government. ASIO is focused on discovering and defending against the most harmful foreign interference activities, which have the potential to adversely affect the fundamental principles of Australia's democratic freedoms.

Self-motivated individuals who exploit their privileged access to government information to make unauthorised disclosures of classified or other privileged information have always been a potential source of harm to Australia's national interests. The harm they can cause has been greatly increased by modern information technology, which allows large amounts of information to be aggregated and copied. The internet has amplified the harm by enabling the information to be distributed easily, as well as providing an audience to consume it.

Investigation of actions by individuals who abuse their privileged access to information, often motivated by personal grievances or agendas, is complex, resource intensive and highly sensitive. ASIO's methodology for investigating this threat is designed to ensure an appropriate and proportionate response, having close regard to both individual privacy considerations and the potential gravity of the harm being inflicted. It is a fundamental duty of government and its public servants to preserve and defend the nation's interests, and this includes holding secrets. Individuals who have or have had privileged access to confidential information have obligations to protect it, in many instances for life. For this reason, parliament has provided mechanisms to ensure accountability while preserving the confidentiality of information. ASIO has no interest in preventing individuals reporting what they believe to be wrongdoing and maladministration through established mechanisms, including mechanisms established under the *Public Interest Disclosure Act 2013*. ASIO's concern is unauthorised disclosure.

Edward Snowden is a compelling example of the wide-scale and indiscriminate harm that can be caused by malicious insiders. The damage caused by Snowden will be felt for many years. Of great concern is the very real potential the Snowden case will inspire and influence people who wrongly regard him as a whistleblower.

The Attorney-General, Senator the Hon. George Brandis QC, said in his speech to the Centre for Strategic and International Studies in Washington DC in April 2014:

> I know some people naively claim that Snowden is a whistleblower. That claim is profoundly wrong. As *The Economist*'s senior editor, Edward Lucas, points out in his recent book, *The Snowden operation*, Snowden meets none of the criteria of a whistleblower. According to a widely accepted series of tests developed by the Princeton scholar Professor Rahul Sagur in his book *Secrets and lies*, there are three principal criteria which define a whistleblower.
>
> First, a whistleblower must have clear and convincing evidence of abuse.
>
> Second, releasing the information must not pose a disproportionate threat to public safety.
>
> Third, the information leaked must be as limited in scope and scale as possible.
>
> Lucas concluded: 'Snowden has failed all three of these criteria'.

Communal violence and violent protest

Most Australian protests are peaceful, and there is little public support for the use of violent or destructive protest tactics. During 2013–14 some issues attracted large protests in Australia. The most notable protest platforms were the environment, animal rights and government policies. Events overseas—including in Syria, Egypt, Russia and Ukraine—have also attracted non-violent protest actions. Since the 2013 election, some protesters against Australian high-office holders have shown an increased willingness to employ confrontational and disruptive tactics.

Large protests occasionally result in violent clashes with police or law enforcement and in subsequent arrests. Planned acts of violence are usually organised by small numbers of protesters with an anarchist or revolutionary agenda who insert themselves into larger legitimate protest groups and then, in the course of protests, incite others to confront police or law enforcement.

The Group of Twenty (G20) Leaders Summit will be held in Brisbane on 15–16 November 2014, with 4000 delegates expected to attend. To support the summit, ASIO is providing G20-related security advice, including intelligence collection support, an extensive body of published assessments, protective security advice for the event organiser (Prime Minister and Cabinet's G20 Taskforce) and security checking of people requiring access accreditation.

Past G20 meetings have attracted violent and destructive protests resulting in mass property damage, injuries and arrests. Protests at the Brisbane summit are expected on a range of enduring platforms—such as anti-capitalism, anti-globalisation, anti-war and environmental platforms—and also on domestic issues, including Indigenous rights, marriage equality and refugee advocacy. Protest issues are fluid and driven by contemporary issues. While ASIO expects that most organised protests will be peaceful, the possibility of violence-prone protesters co-opting large-scale protests remains the key security concern.

LAWFUL PROTEST

Section 17A of the *Australian Security Intelligence Organisation Act 1979* states:

> This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the Organisation shall be construed accordingly.

ASIO investigates protest activity only where it includes, or has the potential to include, premeditated violence; where it has the potential to impinge on the security of designated people and places; or where ASIO suspects there is a link between the protest and conduct that may come within the definition of security.

ASIO's threat assessment function is an integral part of national arrangements for the protection of high-office holders, internationally protected persons, sites of national significance and critical infrastructure. ASIO may prepare threat assessments in relation to any demonstration or protest activity on the basis of information that ASIO already has or information that has been passed to ASIO by other agencies.

Australia has a low incidence of inter- or intra-communal violence. Past incidents of communal violence have tended to be in relation to specific local or international events that resonate locally and add to or reignite the residual influence of communal grievances elsewhere. The most prominent present example of this is the Syrian conflict. Since early 2011, tensions between Australia-based Shia and Sunni communities have continued in response to the ongoing violence in Syria. While these tensions have, for the most part, been managed peacefully within and between communities, they have occasionally escalated into sporadic acts of violence perpetrated by a small number of individuals. This violence is not representative of general Shia and Sunni community feeling, which continues to be demonstrated through peaceful protests, vigils and fundraising activities. However, the thresholds at which communal violence occurs can be difficult to predict, and tensions will remain as events unfold in Syria and Iraq.

Several groups have been established—primarily online—that espouse an anti-Islam agenda. Since May 2013, the scale and intensity of online anti-Islam rhetoric have increased in Australia. Anti-Islam groups and members of the Australian Muslim community have increasingly engaged in hostile, abusive and threatening online exchanges, some of which advocate violence. The potential exists for these tensions to develop into opportunistic acts of inter-communal violence.

Border integrity

Since July 2013, the number of illegal maritime arrivals has declined significantly. Awareness among potential illegal immigrants of Australian Government policies, and execution of these policies, has contributed to this decline. However, Australia's border integrity continues to be challenged, and maritime people smuggling continues to pose a threat to Australia's border integrity and security. People smugglers are resilient and adaptable, and some continue to target Australia.

Part 2

PROGRAM PERFORMANCE

'The public should have confidence that Australia is striking the proper balance between community human rights and individual human and civil rights. It should also have confidence that the nameless, hardworking people of ASIO understand that balance, that tension, and work within it. It is part of our DNA, as it should be in a security intelligence agency dedicated to protecting our democratic values and way of life.'

David Irvine, Director-General of Security
2013 Sir Zelman Cowen Oration, Australian Institute of Public Affairs, 1 October 2013

Outcome 1

ASIO's appropriation, identified in the 2013–14 Portfolio Budget Statement, is directed to a single outcome:

OUTCOME 1

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

ASIO has two key performance indicators:

- the contribution of ASIO's action and advice to the management and the reduction of risk to:
  - people and property
  - government business and national infrastructure
  - special events of national and international significance
- the security of ASIO's activities.

ASIO's outcome supports the Australian Government's policy aim of 'A secure Australia in a secure region'. In 2013–14 this outcome was separated into four program deliverables:

Deliverables

1. **Security intelligence analysis and advice** including strategic, investigative and complex analysis, threat assessments, border security, critical infrastructure protection, policy contribution and support to prosecutions.
2. **Protective security advice** including counter-terrorism checking, personnel security, physical security and contributing to policy development.
3. **Security intelligence investigations and capabilities** including the maintenance and enhancement of all-source security intelligence collection, complex tactical and technical analysis, technical research and development, counter-terrorism response, national and international liaison, and contributing to policy development.
4. **Foreign intelligence collection in Australia** at the request of the Minister for Foreign Affairs or the Minister for Defence, as well as incidentally through security intelligence capabilities and liaison with overseas partners.

DELIVERABLE 1

Security intelligence analysis and advice

ASIO provides assessment and advice on threats to Australians and Australian interests from politically motivated violence, violent protest, communal violence, espionage and foreign interference. Security intelligence analysis and the resulting advice inform stakeholders about the security environment and ASIO's work in countering threats to national security.

This deliverable includes:

- strategic assessment and advice
- threat assessment and advice
- counter-espionage threat assessment and advice
- industry engagement and advice
- proscription-related advice
- security assessment and advice
- border integrity investigations and analysis
- support to security intelligence–related prosecutions and litigation.

Strategic assessment and advice

ASIO's strategic intelligence assessments aim to provide insight into complex issues and foresight of future challenges to help policymakers, decision-makers and responders undertake their functions. They explore and explain the security environment looking at aspects of security issues including people, issues, events and ideologies, and identify or anticipate emerging national security threats. ASIO assessments directly support operational planning, policy development and resource management to help effective management of current and future threats.

Performance 2013–14

In 2013–14 terrorism-related assessments dominated ASIO's strategic analysis, with reports on the conflict in Syria—and the involvement of Australians in that conflict—accounting for almost half of the assessments issued. ASIO also produced assessments on issues such as border security, counter-intelligence, counter-espionage and developments in the regional security environment. The Organisation continued to draw on its work on understanding extremism and radicalisation in Australia to provide advice to the Countering Violent Extremism Taskforce, coordinated by the Attorney-General's Department, and provided strategic analytical support to Operation Sovereign Borders.

Threat assessment and advice

The National Threat Assessment Centre (NTAC) within ASIO, provides assessments and advice on security threats to Australian interests at home and abroad, threats to Australian and overseas dignitaries, violent protest threats, threats to diplomatic premises in Australia, threats to critical infrastructure sectors, and threats to major events. Threat advice helps stakeholders, including government and industry, understand their environment so that they can plan and implement protective security arrangements and risk management strategies. It also assists the Department of Foreign Affairs and Trade (DFAT) to formulate overseas travel advice for its smarttraveller.gov.au website.

NTAC is Australia's national authority for threat assessments. By bringing together officers from a number of agencies, NTAC facilitates a fusion of sector knowledge that is vital to its effectiveness. NTAC has seconded officers from the following agencies:

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

Performance 2013–14

In 2013–14 NTAC regularly updated its advice on terrorist and other threats to Australian interests overseas through a variety of analytical products. Most effort went to assessment and advice on areas where Australians and Australian interests were at greatest threat, but regular reviews of the global threat situation were undertaken. Threat advice was especially critical in respect of countries in the Middle East, Africa and South Asia regions—where al-Qa'ida-affiliated organisations and other terrorist groups control territory and conduct numerous attacks—and in South-East Asia, where terrorist networks persist and continue to pose a threat. These assessments informed a number of Australian Government processes, in particular the development of DFAT travel advice.

NTAC also disseminated advice to the state and territory law enforcement agencies responsible for providing security responses and ensuring public order during protests. Notification of protests specifically targeting Australian high-office holders helped other agencies to allocate security resources appropriately for protests. Overseas issues such as the Syria and Iraq conflicts resonated in Australia among Sunni and Shia communities, and NTAC worked closely with internal and external stakeholders to monitor community tensions for signs that grievances would manifest themselves in violent or destructive protests. Likewise, NTAC provided reporting on the threat of violence between anti-Islam groups and members of the Muslim community.

Image: Iurii Osadchi / Shutterstock.com

In 2013–14 NTAC prepared threat assessment advice to inform the protective security measures for a range of special events, including the Sochi 2014 Winter Olympics and Paralympics in Russia, and the 2014 FIFA Soccer World Cup in Brazil. NTAC also produced assessments to inform security-planning decisions related to Group of Twenty (G20) events in 2014.

NTAC continued to leverage relationships with key international partners who also produce threat assessment products.

Counter-espionage threat assessment and advice

During the reporting period, ASIO provided threat assessments and advice to government partners on the threat posed by foreign espionage and interference activities against Australian interests domestically and overseas, including domestic critical infrastructure, travelling dignitaries and ministers and special events including Australia's hosting of the G20 Summit.

An important aspect of ASIO's role is to build security awareness and resilience through a proactive, prioritised and targeted outreach program across government and industry. During the reporting period this included presentations on the foreign intelligence threat to Australian interests, continuation of the Contact Reporting Scheme, tailored presentations for major events such as the G20 Summit, and staffing of a dedicated position to manage relationships and engagement with agency security advisers.

Industry engagement and advice

Business Liaison Unit

ASIO works in partnership with the private sector to protect Australian interests, including national critical infrastructure. The Business Liaison Unit (BLU) is ASIO's key platform for engaging with the private sector.

The BLU is a resource for security managers, enabling them to:

- recognise and respond to national security threats
- develop appropriate risk mitigation strategies for such threats
- provide informed briefings to executives and staff.

The BLU provides declassified material drawn from intelligence holdings on a broad range of security topics, including the domestic and international threat environments, terrorist tactics, malicious activity indicators, cyber security, protective security, and espionage. The BLU publishes reports prepared by other Australian Government agencies and international partners on its independant website.

The BLU is not corporately funded or sponsored. Interested business and other entities can apply for access to BLU material by submitting an access request form, located on the website.

In addition, the BLU administers the Register of Australian Interests Overseas. This system invites business owners to register the details of their operations throughout the world, enabling ASIO to provide time-critical advice to subscribed companies in the event of an imminent and credible threat.

For further information, visit the BLU website www.blu.asio.gov.au.


Australian Government
Australian Security Intelligence Organisation

BLU Bulletin

ISSUE 18

ASIO Director-General's foreword

In this issue

www.blu.asio.gov.au

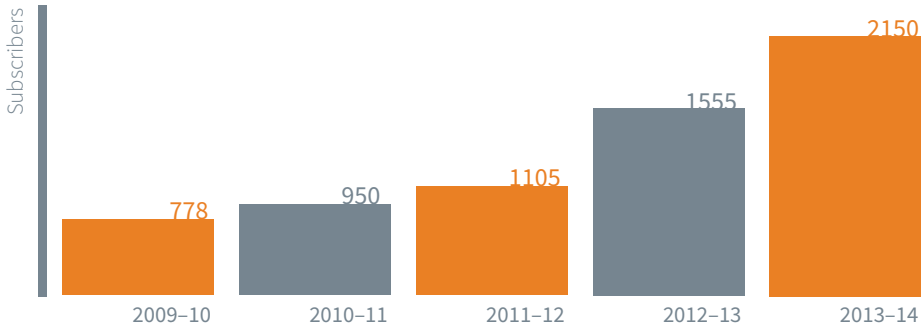
Performance 2013–14

In 2013–14 the BLU continued to meet its objective of providing security awareness to the private sector through bilateral meetings and group briefing days and by publishing reports on its website.

The BLU conducted 233 separate meetings with corporate security and risk managers across Australia, published 157 reports on its subscriber-based website (including 77 reports from foreign liaison counterparts and 14 reports from other Australian Government agencies) and hosted four dedicated security briefing days for corporate security managers from the defence industry security program, the energy and resources sector, the banking and finance sector, and a multi-sector security program.

The BLU has seen a steady increase in the number of subscribers to its website over the last five years. Last year the number of subscribers increased by 38 per cent, from 1555 to 2150.

Figure 1: Total number of BLU subscribers over the last five financial years



Cyber

The threat posed by malicious activity conducted by cyber means has continued to increase. During the reporting period, ASIO provided industry partners with security advice and defensive briefings on the threat posed by cyber espionage to sensitive information and intellectual property. ASIO also developed an intelligence-led outreach program aimed at identifying new and building upon existing productive relationships with private businesses to assist them mitigate these cyber threats.

The establishment of the Australian Cyber Security Centre in late 2014 is expected to deliver substantial dividends and momentum on cyber security issues, not least in enhancing coordinated and targeted industry outreach.

Proscription-related advice

The proscription of an organisation identifies it as a 'terrorist organisation', establishing a number of terrorist offences in relation to the group. Under Division 102 of the *Criminal Code Act 1995*, the government can proscribe an organisation if the Attorney-General is satisfied on reasonable grounds that the organisation:

- is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not a terrorist act has occurred or will occur); or
- advocates the doing of a terrorist act (whether or not a terrorist act has occurred or will occur).

To inform the Attorney-General's decision-making, ASIO provides the Attorney-General's Department with advice about organisations where ASIO assesses a case has been made for proscription. This advice is provided in an unclassified Statement of Reasons, which is prepared in consultation with other government agencies and, upon an organisation's proscription, is made publicly available via the Australian Government's National Security website.

As at 30 June 2014, the Australian Government had proscribed 19 organisations.

Performance 2013–14

During 2013–14, the Attorney-General renewed the proscription of seven terrorist organisations—the Abu Sayyaf Group, al-Qa'ida, al-Qa'ida in the Arabian Peninsula, al-Qa'ida in the Lands of the Islamic Maghreb, the Islamic State of Iraq and the Levant, Jamiat ul-Ansar and Jemaah Islamiyah—and proscribed Boko Haram for the first time. In each case, ASIO provided advice to help inform the Attorney-General's decision. ASIO also briefed the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the groups re-proscribed during 2013–14.

Security assessment and advice

Part IV of the ASIO Act authorises ASIO to provide other government agencies with security assessment advice on individuals. ASIO may issue security assessments to the Department of Immigration and Border Protection (DIBP) in relation to the granting or holding of a visa, or citizenship to DFAT in relation to the issuing of a passport, or to another government organisation in relation to a person's access to national security-classified information. ASIO may also issue security assessments in relation to access to certain security-controlled areas (such as airports or ports) or certain security-controlled substances.

The purpose of this function is to identify people who pose a threat to security—for example, on the grounds of terrorism or espionage—and to ensure that government agencies take this security consideration into account in their decision-making. Government agencies may request a security assessment, or ASIO may provide one of its own volition.

A security assessment may entail extensive investigation or may be limited to checking intelligence holdings. Once a security assessment is complete, ASIO will issue one of three forms of advice:

- a non-prejudicial assessment—ASIO does not have security concerns about the proposed action
- a qualified security assessment—ASIO has information, an opinion or advice that is or could be prejudicial to the interests of the person
- an adverse security assessment—ASIO recommends that a particular action be taken or not taken, which would be prejudicial to the interests of the person, such as the refusal of a visa or cancellation of a passport.

Appeal mechanisms for security assessments

For most categories of security assessments, where ASIO provides a government agency with an adverse or qualified security assessment on an individual, the agency concerned is generally required to notify the subject within 14 days. Merits review of certain assessments (excluding most relating to migration) is available in the Security Appeals Division of the Administrative Appeals Tribunal (AAT). The AAT 'stands in the shoes of the decision-maker,' reviews the material that was before the decision-maker and may inform itself on any matter in such manner as it considers appropriate.

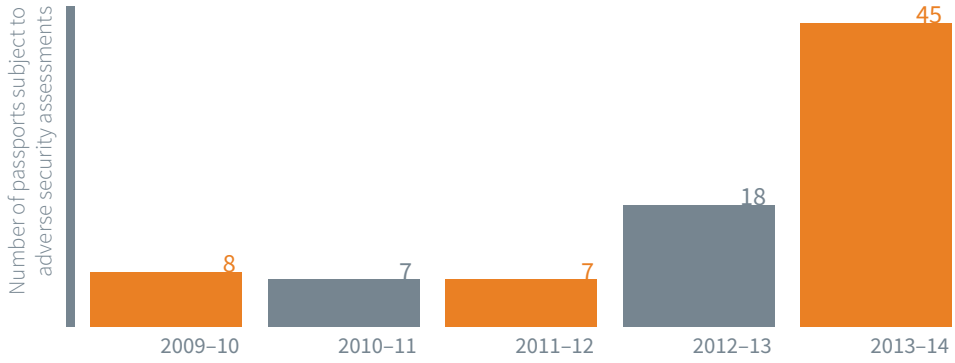
Judicial review of ASIO's administrative decision-making processes—as with all decisions of the executive arm of government—is possible for all security assessments, through the Federal Court and the High Court of Australia.

Passports

ASIO, in cooperation with local and overseas partners, uses a variety of measures to disrupt the travel of individuals likely to engage in activities prejudicial to national security, or where such travel has already occurred, takes measures to mitigate the threat.

Pursuant to the *Australian Passports Act 2005* and the *Australian Passports Determination Act 2005*, ASIO can recommend to the Minister for Foreign Affairs that an individual's passport be cancelled or refused if the individual is likely to engage in activities prejudicial to security and the cancellation or refusal might prevent the activities. Such security assessments consider only factors related to security, as defined in the ASIO Act. The cancellation of a passport does not affect an Australian citizen's right of return to Australia. DFAT can issue temporary documents to facilitate the return of a person whose passport has been cancelled overseas.

Figure 2: Number of passports subject to adverse security assessments by financial year



Performance 2013–14

During the reporting period, ASIO issued adverse security assessments in respect of 45 passports, in respect to individuals located both in Australia and offshore. The overwhelming majority of these assessments related to the Syrian conflict.

Citizenship

ASIO may issue security assessments in relation to Australian citizenship under the *Australian Citizenship Act 2007*. In 2013–14, ASIO did not issue any adverse assessments in relation to citizenship applications.

Visa security assessments

ASIO adopts an intelligence-led, risk-managed approach to identifying persons travelling to Australia who may pose a threat to national security. ASIO may furnish a visa security assessment to DIBP of its own volition or following a referral by DIBP of a visa application.

Where ASIO assesses that an individual is directly or indirectly a threat to security as defined in the ASIO Act, ASIO may issue an adverse visa security assessment, which may result in the refusal of a visa application or cancellation of an existing visa.

ASIO works closely with other border agencies, particularly DIBP, on visa security assessment issues. ASIO's cooperation with DIBP includes a flexible approach to meeting DIBP's prioritisation of visa caseloads, and contributions to relevant training.

Performance 2013–14

The reduction in the number of visa security assessments for illegal maritime arrivals reflects a reduction in the number of such cases referred by DIBP.

Table 1: Total numbers of immigration-related assessments conducted by ASIO over the last two years

Type of entry	Number of assessments completed 2012–13	Number of assessments completed 2013–14[1]
Temporary visas	18 748	17 516
Permanent residence and citizenship	3681	6120
Onshore protection (air)	257	326
Offshore refugee / humanitarian	3369	2310
Illegal maritime arrivals	3394	877
TOTAL	**29 449**	**27 149**

[1] Excludes assessments undertaken to resolve potential matches to national security border alerts

In 2013–14, ASIO undertook a large-scale data remediation project with DIBP which enhanced the quality of data used for national security alerts. ASIO conducted tailored training for ASIO and DIBP staff, and engaged more closely with foreign partners on visa security assessment issues to improve the efficiency of visa security assessment processes.

ASIO worked with the Australian Customs and Border Protection Service in preparation for ASIO's participation in the multi-agency National Border Targeting Centre (NBTC), which commences operation from 1 July 2014. ASIO's involvement in the NBTC is part of a broader national security contribution to intelligence-led border security, which will include enhancing the identification of high-risk border movements.

Counter-terrorism security assessments

ASIO provides counter-terrorism security assessments for applicants seeking access to sensitive air or maritime port areas, or security-sensitive chemical, biological and nuclear sites, and for special events.

Individuals requiring access to sensitive air and maritime port areas must undergo appropriate background checking—including security checking—before being granted Aviation Security Identification Cards (ASICs) and Maritime Security Identification Cards (MSICs), which permit such access.

ASIO's role in the ASIC and MSIC process is to consider whether the applicant poses a threat to national security should they have access to sensitive areas. AusCheck, located within the Attorney-General's Department, coordinates the larger suite of background checks, including criminal history checks, and assesses an applicant's overall suitability to hold an ASIC or MSIC.

ASIO provides, via the Australian Federal Police (AFP), counter-terrorism security assessment advice as part of the licensing process by Australian states and territories for access to security-sensitive ammonium nitrates (SSANs), which are used as an explosive, particularly by the mining industry and as a fertiliser in agriculture. Each state and territory has its own licensing regime, consistent with a set of principles agreed in 2005 by the Council of Australian Governments.

Similar ASIO checks are provided to the Department of Health for individuals requiring access to security-sensitive biological agents (SSBA) as part of the SSBA Regulatory Scheme flowing from the *National Health Security Act 2007*. ASIO may recommend against a licence for access to SSANs or SSBAs.

ASIO also provides, via the AFP, security assessment advice regarding the access of individuals to the Australian Nuclear Science and Technology Organisation nuclear facility at Lucas Heights, New South Wales.

ASIO security assessment advice is also provided to Commonwealth and state government agencies for some special-event accreditation, such as the G20 meetings in Australia in 2014.

Table 2: Number and type of national security clearance assessments completed by financial year

Type of access	2012–13	2013–14
Positive Vetting	1789	1367
Negative Vetting Level 2	6625	6668
Negative Vetting Level 1	19 168	15 482
Other	4	5
Total	**27 586**	**23 522**

Performance 2013–14

In 2013–14 ASIO completed 159 288 counter-terrorism security assessments. No adverse or qualified assessments were issued during the year.

Personnel security assessments

ASIO is the issuing authority for personnel security clearances of its own staff, and for clearances sponsored by ASIO. In all other cases, a department or agency must request security assessment advice from ASIO as part of its overall consideration of whether or not to grant a national security clearance.

Ensuring that access to national security-classified, sensitive and privileged information is provided to individuals suitable to hold a security clearance is a critical element in protecting the integrity of government business.

Border integrity investigations and analysis

ASIO has continued to support whole-of-government strategies to disrupt and deter people smugglers. ASIO also contributes to Australia's border security through border-related threat assessments and intelligence reporting, and visa security assessments. Foreign nationals arriving in Australia, whether through regular or irregular channels, are subject to national security checking.

Performance 2013–14

During the reporting period, ASIO identified and investigated serious threats to Australia's territorial and border integrity and provided advice to government on these threats. ASIO also provided advice in the form of security assessments to DIBP on significant emerging threat issues, including terrorism- and espionage-related threats.

ASIO participated in inter-departmental committees and working groups on border integrity and provided additional staffing support for Operation Sovereign Borders. It also provided reporting on reactions to changes in Australia's people-smuggling policies and supported legal measures, such as passport cancellation, to disrupt the activities of Australians involved in people-smuggling activities.

In addition, ASIO provided information and briefings to support the work of the Australian Government Independent Reviewer of Adverse Security Assessments, former Federal Court judge the Hon. Margaret Stone.

Support to security intelligence–related prosecutions and litigation

The Office of Legal Counsel manages ASIO involvement in legal proceedings in courts, tribunals and other forums, including in terrorism and other prosecutions, civil lawsuits, and administrative matters such as merits review of security assessments.

In doing so, the Office of Legal Counsel works closely with operational areas, external stakeholders and legal representatives to balance the protection of ASIO investigations, capabilities, methodologies, officer and source identities, and foreign liaison relationships with court requirements and the principles of open justice.

In 2013–14, ASIO was involved in over 50 litigation matters, including terrorism and other criminal prosecutions, civil matters in which ASIO material was sought as evidence, and judicial and administrative review of ASIO security assessments. The increase since 2005 in the relative and absolute volume of security assessment litigation—particularly relating to illegal maritime arrivals—and complex matters involving multiple Commonwealth agencies in the Federal and High Courts of Australia, as well as the AAT, required significant legal resources. ASIO was also involved in Australia's response to a complaint brought by Timor-Leste in the International Court of Justice.

ASIO's focus remained the protection of sensitive national security information while facilitating its contribution and disclosure as required in prosecutions and administrative and judicial review of ASIO and other agencies' decisions.

Performance 2013–14

Various criminal prosecutions, administrative reviews and other litigation matters in which ASIO was involved remain before courts or tribunals as at the end of 2013–14. In the review period a number of appeals against or concerning ASIO's security assessments were resolved by the AAT or the Federal Court.

PASSPORT CANCELLATION CASE

In 2010, ASIO had reasonable grounds to suspect that a person was likely to engage in conduct which might prejudice the security of a foreign country, and judged that his passport should be cancelled to prevent him from doing so. The subject challenged ASIO's adverse security assessment and the decision by the then Minister for Foreign Affairs to cancel his passport. On 19 November 2013, the Administrative Appeals Tribunal (AAT) affirmed these decisions. The tribunal acknowledged that ASIO's task of anticipating and helping prevent future dangers necessarily involves speculation, 'understood in a neutral, not pejorative sense. Certainty will rarely, if ever, be attainable. All that is required is that any prediction of future events contained in an adverse assessment must be well informed; the reasoning supporting the prediction must be rational and inferences must be based on sound foundations'. The tribunal also described the ASIO witness as 'credible, thorough and fair' and noted he 'not only advanced, persuasively, ASIO's case but also properly and frankly drew the attention of the tribunal to certain materials and considerations that he accepted should be balanced against the assessment ASIO had made'.

DELIVERABLE 2

Protective security advice

ASIO provides protective security advice for government and industry to enhance physical, technical, procedural, personnel and information security.

This deliverable includes:

- protective security risk reviews and vulnerability assessments
- physical security certifications
- technical surveillance countermeasures
- security services and equipment evaluation
- protective security training.

Overview

ASIO's protective security advice unit, T4, provides advice to the Australian Government, state and territory governments and Australian businesses.

The main focus of T4 protective security advice relates to protection against threats to 'national security' as set out in section 4 of the ASIO Act. However, ASIO's protective security advice function in section 17(1)(d) of the ASIO Act is not limited to that narrow definition of security and can include advice relating to protective security as more broadly understood.

Owners and operators of national critical infrastructure, both government and privately owned, are key clients of T4. State and territory governments are also important clients but, under the ASIO Act, T4 must obtain approval from the Attorney-General before providing advice to them.

Protective security risk reviews and vulnerability assessments

Key elements of T4's work are the provision of vulnerability assessments and protective security risk reviews (PSRRs) and the delivery of security design evaluations.

Vulnerability assessments identify weaknesses in protective security arrangements and provide practical recommendations for clients to address the identified vulnerabilities.

PSRRs assess physical, information, administrative and personnel security risks. A PSRR typically involves extensive consultation with clients, needs analysis, critical asset identification, identification of threats, vulnerability assessment, risk analysis, risk treatment recommendations and security equipment considerations. PSRRs are issued as formal reports providing practical recommendations for risk management and mitigation.

Security design evaluations aim to assist clients at any point in the design phase of a project; they provide a third-party assurance that the project will satisfy the client's requirements.

Physical security certifications

The Australian Government Protective Security Policy Framework (PSPF) requires all Zone 5 facilities (facilities that hold information classified as Top Secret) within Australia to be certified by T4. On behalf of Defence Intelligence Security, T4 also certifies the physical security of sensitive compartmented information facilities (SCIFs). The policy framework requires all Zone 5 facilities and SCIFs to be recertified every five years.

Technical surveillance countermeasures

T4 delivers technical surveillance countermeasures (TSCM) services to Australian Government organisations. This work provides a level of assurance that highly classified or sensitive discussions and information are not subject to compromise through technical attack—for example, by monitoring to detect unauthorised covert listening devices during conferences, or unauthorised access to, or compromise of, information through technical means. Inspections include electronic surveys, the monitoring of premises for possible covert electronic activity, and physical security inspections. While ASIO does not comment publicly on the details of this sensitive work program, the demand for specialised TSCM services remained high in 2013–14.

Security services and equipment evaluation

T4 conducts a security equipment evaluation program on behalf of the Australian Government's Security Construction and Equipment Committee (SCEC). It also evaluates and endorses security services such as couriers (for the transportation of classified material), locksmiths (for the maintenance and repair of government locks and security containers), data destruction facilities, and security consultants (who are endorsed to provide physical security advice across government more broadly).

The security equipment program evaluates security products such as locks, alarms and security containers to determine whether they are fit for purpose and appropriate for use by government. Products assessed as being fit for purpose are listed in the Security Equipment Evaluated Product List. A new version of this list will be published by T4 in late 2014.

Protective security training

T4 conducts a number of practical training courses for Australian Government agencies and their staff. It also regularly delivers training, through the Attorney-General's Protective Security Training College, to enable commercial security consultants and locksmiths to meet the requirements of SCEC programs.

Through the quarterly Security Practitioners Course, T4 also provides training for agency security advisers, defence security officers and security managers throughout the Australian Government in the practical application of protective security measures.

For further information on T4 visit www.asio.gov.au.

For further information on SCEC visit www.scec.gov.au.

Performance 2013–14

In 2013–14 T4 met its objective of providing protective security advice to its clients by delivering the following outputs:

Advice	Performance 2013–14
Protective security risk reviews and vulnerability assessments	▸ 6 protective security risk reviews ▸ 6 design evaluations ▸ 6 vulnerability assessments
Physical security certifications	▸ 25 Zone 5 site certifications ▸ 6 Zone 5 provisional certifications ▸ 73 physical security inspections ▸ 11 destruction companies approvals—includes 14 reports during the reporting period
Technical surveillance countermeasures	▸ While ASIO does not comment publicly on the details of this sensitive work program, the demand for specialised TSCM services remained high in 2013–14.
Security services and equipment evaluation	▸ 15 security equipment evaluations ▸ Site certification for 2 shared internet gateway facilities used by Australian Government agencies ▸ 1 SCEC-endorsed courier report ▸ 1 locksmith bulletin ▸ 5 protective security circulars ▸ 3 security equipment guides
Protective security training	▸ 8 protective security training courses

DELIVERABLE 3

Security intelligence investigations and capabilities

Security intelligence investigations and capabilities support national intelligence priorities through complex tactical operations, all-source security intelligence collection, analysis, and engagement with national and international partners.
This deliverable includes:

- counter-terrorism investigations and analysis;
- counter-espionage and foreign interference investigations and analysis;
- engagement with national partners;
- international advice; and
- contribution to policy development.

Counter-terrorism investigations and analysis

ASIO's security intelligence functions are anticipatory in nature. ASIO's role is to identify and assess possible threats to national security or to the lives and safety of Australians in sufficient time and accuracy to prevent such threats eventuating. ASIO's work is predictive and advisory, informing risk management and enabling government to take preventative actions.

ASIO's Counter-Terrorism Division undertakes security intelligence investigations and operations to identify, monitor and understand threats of terrorism and other politically motivated violence to Australia and Australians, whether that threat originates here or overseas. These activities enable ASIO to assess individuals, groups and entities engaging in acts relevant to politically motivated violence and to advise government on potential mitigating action.

ASIO's investigative horizon is necessarily long term; however, changes to the security environment during 2013–14, both in Australia and globally, were reflected in the focus and tempo of counter-terrorism investigations, a situation likely to persist.

Performance 2013–14

Counter-terrorism investigations grew in volume and complexity during 2013–14 as extremist activities overseas—such as those in Syria and Iraq—increasingly converged with activities in Australia. ASIO remained adaptive. It appropriately prioritised investigative resources and partnered with Australian and international law enforcement and intelligence agencies to detect terrorist planning, assess associated threats and provide advice to government.

Further detail on ASIO's performance relating to counter-terrorism operations and capabilities is provided in the classified Part 3 section of the annual report. Part 1 provides an overview of our current assessment of the threat from terrorism.

Counter-espionage and foreign interference investigations and analysis

ASIO has significantly bolstered its understanding of the scale, nature and threat posed to Australia's interests by espionage and foreign interference in recent years. This has led to an increased output of security intelligence advice to government and the private sector, and an enhanced role in associated policy development and implementation.

A challenge is the scale, diversity and complexity of the sources, methods, targets and objectives involved in the espionage and foreign interference threat that Australia faces. ASIO's objectives are to discover sources of threat and to build resilient defences—spanning the spectrum of personnel, technical and information and communications technology security policies—rather than be limited to providing an investigative response after harmful activity has occurred. ASIO's work relies on strong and collaborative partnerships.

Part 1 provides an overview of our current assessment of the threat from espionage and foreign interference.

Contact Reporting Scheme

The Contact Reporting Scheme is a whole-of-government counter-espionage strategy managed by ASIO. Information obtained through the scheme can:

- provide vital indicators of clandestine or deceptive activity, including attempts to cultivate or recruit Australian Government employees
- assist ASIO to identify espionage and hostile foreign intelligence activity directed against Australia
- inform ASIO's mitigation advice to the Australian Government.

All government employees are obliged to report contact with foreign nationals that appears to be suspicious, ongoing, unusual or persistent in any respect. This contact could be official or social and could occur either in or outside Australia.

Engagement with national partners

The Australian Government's counter-terrorism strategy is characterised by strong intelligence-led collaboration between Australian Government, state and territory agencies, and international counterparts. Australian Government agencies also have productive relationships with partners in the private sector and broader community. ASIO contributes to Australia's security through a number of multi-agency initiatives, including leadership of the Counter Terrorism Control Centre (CTCC), participation in the Australian and New Zealand Counter-Terrorism Committee and participation in the National Counter-Terrorism Exercise Program.

Counter Terrorism Control Centre

The CTCC, hosted by ASIO, is the multi-agency body responsible for coordinating Australia's counter-terrorism intelligence mission. The CTCC sets and communicates Australia's strategic counter-terrorism intelligence priorities and evaluates the performance of Australia's counter-terrorism community against those priorities. The CTCC also fosters inter-agency collaboration and the dissemination of relevant information, chairing regular roundtables and working groups. These programs ensure the Australian Government's counter-terrorism intelligence efforts are coordinated and effective.

During 2013–14, the CTCC improved its evaluation methodology, better reflecting the various roles and capabilities across the counter-terrorism community. This process—with its emphasis on thorough, qualitative feedback—provided the CTCC with greater detail on which to base its judgements and enabled it to provide government with a clearer appreciation of the counter-terrorism issues impacting on Australia.

Although its priority-setting and evaluation functions are managed independently, the CTCC has adopted processes consistent with those developed by the Australian Government's National Intelligence Collection Management Committee (NICMC). The CTCC reports to the government annually via NICMC, and tabled its classified *Counter terrorism intelligence planning document* and *Annual evaluation report* in April 2013.

Australian and New Zealand Counter-Terrorism Committee

ASIO is a committed member of the Australian and New Zealand Counter-Terrorism Committee (ANZCTC), contributing to the development of nationwide counter-terrorism capability. ASIO provides security intelligence advice to the committee, through membership of a number of subcommittees, individual capability forums and the National Counter-Terrorism Exercise Program. This ensures there is a common understanding of the threat environment and helps ANZCTC initiatives remain targeted and efficient.

National counter-terrorism exercises

During 2013–14 ASIO continued its participation in the National Counter-Terrorism Exercise Program. The program successfully conducted a range of exercises to ensure that Australia is well placed to protect the community from acts of terrorism and to respond in an efficient and coordinated manner to terrorist threats. The continuous testing, validation and improvement of Australia's counter-terrorism capability is fundamental to effective prevention, mitigation and incident response. ASIO is a lead member of the Exercise Writing Committee, which develops exercises focused on Australia's coordinated response to counter-terrorism-related incidents, multi-jurisdiction investigation arrangements and intelligence support to operational decision-making.

The exercise program enables multi-agency, cross-sector engagement to:

- test current plans and arrangements to identify capability gaps
- validate and confirm levels of capability achievement
- validate training and inform training requirements
- develop and maintain interoperability across agencies and sectors
- inform the review and development of security legislation, policy, plans, arrangements and processes
- maintain consistency in the application of Australia's counter-terrorism arrangements.

Performance 2013–14

The CTCC published updated editions of its *Counter-terrorism intelligence planning document* and *Annual evaluation report*. These documents provide guidance to help agencies address Australia's counter-terrorism priorities more effectively, and inform government of the performance of agencies in fulfilling Australia's counter-terrorism mission.

ASIO co-wrote, directed and participated in a number of national counter-terrorism exercises. The G20 series of exercises conducted during the reporting period identified and explored gaps in current planning and training in the lead-up to the G20 Leaders Summit, enabling improvement in communication and incident response practices.

International engagement

Responding effectively to the transnational nature of security and intelligence threats demands international cooperation between security and intelligence agencies. To maximise its effectiveness, ASIO engages with, and receives support from, a number of international partners.

Effective liaison relationships with international partners have proved to be vital in protecting Australia from the threat posed by foreign fighters returning from current conflicts in the Middle East.

International liaison relationships enable ASIO to draw on the expertise and capability of overseas partners, enhancing ASIO's ability to pursue intelligence investigations.

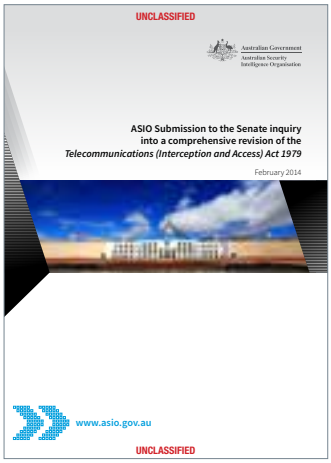
Contribution to policy development

ASIO makes a sustained contribution to policy development through the Australian Government and domestic partners.

In 2013–14, ASIO worked with the Attorney-General's Department and other stakeholders in the development of a broad suite of policy, resourcing and legislative measures to respond to the increasing threat posed to Australians by Islamist terrorism, both domestically and internationally. ASIO assessments informed policy makers of the implications of the conflicts in Syria and Iraq for Australia's security, including the consequences arising from the involvement of Australian citizens in those conflicts and their impact on radicalisation within Australia.

The Organisation worked closely with policy agencies to develop specific measures to improve the ability of Australian Government agencies to prevent or disrupt Australians seeking to provide support to terrorist groups engaged in the Syria and Iraq conflicts and to manage the threat posed by individuals returning to Australia after participating in the conflicts.

ASIO supported policy agencies in the development of the National Security Legislation Amendment Bill (No. 1) 2014, which was introduced on 16 July 2014 and implements the government's response to recommendations made by the PJCIS in Chapter 4 of its *Report of the inquiry into potential reforms of Australia's national security legislation* (tabled in June 2013). The Bill seeks to modernise and improve the Australian Intelligence Community legislative framework, primarily through amendments to the ASIO Act and the *Intelligence Services Act 2001*.



ASIO also contributed to the Senate inquiry into the comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). ASIO made an unclassified submission to the inquiry, highlighting the importance of telecommunications interception and data to ASIO's activities and the growing challenges of maintaining lawful access. The Director-General of Security attended a public hearing on 21 July 2014 to supplement this submission. ASIO also provided a private briefing with the Senate inquiry committee.

ASIO has significantly increased engagement with the broader Australian Government—at both executive levels and with agency security advisors—to raise awareness of the malicious insider threat. Malicious insiders are trusted employees and contractors who deliberately and wilfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.

Of note, ASIO has used its investigative and personnel security assessment experience, and that of its allied partners, to inform the development and implementation of robust policy and procedures to strengthen the Australian Government's defence against the malicious insider threat. The Organisation has worked closely with key agencies, including the Attorney-General's Department, the Department of the Prime Minister and Cabinet and the Department of Defence, on personnel security policy reforms and other associated policy initiatives. ASIO's focus has been to simultaneously address:

- access—the suitability of ASIO's clearance holders and the need for comprehensive and robust vetting, revalidation and clearance maintenance processes
- accessibility—ensuring ASIO's systems and processes appropriately restrict access to information to a 'need to know' while not inhibiting secure and effective government business processes.

This work will be the focus of continued effort over the next reporting period, but it has already resulted in significant improvements in personnel security outcomes and an increased awareness of the potential threat to the security and integrity of government business.

DELIVERABLE 4

Foreign intelligence collection in Australia

ASIO has the statutory authority under section 17(1)(e) of the ASIO Act to collect foreign intelligence in Australia on matters relating to Australia's national security, Australia's foreign relations or Australia's national economic wellbeing. ASIO exercises its foreign collection powers under warrant at the request of the Minister for Defence or the Minister for Foreign Affairs.

Overview

At the request of the Minister for Foreign Affairs or the Minister for Defence, ASIO has used its special collection powers to undertake foreign intelligence collection within Australia.

ASIO exercises its foreign intelligence collection powers where authorised by the Attorney-General, in relation to matters that are in the interests of Australia's national security, Australia's foreign relations or Australia's national economic wellbeing. ASIO undertakes this activity in close cooperation with its foreign intelligence collection partners: the Australian Secret Intelligence Service and Australian Signals Directorate.

Performance 2013–14

ASIO's performance in relation to this intelligence collection activity is measured by stakeholders in terms of ASIO meeting the intelligence requirements of the sponsoring agency, and also the National Intelligence Priorities set by the National Security Committee of Cabinet.

For reasons of national security, ASIO's outcomes in relation to its foreign intelligence collection operations are reported in the classified Part 3 of the annual report.

Part 3

OUTCOMES AND HIGHLIGHTS

'There is a persistent threat of terrorist violence in Australia, associated with a range of extremist and distorted political, religious and racist ideologies. We also continue to face quite sophisticated attempts to gain access to our most precious government and business secrets via espionage, including by cyber means.'

David Irvine, Director-General of Security
The Crescent Institute, 11 February 2014

PART 3 EXCLUSION

The Attorney-General has approved the exclusion of Part 3, under Section 94(4) of the ASIO Act, in its entirety from the unclassified *ASIO Report to Parliament* after obtaining advice from the Director-General of Security that this is necessary in order to avoid prejudice to security.

Part 4

ASIO AND ACCOUNTABILITY

'Today's intelligence community, its conceptual philosophy, its scope, its essential structure, its balance of human rights and state power, its operating procedures and its accountability and oversight mechanisms derive in large part from the extraordinarily insightful work of Justice Hope and his team.'

David Irvine, Director-General of Security
2013 Sir Zelman Cowen Oration, Australian Institute of Public Affairs, 1 October 2013

Attorney-General

ASIO's ministerial accountability is to the Attorney-General. Senator the Hon. George Brandis QC is Australia's Attorney-General, sworn into office following the federal election on 7 September 2013. Prior to the election, the Hon. Mark Dreyfus QC MP held the office of Attorney-General.

Functional responsibility

ASIO's security intelligence activity is conducted in accordance with the Attorney-General's Guidelines—last updated by the Attorney-General on 10 December 2007—under sections 8A(1) and 8A(2) of the ASIO Act.

The guidelines stipulate that ASIO's activities must be conducted in a lawful, timely and efficient manner, applying the principal of proportionality to ensure the least intrusion necessary into an individual's privacy.

The Attorney-General issues all ASIO warrants, other than questioning warrants and questioning and detention warrants that are issued and approved as specified under Part III, Division 3 of the ASIO Act. If ASIO judges that a warrant is required, the Director-General of Security will present a warrant request to the Attorney-General. The Attorney-General will consider the request and, if in agreement, will authorise the warrant. For every warrant authorised, ASIO must report to the Attorney-General on the extent to which it assisted the Organisation in carrying out its functions.

The Attorney-General, Senator the Hon. George Brandis QC and Deputy Director-General Kerri Hartland

ASIO also keeps the Attorney-General informed of significant national security developments, as well as other important issues affecting ASIO. During the reporting period, ASIO provided advice to the Attorney-General on a range of investigative, operational and administrative issues, primarily communicated through Attorney-General ministerial submissions. In 2013–14 ASIO submitted over 300 ministerial submissions.

Parliamentary oversight

ASIO has been subject to parliamentary joint committee oversight since 1986. In 2013–14 that oversight was performed by the PJCIS, Senate Estimates hearings and several parliamentary inquiries relating to national security.

Parliamentary Joint Committee on Intelligence and Security

The PJCIS is a bipartisan statutory committee established under section 28 of the *Intelligence Services Act 2001*. More information on the role of the committee and its previous inquiries is available on the Parliament of Australia website at www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security.

The primary ongoing responsibility of the PJCIS is to review annually the administration and expenditure of Australia's intelligence agencies, including their annual financial statements. These reviews provide assurance to the parliament and the public that the administration and expenditure of Australian intelligence agencies are conducted appropriately. The committee has access to national security-classified material provided by the agencies to inform its public report.

Additional functions of the PJCIS include:

- reviewing any matter in relation to Australia's intelligence agencies referred to it by the responsible minister or a resolution of either House of the Parliament of Australia
- reviewing a regulation which lists an entity as a terrorist organisation
- reporting comments and recommendations to each House of the Parliament of Australia and to the responsible minister.

Due to changes to the PJCIS membership during the reporting period, ASIO hosted a classified briefing session with members of the committee in March 2014 to inform their understanding of ASIO's role in protecting Australia, including the current terrorism and espionage challenges in the security environment and ASIO's technical capabilities.

Review of administration and expenditure

During the reporting period, the PJCIS initiated its review of the administration and expenditure of Australian intelligence agencies for the period 2012–13. ASIO provided the committee with a classified submission and an unclassified submission; the latter is available from the committee's website. The submissions provide information on the security environment, as well as ASIO's expenditure, organisational structure, corporate direction and strategic planning, human resource management, accommodation, legislation, approach to security, relationships and accountability. On 27 March 2014, ASIO attended a private hearing before the committee to inform its inquiry. This hearing covered both the 2011–12 and the 2012–13 reporting periods and will assist the committee to provide reports to parliament for both periods.

Review of national security legislation

On 24 June 2013 the committee tabled its findings from its review of national security legislation. During the reporting period, ASIO worked with the Attorney-General's Department to inform the Australian Government's response to the committee's report. Outside the reporting period, on 16 July 2014, the Attorney-General introduced the *National Security Legislation Amendment Bill (No.1) 2014* in the Senate to respond to the Committee's recommendations in Chapter 4 of the report.

Senate Standing Committee on Legal and Constitutional affairs

Senate Estimates

Senate Estimates hearings provide an opportunity for senators to publicly scrutinise the operation and expenditure of Australian Government departments and agencies. ASIO first appeared at Senate Estimates in August 1993, and the Organisation continues to welcome the opportunity to engage in public with the Parliament of Australia on all aspects of ASIO's work, consistent with the requirements of national security.

As part of the Attorney-General's portfolio, ASIO appears before the Legal and Constitutional Affairs Committee. In 2013–14, the Director-General of Security and the Deputy Director-General, Kerri Hartland, appeared before the committee on three occasions: Supplementary Budget Estimates, on 18 November 2013; Additional Estimates, on 24 February 2014; and Budget Estimates, on 29 May 2014.

During these appearances, ASIO responded to questions on topics such as ASIO's budget, security assessments, the Ben Chifley Building, the execution of ASIO search warrants, and proposed changes to the *Telecommunications (Interception and Access) Act 1979*. Transcripts of ASIO's evidence at these hearings are available on the committee's website, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs.

Migration Amendment Bill 2013 inquiry

On 12 December 2013, the Senate referred the Migration Amendment Bill 2013 to the Legal and Constitutional Affairs Legislation Committee for inquiry and report.

On 4 February 2014, the Director-General of Security provided evidence at a confidential hearing of the inquiry. The Director-General of Security addressed questions from committee members relating to ASIO's security assessments for protection visa applicants, caseload numbers, internal reviews of security assessments, and the Independent Reviewer of Adverse Security Assessments, former Federal Court judge the Hon. Margaret Stone. Further detail can be found in the transcript of the hearing, available online from the committee's website.

The committee tabled its report on 12 February 2014, recommending the Bill be passed and the government consider putting in place a regulatory framework to underpin the powers, authority and role of the Independent Reviewer of Adverse Security Assessments. The Bill was passed by parliament, and the *Migration Amendment Act 2014* came into effect on 2 June 2014. This Act:

- amends the *Migration Act 1958* so that a protection visa can be issued only where the applicant is not the subject of an adverse security assessment
- confirms that an individual who has had their visa application refused due to an adverse security assessment is unable to appeal to the Refugee Review Tribunal, the Migration Review Tribunal or the Administrative Appeals Tribunal (AAT)
- does not affect a visa applicant's right to seek judicial review of an adverse security assessment under the original jurisdiction of the High Court of Australia
- does not remove the discretionary power of the Minister for Immigration and Border Protection to issue a visa to any person in immigration detention, regardless of whether ASIO has issued an adverse security assessment.

Senate inquiry into the *Telecommunications (Interception and Access) Act 1979*

In December 2013, the Senate referred a comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to the Legal and Constitutional Affairs References Committee.

The inquiry is focusing on previous recommendations relating to the TIA Act made by the Australian Law Reform Commission in its 2008 review of Australian privacy law and practice; and those made by the PJCIS in its *Report of the inquiry into potential reforms of Australia's national security legislation*.

During the reporting period, ASIO made an unclassified submission to the inquiry, highlighting the importance of telecommunications interception and data to ASIO's activities and the growing challenges ASIO faces in maintaining access to this information. ASIO's submission is available online from the committee's website.

Subsequent to the reporting period, the Director-General of Security attended a public hearing on 21 July 2014 to supplement this submission. ASIO also hosted committee members for a private briefing. The inquiry was ongoing at the end of the reporting period.

Independent oversight

Inspector-General of Intelligence and Security

The Office of the Inspector-General of Intelligence and Security (IGIS) was established under the *Inspector-General of Intelligence and Security Act 1986* and sits within the Prime Minister's portfolio.

The current IGIS, Dr Vivienne Thom, was appointed in 2010. The IGIS is an independent statutory office holder responsible for reviewing the activities of the Australian Intelligence Community to provide assurance that agencies operate with propriety, according to law, consistent with ministerial guidelines and directives and with due regard for human rights.

The powers of the IGIS are wide-ranging and similar to those of a royal commission; they include access to ASIO records and premises at any time. The IGIS conducts regular inspections and monitors ASIO's activities on an ongoing basis. ASIO does not wait for an inspection of a case to bring issues or errors to the attention of the IGIS but proactively provides that advice.

ASIO also ensures that the staff of the Office of the IGIS have the access they need, and it provides the office with briefings about particular aspects of ASIO's work and systems.

Outcomes of IGIS inquiries

During the reporting period, two full IGIS inquiries examined ASIO's role and functions, one stemming from a complaint to the IGIS about ASIO, and the other from a ministerial referral relating to an illegal maritime arrival.

Inquiry into attendance of lawyers at ASIO interviews

In May 2013 the IGIS initiated an inquiry into the attendance of legal representatives at ASIO interviews. The inquiry originated in a complaint, lodged by the Refugee Advisory and Casework Service, alleging inconsistent and arbitrary practices by ASIO in relation to the attendance of legal representatives at security assessment interviews.

The IGIS completed her inquiry during the reporting period, and the public version of the report can be found on the IGIS website www.igis.gov.au. In her report, the IGIS stated that ASIO's internal policies were sound and appropriate and that ASIO officers conducted themselves in a professional manner during the interviews. However, the IGIS made five recommendations that would serve to refresh and reinforce ASIO's policies and procedures. Of the five recommendations in the report (see Table 3), ASIO agreed in full to Recommendations 1 to 4 and agreed in part to Recommendation 5. ASIO has fully implemented all recommendations to which it agreed.

Table 3: IGIS recommendations resulting from the inquiry into the attendance of lawyers at ASIO interviews

Recommendation	
1	ASIO should work with the Department of Immigration and Border Protection (DIBP) to ensure that: ▸ when making interview arrangements in Australia, visa applicants are specifically asked whether they want to have a legal representative attend ▸ the lawyer's personal details are obtained by Immigration and passed to ASIO ▸ a decision is made about whether the lawyer may attend and is conveyed prior to the day of interview.
2	ASIO should: ▸ review its training to reinforce that the attendance of a lawyer at a security assessment interview is not to be considered problematic, unless sound reasons exist for deciding otherwise ▸ ensure that decisions about whether a lawyer may attend an interview are considered and recorded on a case-by-case basis ▸ ensure that, in the absence of a specific cause for concern, interviews should commence without efforts by interviewing officers to discourage the attendance of a legal representative.
3	ASIO should: ▸ clarify the status of any person who wants to attend an interview to ascertain whether they are the interviewee's legal representative ▸ further consider whether migration agents should be accorded the same status as lawyers, with their attendance at interviews being addressed on a case-by-case basis.
4	ASIO should: ▸ provide guidance for interviewing officers on when a written or verbal confidentiality undertaking should be requested from a person ▸ provide the template undertaking document to attendees before the interview commences ▸ provide a copy of a written undertaking to the signatory.
5	The details of this recommendation are afforded a national security classification and cannot be included in this abridged report.

Table 4: IGIS recommendations relevant to ASIO resulting from the inquiry into Egyptian maritime arrival Mr E.

Recommendation	
1	Immigration and ASIO should continue to build on recent improvements in implementing a coordinated approach to resolving potential matches to national security alerts and document agreed procedures. This approach includes mechanisms to: ▸ escalate the priority of requests for information ▸ ensure that requests are followed up ▸ access all relevant existing information.
4	Immigration should review its procedures for conducting risk assessments in cases involving national security to ensure that those undertaking the assessment: ▸ have access to relevant information and expertise including from ASIO and the Australian Federal Police (AFP) ▸ have appropriate training and a standard process to follow; ▸ reference source information ▸ ensure that risk assessments become part of corporate records and are linked to the particular client's case.
6	Immigration and ASIO should ensure that in the small number of cases where there are potentially national security issues all relevant information is taken into account by Immigration when making immigration detention management decisions. Where such a case also involves issues of serious criminality Immigration should also work with the AFP to ensure relevant AFP information is also obtained and taken into account. This recommendation is not intended to suggest that responsibility for the decision in relation to the level of security for a person in immigration detention should rest with ASIO or the AFP; that decision is ultimately one for Immigration to make based on the best available information and advice.

Inquiry into Egyptian maritime arrival Mr E.

On 5 June 2013 the then Prime Minister, the Hon. Julia Gillard MP, requested that the IGIS conduct an inquiry into the management by Australian Government agencies of people seeking asylum who present complex security issues, with particular reference to an Egyptian illegal maritime arrival who was subject to an Interpol 'red notice'.

The IGIS completed her inquiry during the reporting period, and the public version of the report can be found on the IGIS website. The report noted that, prior to the case becoming a matter of public interest, ASIO had already initiated significant changes addressing a number of the issues raised during the inquiry.

Of the six recommendations made by the IGIS, three were relevant to ASIO: Recommendation 1, Recommendation 4 and Recommendation 6 (see Table 4). ASIO accepted the three recommendations in full. During the reporting period, ASIO worked with DIBP to implement the recommendations, with consequent changes to ASIO processes, training and guidance to staff.

Independent Reviewer of Adverse Security Assessments

The role of the Independent Reviewer of Adverse Security Assessments, currently former Federal Court judge the Hon. Margaret Stone, was established in December 2012. The Independent Reviewer conducts independent advisory reviews of ASIO adverse security assessments provided to the DIBP in relation to 'eligible persons'. An 'eligible person' is an individual who remains in immigration detention, having been found by DIBP:

- to be owed protection obligations under international law
- to be ineligible for a permanent protection visa, or who has had their permanent protection visa cancelled, because they are the subject of an adverse security assessment.

In performing her role, the Independent Reviewer has access to all materials relied on by ASIO to make its assessment, as well as any additional information obtained by ASIO since the assessment was made. The Independent Reviewer's full terms of reference are available online at www.ag.gov.au/asareview.

At the start of the reporting period, the Independant Reviewer had a caseload of 54[1]. Reviews ceased for three individuals during the reporting period as ASIO independently issued new non-prejudical or qualified assessments, reducing the caseload to 51. During the reporting period, the Independent Reviewer finalised 17 reviews. Of these:

- The Independent Reviewer found 15 adverse security assessments were appropriate, and these are now subject to periodic review. This includes one case where ASIO issued a new adverse security assessment taking into account new information referred by the Independent Reviewer. The Independent Reviewer found the new adverse security assessment to be an appropriate outcome.
- In one case, the Independent Reviewer found to be appropriate a new, qualified security assessment issued by ASIO as a result of new information referred by the Independent Reviewer in the last reporting period.
- In one case, the Independent Reviewer found ASIO's adverse security assessment was not appropriate and recommended ASIO issue a qualified assessment. After re-examining the case, ASIO issued a qualified security assessment.

Table 5: Summary of the Independent Reviewer's caseload since December 2012

	2012–13	2013–14	Total
New non-prejudicial or qualified security assessments issued by ASIO in relation to eligible persons separate to independent review process	1	3	4
Finalised preliminary reviews	5	17	22
Number of assessments where the Independent Reviewer formed the view that the assessment was an appropriate outcome	3	15	18
Number of assessments where the Independent Reviewer formed the view that the assessment was not an appropriate outcome	2 (resulted in non-prejudicial assessments)	1 (resulted in a qualified assessment)	3
Number of cases where ASIO issued a new non-prejudicial or qualified assessment after considering new information referred by the Independent Reviewer	0	1 (resulted in a qualified assessment)	1
Oral submissions heard	10	28	38
Periodic reviews initiated	N/A	2	2
Periodic reviews completed	N/A	0	0

[1] 5 of the 54 primary reviews were completed in 2012–13, see *ASIO 2012–13 Report to Parliament* for details.

In addition to the finalised cases, during the reporting period, the Independent Reviewer referred new information concerning three cases to ASIO, together with incomplete but advanced drafts of her reports. The drafts summarised all the information before her but did not include any recommendations. ASIO was still considering the new information in these three cases at the end of the reporting period. Under the terms of reference, the review process remains on hold until ASIO concludes its consideration of the new information.

In a further two cases, the Independent Reviewer submitted draft reports concluding that the original assessments were not an appropriate outcome. ASIO was still considering these cases at the end of the reporting period.

In addition to the primary reviews that were either finalised or referred to ASIO, the Independent Reviewer had prepared advanced drafts of a further 11 reports. A number of these reviews were finalised just after the end of the reporting period.

The Independent Reviewer's terms of reference require her to conduct a periodic review of adverse security assessments for eligible persons every 12 months. In June 2014, the Independent Reviewer commenced periodic reviews of two cases. These reviews were ongoing at the end of the reporting period.

Independent National Security Legislation Monitor

The Office of the Independent National Security Legislation Monitor (INSLM) was established by the *Independent National Security Legislation Monitor Act 2010*. The role of the INSLM is to assist ministers in ensuring Australia's counter-terrorism and national security legislation:

- is effective in deterring, preventing and responding to terrorism
- is consistent with Australia's international obligations
- contains appropriate safeguards to protect the rights of individuals.

Mr Bret Walker SC was appointed as the INSLM on 21 April 2011, and his term ended on 20 April 2014. At the time of writing, the government had yet to appoint a new INSLM.

During the reporting period the INSLM's third and fourth annual reports were tabled in parliament, on 12 December 2013 and 18 June 2014 respectively. The reports are available online from the website of the Department of the Prime Minister and Cabinet, www.dpmc.gov.au. The reports detail the outcomes of the INSLM's examinations of the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which is designed to:

- counter-terrorism financing and prevent Australians participating in offshore conflicts
- address issues in the existing legislation that may adversely affect the investigation and prosecution of terrorism offences or the identification and investigation of security threats.

During the reporting period ASIO provided submissions and evidence in private hearings to the INSLM on these matters, and the INSLM's reports made several recommendations relating to ASIO's activities:

- amending ASIO's questioning powers to include offences against the *Charter of the United Nations Act 1945*
- introducing the ability for an interim passport suspension to be approved by the Director-General of Security, including suspending the capacity to use a foreign passport
- introducing a legislative 'special intelligence operation' scheme where ASIO officers and human sources are protected from criminal and civil liability for certain conduct in the course of intelligence operations
- amending the *Intelligence Services Act 2001* to streamline intelligence cooperation between ASIO and the Australian Secret Intelligence Service (ASIS)—that is, not requiring a ministerial authorisation for requests to ASIS, Australian Signals Directorate and Australian Geospacial-Intelligence Organisation where it is at the request of the Director-General of Security and is for the purpose of assisting ASIO in the performance of its functions;
- introducing a power for the Minister for Immigration and Border Protection to revoke the citizenship of Australians on security grounds, where to do so would not render the individual stateless
- amending the name or alias of a proscribed terrorist organisation without having to conduct the proscription process from the beginning.

The PJCIS has separately considered several of these issues, and shortly after the reporting period the Australian Government introduced the National Security Legislation Amendment Bill (No. 1) 2014 into parliament to amend Australia's national security legislation.

Legal assurance and capability protection

ASIO's Office of Legal Counsel assists ASIO to manage its legal compliance and risk in carrying out its operational activities. In particular, the office provides advice on capability risks and on the scope of ASIO's powers and functions. In relation to ASIO's involvement in legal proceedings, the office works closely with operational areas, external stakeholders and legal representatives to balance the protection of ASIO investigations, capabilities, methodologies, officer and source identities, and foreign liaison relationships with court requirements and the principles of open justice.

The office assists ASIO in the proper use of its special powers warrants by providing advice on whether the information available satisfies the legislative requirements; assessing and processing warrant documentation; overseeing the ongoing management and timeliness of warrants; and helping in the provision of warrant revocation and reporting documentation to the Attorney-General.

During 2013–14, the office assisted ASIO across a range of operations, investigations and legal and administrative proceedings. This assistance included:

- providing legal advice and assistance to operational planning around the growing threat of radicalised individuals training in or returning from Syria
- providing legal and capability protection support to a number of significant counter-espionage investigations
- providing legal support to operational staff for planning and deployment ahead of the G20 meetings
- providing legal support to operational areas in the provision of security advice to inform Australian Government agency decision-making—this included the provision of legal advice to support security assessment interview preparation, legal evaluation of the intelligence case and preparation of decision records
- providing training to operational staff in relation to various matters, including security assessments, procedural fairness and use of legal powers under the ASIO Act
- reviewing and processing warrants and associated documentation
- managing ASIO's involvement in over 50 cases as a party or where ASIO's information was used in evidence
- providing advice on the effect on operations of prospective legislative change at both the Commonwealth and state level.

The office continued to provide a range of capability protection advice to support both the merits review process in the AAT and judicial review in the Federal and High Courts of Australia.

The office also continued its work in ensuring that legislation affecting ASIO adequately equips and assists it to fulfil its functions. This work included advocating for legislative amendment within a whole-of-government agenda and actively contributing to reviews such as those conducted by the INSLM. The INSLM's fourth annual report contained a number of recommendations, including the implementation of a special intelligence operations scheme, a recommendation taken up in the National Security Legislation Amendment Bill (No. 1) 2014 (see 'National Security Legislation Amendment Bill (No. 1) 2014', on page 53).

Legislative change

Public Governance, Performance and Accountability legislation

The Public Governance, Performance and Accountability Amendment Act 2014, which amends the *Public Governance, Performance and Accountability Act 2013*, received royal assent on 26 June 2014 and became effective on 1 July 2014. Its consequential counterpart, the *Public Governance, Performance and Accountability (Consequential and Transitional Provisions) Act 2014*, received royal assent on 30 June.

During the reporting period, ASIO reviewed the proposed draft legislation and subordinate rules and regulations and worked cooperatively with other intelligence and security agencies, the Department of Finance and the Attorney-General's Department to ensure a smooth transition from the previous accountability regime (under the *Financial Management and Accountability Act 1997*) to the new regime under the Public Governance, Performance and Accountability legislation.

This included work with the Department of Finance to ensure that ASIO would still be subject to the same accountability mechanisms as before and that these mechanisms would not jeopardise the ongoing security of intelligence personnel or investigations. This was achieved in part by ASIO advising on the practical application of parts of the proposed regime to ASIO's day-to-day work in collecting intelligence relevant to security. See Part 5 for further information about the Public Governance, Performance and Accountability legislation.

Information Privacy Act 2014 (ACT)

The *Information Privacy Act 2014* (ACT) was passed by the Legislative Assembly of the Australian Capital Territory (ACT) on 3 June 2014. It was introduced to regulate the handling of personal information (other than personal health information) by public sector agencies in the ACT.

During the reporting period, ASIO provided advice to the ACT Government that the Bill, as it had been introduced, might prevent the timely disclosure to ASIO of personal information relevant to security that would assist in the collection of security intelligence. ASIO undertook a large amount of work to review proposed amendments to the Bill and provide briefings to relevant ministers and departments on the practical application of parts of the proposed regime to the performance by ASIO of its function of collecting intelligence relevant to security.

In ASIO's view, the resulting exemptions in the *Information Privacy Act 2014* achieve a balance between the right to privacy of individuals, and the public interest in ensuring intelligence and law enforcement agencies can perform their role effectively in the interests of national security and safety.

Legislation on assumed identities

With the support of the Attorney-General's Department, ASIO has been pursuing amendments to state and territory legislation on assumed identities (AIs). During the reporting period, this work resulted in amendments to New South Wales, ACT and Victorian legislation on AIs.

New South Wales

The *Law Enforcement and National Security (Assumed Identities) Act 2010* (NSW) was amended on 23 August 2013 to allow the Director-General of Security to apply for an order from an eligible NSW Supreme Court judge for entry of an AI in the NSW Births, Deaths and Marriages (BDM) register in acquiring evidence of the assumed identity under a Commonwealth AI authority. The legislative amendments also ensure that sensitive information is protected in applications for orders for entry, or cancellation of an entry, of an AI in the NSW BDM register by requiring that applications be heard in chambers and not in open court.

Australian Capital Territory

The *Crimes (Assumed Identities) Act 2009* (ACT) was amended on 10 December 2013 to allow the Director-General of Security to apply for an order from the ACT Supreme Court for entry of an AI in the ACT BDM register in acquiring evidence of the AI under a Commonwealth AI authority.

Victoria

The Crimes (Assumed Identities) Regulations 2006 (Vic) was amended on 15 July 2013, declaring Part IAC of the *Crimes Act 1914* (Cwlth) a corresponding law for the purposes of the *Crimes (Assumed Identities) Act 2004* (Vic). This means ASIO can rely on the Victorian AI legislation to apply for orders from the Victorian Supreme Court for entry, or cancellation of entry, of an AI acquired under a Commonwealth AI authority in the Victorian BDM register, and to support the acquisition/cancellation of other evidence of an AI authorised by a Commonwealth AI authority.

These amendments represent a significant outcome for ASIO in the protection of the identity of its officers and people.

National Security Legislation Amendment Bill (No. 1) 2014

Senator The Hon. George Brandis QC introduced the National Security Legislation Amendment Bill (No. 1) 2014 into parliament on 16 July 2014. While outside of the reporting period, the introduction of the Bill was built on a significant body of work during the reporting period.

The Bill gives effect to important recommendations in Chapter 4 of the PJCIS's *Report of the inquiry into potential reforms of Australia's national security legislation.* ASIO believes this legislative reform is critical to ensuring ASIO is equipped to carry out its mandate in the face of rapidly changing security environments.

The Bill is intended to modernise and address gaps in the legislative framework that governs the activities of the Australian Intelligence Community, primarily through changes to the ASIO Act and the *Intelligence Services Act 2001* (the ISA). The Bill also contains some additional measures to update and strengthen secrecy offences in the ASIO Act and the ISA to protect intelligence personnel and information.

The proposed amendments fall into four broad themes; effectiveness, modernisation, cooperation and the protection of information and capabilities.

BROAD THEMES OF THE BILL

Effectiveness

The National Security Legislation Amendment Bill (No. 1) 2014 includes amendments to address problems being experienced with the scope and effectiveness of ASIO warrants, including:

- amendments to ASIO's computer access legislation (section 25A of the *Australian Security Intelligence Organisation Act 1979*)
- introduction of an identified person warrant
- a proposed special intelligence operations scheme to protect ASIO employees and other persons from liability for certain lawfully authorised activities that would otherwise be unlawful.

Modernisation

Also included are amendments to update ASIO's surveillance device provisions, including by making clarifications to legislation in respect of the use of surveillance devices and alignment with the *Surveillance Devices Act 2004*. The Bill also incorporates amendments to modernise ASIO's employment provisions.

Cooperation

The Bill includes changes to enhance further cooperation between ASIO and ASIS, by enabling ASIS to undertake an activity, or series of activities, to support ASIO in the performance of its functions and for the specific purpose of producing intelligence on an Australian person (or class of Australian persons) without a ministerial authorisation.

The Bill also contains changes to confirm the existing power for ASIO to cooperate with the private sector—for example, through the Business Liaison Unit.

Protection of information and capabilities

The Bill includes amendments to the communication-of-information provisions in the *Intelligence Services Act 2001* and the ASIO Act to increase the penalty for existing offences of unauthorised communication of national security information and to introduce offences for unauthorised copying and/or removal of information relating to an agency in the Australian Intelligence Community.

Another change reflected in the Bill is to ensure that breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) can be referred to law enforcement for investigation when it is not otherwise relevant to security.

Amendments in the Bill also include the introduction of a prima facie evidentiary certificate regime to apply to some ASIO Act warrants and authorisations, similar to the regimes in the *Telecommunications (Interception and Access) Act 1979*. This amendment provides an additional legislative basis to help ASIO protect the identity of employees, sources and sensitive capabilities used in connection with certain warrants or authorisations issued under the ASIO Act.

Public Interest Disclosure Act 2013

By the time the *Public Interest Disclosure Act 2013* (the PID Act) came into effect on 15 January 2014, ASIO had implemented policies and procedures to support the PID Act. The new policy framework provides public officials with a clear and legitimate pathway for reporting concerns about wrongdoing or maladministration, either within the Organisation or in the wider Australian Public Service (APS).

The framework complements ASIO's existing security protocols and provides the Organisation with an additional mechanism to develop a strong and supportive security culture. ASIO strongly supports the need for all APS agencies to have the ability to facilitate disclosure and investigate wrongdoing and maladministration in the APS, including within ASIO.

For intelligence agencies, the PID Act works in conjunction with other legislation—such as the ASIO Act, the IGIS Act, the ISA and the *Crimes Act 1914*—to protect intelligence information and provides specific avenues for individuals to make a public interest disclosure involving intelligence information.

Throughout the reporting period, ASIO worked in close consultation with the Office of the IGIS and with the Department of the Prime Minister and Cabinet in implementing policies and procedures to deal with any disclosures made under the PID Act.

Since implementing the policies and procedures in January 2014, ASIO has embarked on an education program for all staff, including delivering training for supervisors, authorised officers and investigating officers. In addition, all staff are required to undertake mandatory e-learning training outlining their rights and responsibilities under the PID Act.

In the first six months of the new framework, two disclosures were received and allocated to an investigating authority. One of the allocated disclosures was withdrawn by the discloser prior to investigation, and the second resulted in an investigation reviewing internal processes. The completed public interest disclosure investigation produced recommendations aimed at improving organisational effectiveness and increasing overall accountability.

Public interest disclosures regarding ASIO can be made via telephone to 02 6249 6804 or sent to:

Public Interest Disclosures
PO Box 7241
Canberra BC ACT 2610

Council of Australian Governments review of counter-terrorism legislation

The Council of Australian Governments (COAG) review committee completed its review of counter-terrorism legislation and tabled its report on 14 May 2013. COAG made recommendations regarding counter-terrorism offences, such as creating a terrorism hoax offence and expanding the definition of 'terrorist act' in relevant legislation to clearly include threats of action. It also made changes to control orders and preventative detention orders under the *Criminal Code Act 1995*. Some of the COAG recommendations are being considered for introduction in the proposed National Security Legislation Amendment Bill (No. 2) 2014 as part of the Australian Government's response to that review.

Internal audits and fraud control

Fraud control

ASIO is committed to enhancing its fraud control and management arrangements so that they reflect best practice. In preparation for the introduction of the *Public Governance, Performance and Accountability Act 2013* and associated rules on 1 July 2014, ASIO reviewed its fraud policies and guidance documents and conducted a fraud risk assessment to inform its current Fraud Control Plan.

In the reporting period, ASIO also developed its Fraud Management Guidelines. These provide staff with specific guidance on the Commonwealth fraud control policy framework, ASIO's fraud control and management arrangements and fraud allegation reporting procedures. ASIO received one allegation of fraud, which was dealt with through the PID Act investigative process. No external allegations of fraud were reported.

Fraud awareness training for all new employees and contractors has been a feature of ASIO induction training for several years. The Organisation also provides a mandatory e-learning training module on fraud awareness, which ASIO personnel must complete every three years.

Audit

The Internal Audit directorate undertakes performance audits of business areas and processes to improve ASIO performance and ensure the Organisation is meeting legislative, regulation and policy requirements. In 2012–13, the directorate audited ASIO's compliance with the requirements of the *Work Health and Safety Act 2011* and recommended a follow-up audit be conducted to assess the outcomes of a number of projects underway at the time. The directorate conducted the follow-up audit in the reporting period and found ASIO had made improvements in the area of work health and safety policy development and guidance material, had expanded the Health and Safety Representative role and had implemented a health and safety inspection program.

In 2013–14, ASIO continued to conduct compliance audits to ensure the Organisation's conformance with privacy requirements and agreements made with external partners. ASIO also continued to formalise existing informal arrangements in order to promote a better compliance framework and provide accountability for, and assurance of, internal controls.

The 2013–14 Internal Audit Work Plan included an additional annual compliance audit. This audit focused on ASIO's Rehabilitation Management System and arose from new requirements in the *Safety Rehabilitation and Compensation Act 1988.* The audit sought to establish whether ASIO was using the framework of the legislation and the Guidelines for Rehabilitation Authorities 2012 to manage the return to work of its injured employees. The audit found ASIO was meeting the requirements of the framework and the guidelines.

Audit of assumed identities

Assumed identities are used to protect ASIO officers' identities and prevent the potential compromise of ASIO operational activities. The authority for this is drawn from Part IAC of the *Crimes Act 1914,* under which stringent audit requirements are applied six-monthly. Additionally, a small number of authorities are maintained under the New South Wales *Law Enforcement and National Security (Assumed Identities) Act 2010.*

The Internal Audit directorate undertook all mandated audits and provided certificates of compliance to the Office of the IGIS and privacy commissioners where specifically required. No compliance issues requiring rectification were identified.

Security in ASIO

ASIO is committed to ensuring ASIO officers, premises, information and assets are protected from compromise. To achieve this, ASIO adheres to a best practice security model which meets Australian Government requirements and also has additional ASIO-specific protective security measures. These measures include security awareness programs and initiatives designed to reflect contemporary issues as well as emerging threats to ASIO's internal security. Such programs, coupled with robust security policies and procedures, assist in promoting an active security culture amongst ASIO officers.

Security policy and coordination

ASIO complies with the Australian Government's Protective Security Policy Framework's requirements for the management and oversight of the Organisation's protective security, and it develops policies aligned with this framework. ASIO also has internal security policies and procedures specific to the Organisation's unique security environment. These are continually reviewed to ensure they remain current and relevant. New or significantly altered policies are communicated to staff via security education and awareness campaigns.

Personnel security

All ASIO officers hold high-level security clearances. The suitability to hold a clearance is assessed as part of entry to ASIO and as per Australian Government security clearance requirements. ASIO officers must be honest, trustworthy, mature, tolerant and loyal and not susceptible to influence or coercion. Throughout their employment with ASIO, officers' suitability to hold this clearance is continually evaluated by a variety of government-mandated and ASIO-specific reviews.

Physical and information security

All ASIO premises are designed to meet the Australian Government Protective Security Policy Framework's requirements for the protection of officers, premises, information and assets. ASIO also implements information security programs designed to protect ASIO's information and communication systems. These programs focus on ensuring that usage of ASIO information systems is appropriate, authorised and secure and that classified and/or sensitive information is effectively protected. Protection strategies are continually reviewed in recognition that the security environment is always changing, with new threats and challenges constantly emerging.

Information technology security

ASIO employs a range of activities and capabilities to ensure that ASIO's information technology systems are secure and that usage is appropriate and authorised. These programs include ongoing security awareness campaigns designed to develop a strong security culture, reviews of system security compliance, and ongoing audit and monitoring activities.

Part 5

CORPORATE MANAGEMENT

'National security is as relevant today as it has ever been. The threats exist, and they endure. We are in the business of dealing with the unknown, often in a fast and fluid environment—in fact, very little in our business is certain.'

David Irvine, Director-General of Security
Security in Government Conference 2013, 13 August 2013

Image: Neale Cousland / Shutterstock.com

Corporate strategy and governance

ASIO Strategic Plan 2013–16

To operate effectively, ASIO must not only meet the security needs of Australia today but prepare for the challenges of tomorrow. ASIO's Strategic Plan 2013–16 reflects that requirement and contains elements specific to ensuring that Australia's national security capability is maintained.

In 2013–14 the Strategic Plan served as the keystone of ASIO's strategic and operational planning, including:

- setting the overall direction of the Organisation through business plans, corporate committee priorities and executive focus
- ensuring ASIO's capability development investments contributed to meeting the goals outlined in the Strategic Plan
- measuring and reporting on performance as it pertained to the Strategic Plan.

Importantly, the Strategic Plan was also used to prepare ASIO for the introduction of the *Public Governance, Performance and Accountability Act 2013*, particularly through the development of ASIO's Risk Management Policy.

ASIO's Strategic Plan 2013–16 is an unclassified, publicly available document. It is available on ASIO's website www.asio.gov.au.

Figure 3: ASIO's governance committees

ASIO's governance committees

The Director-General of Security is responsible for ensuring that ASIO achieves its mission: to identify and investigate threats to security and provide advice to protect Australia, its people and its interests. ASIO's corporate governance framework provides the information and advice required to support the Director-General of Security in his responsibilities.

Unless otherwise noted, all sitting members of ASIO committees are serving ASIO officers.

ASIO Executive Board

The Executive Board is the peak advisory committee to the Director-General of Security. ASIO's Executive Board comprises the Director-General of Security, the Deputy Directors-General and an external member, Ms Jenet Connell, a highly experienced and distinguished public servant currently serving as the Chief Operating Officer of the Department of Finance.

ASIO STRATEGIC PLAN 2013–16

VISION

The intelligence edge for a secure Australia

MISSION

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

GOALS

Deliver high-quality security intelligence collection, analysis, assessment and advice in support of our mission
We excel in our use of security intelligence in support of our mission.
We work with partners to ensure capabilities are managed to optimise security outcomes.
We provide timely and accurate security intelligence advice to support decision-makers.
We manage risk in a constantly evolving security environment.

Continue to enhance our strategic impact and reputation
We work effectively and collaboratively with national and international partners and are seen as a responsive and collegial partner.
We are influential in shaping Australia's response to the national and international security environment.
We promote security awareness and understanding across government and private industry.
We provide leadership and expertise on security intelligence in support of our mission.

Evaluate, evolve and strengthen our capabilities and business practices
We are professional, with the flexibility, initiative and determination to anticipate and drive change.
We harness opportunities and address challenges presented by technology.
We build accountability and evaluation into everything we do.
We evaluate activities to strengthen future planning and decision-making.

Attract, develop and retain a professional and highly competent workforce
We exemplify excellence in security practices, cooperation, accountability and integrity.
We develop and support people to succeed.
We have a motivated, high-performing workforce who exemplify professionalism in all they do.
We have a strong, unified leadership team who encourage and motivate others to achieve.

The Executive Board meets monthly. Its functions are to set ASIO's strategic direction, consider significant resource and budget issues, consider security strategy, and provide guidance and oversight to significant policy developments. The minutes of the Executive Board are visible to Australian National Audit Office (ANAO) as part of its governance audit.

Over the reporting period, the Executive Board received regular reporting from ASIO's corporate committees on outcomes, key security issues (including the conflict in Syria, developments in the domestic security environment and espionage threats), the Organisation's budget and investment program, and risks.

In the lead-up to the *Public Governance, Performance and Accountability Act 2013* (the PGPA Act) coming into effect, the Executive Board received submissions from ASIO's Audit and Risk Committee and a briefing with representatives from the Department of Finance, enabling ASIO to put in place policies and procedures to meet the requirements of the PGPA Act.

Internal performance reporting

ASIO conducts quarterly internal performance reporting, which the corporate committees provide to the Executive Board. Over the reporting period, the process and system for reporting performance to the Executive Board were refined and parameters were set against ASIO's Strategic Plan 2013–16. This was done to facilitate the Executive Board's consideration of matters of strategic importance to ASIO and to highlight when an emerging or ongoing strategic risk requires action.

Intelligence Coordination Committee

The Intelligence Coordination Committee (ICC) directs ASIO's investigative and assessment priorities, including the coordination and allocation of resources. The ICC also performs the functions of a program board and provides governance for intelligence and related investment projects in ASIO. The committee is chaired by a Deputy Director-General.

The focus of the ICC ranges across different intelligence thematic areas, including counter-terrorism, counter-espionage and the protection of Australia's territorial and border integrity from serious threats.

Workforce Capability Committee

ASIO's ability to both respond to and prepare for challenges in the security environment depends largely on its highly skilled workforce. The Workforce Capability Committee (WCC) considers matters relevant to the size, skill set and accommodation of ASIO's workforce. It also provides reporting to ASIO's Executive Board on the performance of ASIO's recruitment, internal transfer and training programs. The committee is chaired by a Deputy Director-General. A subcommittee of the WCC is the Work Health and Safety Committee, which is responsible for ensuring better health and safety policies and practices across ASIO.

Over the reporting period, the WCC oversaw the compliance rates for ASIO mandatory e-learning modules. Similarly, the WCC reported to the Executive Board on ASIO's Enhancing Performance framework, including statistics on compliance rates across the Organisation.

These reports, provided to the Executive Board, informed management of compliance levels across their teams in both training and performance management. This heightened awareness resulted in an increased uptake of the training and performance programs.

Counter Intelligence and Security Review Committee

The security of information, systems and people is fundamental to the effective operation of ASIO as a security intelligence organisation. The Counter Intelligence and Security Review Committee (CISRC) is the coordinating body for approving security policy and procedures in ASIO. In fulfilling that role, the CISRC provides assurance to the Executive Board—and, through it, the Director-General of Security—of sound and secure practices in ASIO.

A subcommittee of the CISRC is the ASIO Security Committee, which has primary responsibility for the application and integration of security practices and processes in ASIO.

Finance Committee

The Finance Committee (FC) monitors ASIO's financial performance and provides advice to the Executive Board on the financial management of the Organisation.

A subcommittee of the FC is ASIO's New Building Committee (NBC), which is responsible for ensuring that the Ben Chifley Building will meet ASIO requirements. As the building project nears completion, reporting lines will change and the NBC will begin reporting to the WCC. This is in acknowledgment that the project will have shifted from one of project management to one requiring oversight of the move of ASIO's workforce to the Ben Chifley Building.

Each year, ASIO undertakes a program of investment aimed at delivering the capabilities required to meet identified priorities and address strategic risks. In 2013–14 the FC oversaw and reported on the financial aspects of this program to the Executive Board, providing additional assurance to the board as each project advanced.

Audit and Risk Committee

The Audit and Risk Committee (ARC) provides advice on ASIO's risk management, a range of internal controls and legislative and policy compliance. The ARC is a senior corporate committee, comprising three internal and two external members.

Two years ago, the Director-General of Security appointed an independent chair to the ARC, underlining the committee's role in providing independent assurance and advice to the ASIO executive on a range of governance and compliance matters. The current independent chair is Ms Lynelle Briggs AO, a distinguished former public servant whose experience includes serving as the Australian Public Service Commissioner and the Chief Executive of Medicare Australia. The committee also includes a second external agency member, Mr Roman Quaedvlieg, Deputy Chief Executive Officer of Australian Customs and Border Protection Service and an observer from the ANAO, reinforcing the committee's role in providing independent assurance and advice.

In the reporting period, consistent with the ANAO's *Better Practice guide on audit committees*, ASIO conducted a biennial performance review of the ARC. The review found the overall performance of the committee was sound. Recommendations centred on enhancing committee administration and member induction and training, as well as incorporating changes relating to the introduction of the Public Governance, Performance and Accountability rules. The ARC endorsed the review findings and ASIO implemented all recommendations.

The ARC has particularly focused on the development of a risk management policy that seamlessly covers the corporate and operational functions of ASIO. This work is essentially complete. The ARC expects the policy to be integrated into the existing risk management framework, augmenting existing risk management guidance documentation. For further information on the policy, see 'Risk management', page 64.

The ARC has considered all audits undertaken by ASIO's Internal Audit during the period and monitored and reviewed ASIO's response and action in relation to recommendations or significant issues raised in external audit and review reports and Better Practice guides. For further information on the audits and reviews considered by the committee, see 'Internal Audit' in Part 4.

Communication and leadership meetings

Distinct from ASIO's corporate committees are ASIO's communication and leadership meetings. They do not represent decision-making points but instead focus on communicating current and emerging issues and ensuring they are understood across the Organisation.

- The Senior Executive Meeting is a meeting of all ASIO division heads at Senior Executive Service level 2 and above and occurs weekly.
- The Senior Executive Service Meeting is a meeting of all officers at Senior Executive Service level 1 and above and occurs monthly.

ASIO Consultative Council

The ASIO Consultative Council provides a conduit between the staff and executive of ASIO on matters of employment conditions and provisions. Two representatives from ASIO's Staff Association and two representatives from ASIO's management group constitute a quorum for the meeting. Over the reporting period, the ASIO Consultative Council received updates regarding:

- the Australian Government Employment Bargaining Framework;
- ASIO's first Consolidated Determination of Terms and Conditions of Employment; and
- the ASIO Staff Survey.

Risk management

In May 2013 ASIO commenced a review of its Strategic Risk Management Framework. The purpose of the review was twofold: to establish whether the framework still served ASIO's requirements and to ensure ASIO was well placed to implement changes required by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The review found that the framework ensured ASIO met the compliance requirements of risk management standard (AS/NZS ISO 31000:2009) but that it did not focus on treating risk as an opportunity. The review also identified changes required for ASIO to be suitably prepared for commencement of the PGPA Act. In response to the review, ASIO developed a new draft risk management policy. This draft policy was endorsed by ASIO's Executive Board in December 2013 and has since been reviewed to ensure compliance with the PGPA Act.

To support the new policy, ASIO has developed an overarching statement on its tolerance of risk, and it is developing risk threshold statements for each of its corporate committees. These statements will enable the committees to communicate to staff the risks ASIO is prepared to take to achieve its objectives. Such communication is aimed at assisting ASIO officers at all levels to assess the level of risk they are taking to achieve outcomes in their work.

At the conclusion of the reporting period, ASIO's risk management policy met the requirements of the PGPA Act. Work is ongoing to further build on progress made in ASIO's approach to risk.

PUBLIC GOVERNANCE, PERFORMANCE AND ACCOUNTABILITY ACT

The *Public Governance, Performance and Accountability Act 2013* (the PGPA Act) establishes a principles-based financial management framework covering governance, accountability and performance. Regulatory details have been provided in rules made under the PGPA Act. The PGPA Act replaces the *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act 1997*. The substantive provisions of the PGPA Act came into effect on 1 July 2014, while some requirements will come into effect from 1 July 2015.

The PGPA Act imposes a number of duties both on 'accountable authorities', including the Director-General of Security, and on officials. ASIO has undertaken a range of activities to prepare for the commencement of the PGPA Act.

- The Executive Board and the Audit and Risk Committee (ARC) received briefings from the Department of Finance on the PGPA Act and its implications.
- ASIO reviewed the ARC's charter and composition to ensure the committee fulfils the responsibilities set out in the PGPA Act.
- ASIO has updated its financial instructions and delegations to reflect the requirements of the PGPA Act.
- A principles-based Commonwealth Risk Management Policy has been developed by the Department of Finance to support the discharge of responsibilities under the PGPA Act. ASIO has refreshed its enterprise risk framework to comply with the PGPA requirements.

The PGPA Act brings together responsibilities in relation to planning, measuring, assessing and reporting financial and non-financial performance. The Act establishes seven elements to provide a means for recording and reporting on performance; of these elements, six are new features.

The PGPA rules on fraud establish minimum standards for managing the risk and incidents of fraud. They are consistent with the current Commonwealth Fraud Control Guidelines and ASIO already complies with them.

Further PGPA legislation—the *Public Governance, Performance and Accountability Amendment Act 2014* and the *Public Governance, Performance and Accountability (Consequential and Transitional Provisions) Act 2014*—was enacted in 2014. See Part 4 for further information.

Outreach

ASIO is committed to engaging across the public, community, government and business sectors. Building effective relationships and meaningful dialogues is integral to ASIO's work in maintaining the security of Australia, its people and its interests.

As Australia's security intelligence organisation, ASIO may pique interest, curiosity and reserve. Through direct public contact, such as the Director-General of Security's speeches at community events, ASIO seeks to dispel inaccuracies, foster a broad understanding of the Organisation and its challenges, and continue to build trust among the Australian community. The public can also contact ASIO directly, through the ASIO public line (1800 020 648).

Through a constant exchange of information and ideas, ASIO builds indispensable relationships with agencies in both government and business. ASIO's protective security program, targeted briefing days and unclassified reports on issues of national security are all elements in ASIO's comprehensive program of outreach and engagement.

ASIO Partnership Forum

ASIO's Partnership Forums involve participants from the national security community and broader government partners. The forums aim to develop the participants' understanding of ASIO's role, structure and capabilities in the context of the wider national security community, as well as to foster a common understanding of priorities and shared challenges.

During the reporting period, ASIO held six Partnership Forums: three forums for senior officers and three for Senior Executive Service officers. These forums attracted attendance from 120 people across 42 state, territory and Commonwealth government agencies. Feedback from the forums was overwhelmingly positive, with attendees remarking on the high level of detail and contemporary nature of the information provided.

Stakeholder Satisfaction Survey

The annual Stakeholder Satisfaction Survey is a vital mechanism in understanding ASIO's relationship with partner agencies. The survey provides ASIO with feedback on ASIO's engagement with partners, with a focus on strategic and administrative issues. At a strategic level, topics covered in the survey include collaboration, stakeholder focus, and capabilities and people. At an administrative level, feedback is sought on the quality, timeliness and accessibility of ASIO's information and advice.

ASIO has engaged an external consultant to prepare and conduct the survey to ensure feedback is forthright. Preparations for the next survey have commenced, with interviews scheduled to be conducted in July–August 2014. It is expected that the findings will be presented to ASIO senior management in late 2014.

Public statements and the media

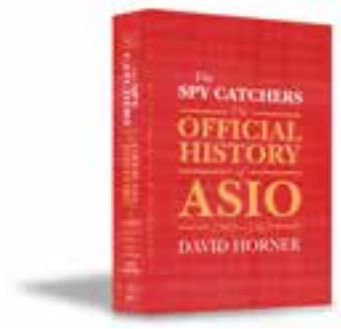
ASIO endeavours to provide timely and considered public comment on contemporary security-related matters, such as terrorism and espionage. While ASIO does not comment on specific operations, investigations or individuals, public statements are made by the Director-General of Security and by ASIO Media when responding to media inquiries.

The Director-General of Security is the face of ASIO and provides first-hand comment though occasional public speeches, media interviews and statements. Transcripts of public speeches by the Director-General of Security are available on the ASIO website www.asio.gov.au.

ASIO makes a concerted effort to provide meaningful information to assist the media when reporting on national security. For ASIO, it is an opportunity to clarify the Organisation's position and inform the public about the current security environment. ASIO appreciates the value of accurate media reporting on national security.

The Official History of ASIO

The Australian National University (ANU), under the direction of Professor David Horner AM, has completed writing Volume 1 of *The Official History of ASIO*. Volume 1 covers the period 1949 to 1963 and explores the reasons ASIO was established and its role during the Cold War. Following a competitive process, ASIO selected Allen & Unwin to publish the *Official History*, and Volume 1 will be available in retail outlets from October 2014.



Over 5500 unredacted ASIO files were viewed by the ANU researchers writing the *Official History of ASIO*. ASIO subjected the manuscript to an exhaustive clearance process to ensure it contained no information prejudicial to national security, while maintaining the academic integrity and factual accuracy of the history itself.

Because of the significance and amount of material uncovered during the research, the Director-General of Security agreed to the ANU's proposal to reconfigure the original two volumes into three volumes. Three volumes will allow the history to be told in a more thorough and constructive manner. Volume 2 (1963 to 1975) covers the period of the Vietnam War and the Whitlam government. Volume 3 (1975 to 1989) covers the advent of the Hope Royal Commissions and their profound impact on ASIO, and the Fraser and Hawke governments.

The History of ASIO Advisory Committee has monitored the progress of the project since its inception. The committee meets every six months and comprises two external members—Mr Geoff Gallop AC and Mr Jim Carlton AO—as well as the Director-General of Security and a Deputy Director-General.

People

Overview

The rapidly evolving security environment is shaping ASIO's work program. To meet the challenges of its environment, ASIO delivers high-quality, agile human resources programs and services that support the Organisation in achieving security intelligence outcomes that protect Australia, its people and interests.

ASIO's work in the human resources area has contributed towards all four of the goals described in ASIO's Strategic Plan, particularly 'Attracting, developing and retaining a professional and highly competent workforce'. ASIO continues to develop and refine programs and services that enable the Organisation to meet increasingly diverse and complex security challenges.

OUTCOMES AND ACHIEVEMENTS

During the 2013–14 reporting period, ASIO:

- Made significant progress in the review and redevelopment of its employment relations framework—in particular, establishing ASIO's Consolidated Determination of Terms and Conditions of Employment and conducting a comprehensive review of human resources delegations.
- Implemented a Professional Conduct and Behaviour Strategy that saw the development of a range of new policies, as well as a review of ASIO's Values and Code of Conduct. These initiatives seek to clarify the behavioural expectations of all staff, at work and in connection with work, to ensure ASIO maintains a professional, ethical and high-performance culture.
- Developed and delivered, in close collaboration with partner agencies, a shared-services approach to management and leadership training that will build a pipeline of future leaders in the Australian Intelligence Community.
- Introduced a framework for strategically managing local and international postings, affording greater flexibility in balancing the requirements of the Organisation and individuals.
- Significantly strengthened relationships with international partner agencies on corporate and human resources matters, sharing corporate strategies and resources to build capability.
- Reviewed and implemented a revised intelligence training model and enhanced ASIO's suite of advanced operational training programs.

Workforce management and reporting

In 2013–14, ASIO continued with downsizing activities, a result of recommendations from the internal Review of the Staffing and Resource Allocation (2012–13). Such activities included a capability-reshaping program, with targeted voluntary redundancies, suspended recruitment for non-critical job families and heightened efforts to recruit for intelligence officers, technical officers and security assessors. These initiatives reduced our middle management structure and enabled ASIO to prioritise growth and effort in key operational areas to ensure the Organisation has the workforce capacity and capability to respond to current and future priorities. As at 30 June 2014, ASIO employed 1685.4 full-time equivalent staff.

The Organisational Capability Program provides ASIO with a variety of mechanisms to deploy staff around the Organisation, including internationally, developing the capability and capacity required by ASIO to deliver on its mission. In 2013–14 the program was expanded to include all roles, meeting ASIO's requirement to develop depth and breadth of experience in its staff while delivering flexibility for staff to manage their careers and balance personal and family responsibilities.

Recruitment and staff movements

In 2013–14, recruitment remained one of ASIO's key challenges. The focus for the period was on the difficult-to-fill roles of intelligence officer, technical officer and security assessor.

ASIO places a range of security-related requirements on staff over and above those required by other employers, and this increases the challenge in attracting suitable candidates. The skill-sets and backgrounds required can be either very broad or very specific. To engage with prospective employees and promote employment opportunities, ASIO placed recruitment advertising across a range of online media, including social-networking sites and the ASIO website. While it receives a large volume of applications, ASIO is often aiming to attract passive job seekers with specialist skills, people who are not actively seeking specific opportunities but who are open to changing employment if an interesting role catches their eye. To ensure that these passive job seekers were reached, ASIO also advertised employment opportunities in a range of targeted newspapers and specialist professional publications.

ASIO's expenditure on recruitment advertising for difficult-to-fill roles increased from $317 729 in 2012–13 to $599 739 in 2013–14. Since the implementation of this new advertising strategy, one recruitment campaign for intelligence officers has been finalised. The campaign attracted 1049 applications, compared with 638 applications for the previous campaign—an increase of approximately 40 per cent.

Through the introduction of a new technical officer graduate program, ASIO strengthened its 'grow your own' strategies to attract and develop entry-level staff in specialist areas. Aimed at university graduates, the one-year structured program includes placements in a range of technical areas, supported by a senior mentor. The program provides graduates with the skills and knowledge required to undertake a range of roles in ASIO's technical areas. At its conclusion, graduates specialise in a technical area and continue to develop and expand their skills.

Employment relations

In 2013–14, ASIO focused on improving human resource governance arrangements by strengthening its employment instruments and using them to enhance the positive culture of the Organisation. A critical component of this was the introduction in September 2013 of the ASIO Consolidated Determination of Terms and Conditions of Employment and supporting human resource delegations, which underpin all employment-related decisions in ASIO. The development of these instruments reflects ASIO's contemporary approach to people management and provides staff and managers alike with a transparent and accountable employment framework. These instruments are now embedded in ASIO's employment framework and continue to be refined to ensure they meet the progressing needs of the Organisation.

Culturally, ASIO continues to focus on the expected standards of behaviour and professional conduct of staff. ASIO's new Professional Conduct and Behaviour Strategy outlines the Organisation's approach in clarifying behavioural expectations, managing hazards and risks and addressing infractions. A review of the ASIO Values and Code of Conduct formed part of the strategy and has brought about greater alignment with the Australian Public Service.

Initial consultation on the 10th ASIO Workplace Agreement commenced in June 2014. The Workplace Agreement is the mechanism through which ASIO negotiates changes to terms and conditions of employment, consistent with the Australian Government Public Sector Workplace Bargaining Policy.

ASIO'S PROFESSIONAL CONDUCT AND BEHAVIOUR STRATEGY

The Professional Conduct and Behaviour Strategy takes a multifaceted approach to addressing all forms of inappropriate behaviour. The strategy focuses on the importance of professional conduct and behaviour in the workplace but also raises awareness of a staff member's obligations and responsibilities when their conduct is 'in connection' with work but they are not physically at work. Examples are attendance at a training course or a work-related social function, or use of social media about work or more generally. In addition to clearly articulating and reinforcing ASIO's expectations, the strategy also educates staff on their rights and sets out the culture ASIO wants for its people.

Consistent with Safe Work Australia's Code of Practice, considerable work has been undertaken to identify risks or hazards. This work includes:

- the ASIO staff survey
- focus groups
- analysis of data from existing human resources reporting mechanisms
- extensive consultation with staff.

Some examples of strategies being implemented to manage identified risks or hazards include:

- strengthening the foundations that support professional conduct and behaviour
- consolidating human resources policies in the Consolidated Determination of Terms and Conditions of Employment
- updating the ASIO Values and Code of Conduct
- developing and reviewing related human resources policies such as those on bullying, harassment and discrimination, and professional conduct and behaviour
- reviewing induction information, on-boarding materials and e-learning content
- contributing to the redevelopment of ASIO's Leadership Strategy
- continually strengthening and enhancing ASIO's Harassment and Discrimination Advisor network.

Elements of the Professional Conduct and Behaviour Strategy will continue to be embedded over a 12-month schedule, followed by ongoing review and evaluation.

Ombudsman

The ASIO Ombudsman is an external service provider who acts to resolve staff issues or concerns impartially and informally, through advice, consultation and mediation.

In 2013–14 the ASIO Ombudsman provided advice in relation to 42 general queries and responded to 36 staff in relation to formal matters. Four reviews of complaints were conducted during this period at the direction of management.

During this period, the ASIO Ombudsman provided valuable input into reviewing and amending the ASIO Values and Code of Conduct, and into the design and development of content for ASIO's bespoke management training programs, while also delivering, in the ASIO new starter program, regular presentations on the role of the Ombudsman.

ASIO staff also have the opportunity to formally raise concerns through the *Public Interest Disclosure Act 2013* and the Office of the Inspector-General of Intelligence and Security.

Work Health and Safety

ASIO maintains a strong focus on early intervention and active rehabilitation case management, and initiatives such as the HealthINT program continue to raise ASIO officers' awareness and understanding of their own lifestyle choices. This approach seeks to minimise the financial cost and personal impact associated with long-term people management issues, while supporting line management to resolve complex staffing situations.

During the reporting period, no notifications were made to Comcare and no investigations were conducted, nor were any notices issued to ASIO under the *Work Health and Safety Act 2011* (WHS Act). In 2013–14 much of the focus in work health and safety was on developing and embedding policies and guidelines to help ASIO manage risks to the health and safety of its workers.

Following an internal audit conducted in 2013 to determine ASIO's compliance with the WHS Act, the Organisation implemented a number of projects, including:

- an incident reporting campaign to encourage ASIO workers to report work health and safety incidents and near-misses
- the development of key performance indicators to help identify trends and more effectively manage risk
- monitoring of the staff completion rate of mandatory work health and safety e-learning to ensure current knowledge among staff.

In 2012, ASIO invited Comcare to conduct an audit of the Organisation's rehabilitation management system to provide a benchmark of how effectively it is meeting its obligations under the *Safety, Rehabilitation and Compensation Act 1988*. Following the Comcare audit, ASIO established an annual internal audit program, in accordance with the requirements of the 2012 Guidelines for Rehabilitation Authorities, issued by Comcare. The first internal audit of ASIO's rehabilitation management system commenced in May 2014.

Health and safety representatives (HSRs) actively engage with their work groups on the benefits of maintaining a safe work environment. They also conduct quarterly workplace safety inspections to identify specific hazards and risks; these are supported by the Work Health and Safety directorate and senior management. In the reporting period, HSRs conducted workplace safety inspections on general work areas and electrical safety, and a review of procedures and general safety is scheduled for the second half of 2014. Corrective actions identified in the quarterly workplace safety inspections were assigned priority using a risk management approach, and 100 per cent of high-priority corrective actions for 2013–14 have been completed.

The First Aid Officer program, which underwent a restructure in 2012, has been reviewed in preparation for ASIO's occupation of the Ben Chifley Building.

The Staff and Family Liaison Service continues to support ASIO staff, including by providing support to those who are relocating interstate or overseas. Family information evenings typically attract 70–100 attendees and provide an opportunity for the families of serving ASIO officers to gain a greater understanding of ASIO's work.

In 2013–14, absences due to work-related injury increased by 18 per cent compared to 2012–13 but remain low compared to pre-2011 figures. ASIO's Comcare premium rate has risen from 1.05 per cent of payroll in 2013–14 to 1.18 per cent of payroll in 2014–15, which has been attributed to an increase in cost-of-injury claims in ASIO and across the Australian Public Service (APS).

Despite this, ASIO's premium rate for 2014–15 is 55 per cent of the average premium rate for APS agencies.

Training and development

Intelligence training

The Intelligence Development Program (IDP) is ASIO's program for training and developing new intelligence officers in analytical and operational tradecraft. It is an intensive, practical program conducted over six months, followed by a further six months of coaching and assessment on the job. Two IDPs were completed in the reporting period, with a number of intelligence officers graduating and commencing their first posting.

ASIO's post-IDP training team continued to deliver advanced and specialised courses, enhancing the skills of practising intelligence professionals in areas such as analytical and operational leadership, situational awareness, agent running and complex tradecraft. Additional courses reflected strategic shifts in the Australian security environment, with courses addressing new risks and new targeting requirements. Strong partnerships have been developed internally and externally to address Organisation-wide intelligence training requirements, as well as more localised and immediate skills development.

Core capabilities

ASIO's capability requirements continue to evolve in response to changes in the operating environment, and training continues to be an important investment in building and sustaining capability.

ASIO provides training and development opportunities through internal and external training programs delivered in-house and by external agencies. During the reporting period, ASIO approved 1400 instances of face-to-face training, attended by 383 officers across 48 training courses at a cost of $588 655. This included training in management and leadership development; corporate programs such as project management and financial management; and Organisational information technology.

In 2013–14, ASIO began implementing the Management and Leadership in Security Intelligence Strategy (2013–16). The strategy focuses on the management and leadership behaviours and skills required of current and future ASIO leaders, providing a framework for talent management and succession planning. The strategy also guides investment and decision-making for targeted development across a suite of management and leadership programs available internally, within the Australian Intelligence Community and in the public and private sectors.

Senior Executive Service development

ASIO has implemented a targeted approach to the development of our Senior Executive Service (SES) that will continue to see ASIO's leadership group capable of setting the right culture and preparing the Organisation for future challenges. This approach will provide ASIO with effective SES succession management, a diverse pool of leadership talent, 'bench strength' for critical roles, and targeted development investment. In 2013–14 ASIO delivered leadership training and provided development opportunities for its SES officers, including:

- a 360-degree survey and coaching program for SES Band 1 officers
- leadership programs in the broader public sector for Bands 1, 2 and 3 officers
- career and succession planning.

e-learning

In addition to existing modules in work health and safety, workplace behaviour, and ethics and accountability, ASIO has added two new modules to its online training catalogue. These mandatory modules help to ensure the Organisation adheres to requirements related to environmental management and public interest disclosure legislation.

All staff are expected to be up to date with mandatory training requirements, and refresher training must be completed regularly. Compliance records are reported to division heads on a monthly basis, and any outstanding requirements are followed up with individuals.

BUILDING LEADERSHIP CAPABILITY IN THE AUSTRALIAN INTELLIGENCE COMMUNITY

During the reporting period ASIO led a shared-services approach to development, designed to build management and leadership capability across the Australian Intelligence Community through the joint design, development and delivery of two training programs:

- The Introduction to Management Program is a management development program aimed at first-time managers and high performers preparing for management roles.
- The Mastering Management Program is for high-performing officers in the Executive Level (EL) cohort. The program is designed for officers who demonstrate experience in managing and leading teams and who are showing potential, ability, motivation and commitment for continued progression into future management and leadership roles.

In 2013–14, 30 officers attended the Introduction to Management Program and 10 EL officers attended the Mastering Management Program. These programs will continue throughout 2014–15, with four of each program scheduled per annum.

Feedback for both programs has been very positive, with participants noting that the use of program champions and EL2 sponsors demonstrated the importance the Organisation places on leadership development. Participants also commended the involvement in the program of the Senior Executive Service and other agencies, as well as the high calibre of the participants and instructors.

ASIO is also developing a program to build foundational skills, including managing performance and managing resources in the context of security intelligence.

Study support and language development programs

Across ASIO, six per cent of staff receive support to undertake study or language development.

ASIO's Study Support Program is intended to provide assistance in the form of financial and/or leave provisions to staff committed to their ongoing professional development. In 2013–14, a review of the program resulted in a simplified framework and a cost-effective funding model, ensuring ASIO can continue to afford to provide these opportunities.

During the reporting period, 166 officers participated in the Study Support Program across more than 100 courses and disciplines—including business management and strategic studies, security and policy, engineering, commerce, project management and information technology—at a total cost of $395 229.

In addition to training, officers can apply for study assistance and support to undertake language skills development. ASIO's Language Skills Development Program is aimed at building language capability across the Organisation. Officers provide a business case outlining their language development proposal, which may include tuition, immersion opportunities or university study in their chosen language. During the reporting period, ASIO allocated $653 622 to fund 38 language development business cases to 34 officers across 11 different languages.

Rewards and recognition

ASIO holds awards ceremonies each year as part of its Rewards and Recognition Framework. This framework recognises the excellent work and dedication of ASIO officers at work and in the broader community. Director-General's medallions are awarded to teams and individuals in the categories of Innovation, Exceptional Leadership, Significant Contribution and Modelling ASIO Values. At the Foundation Day awards ceremony, staff are also recognised for service over 10, 20, 30 or 40 years.

In addition to these awards, the Director-General's bursaries recognise and reward staff who dedicate themselves to personal development and pursuits or community-based work without compromising their work performance.

Property

Ben Chifley Building

ASIO's new central office was opened on 23 July 2013 and named the Ben Chifley Building, after Australia's 16th Prime Minister and the founder of ASIO, Joseph Benedict 'Ben' Chifley. The Ben Chifley Building has been designed and built from the ground up to provide a purpose-built high-security facility. The building will be owned by the Department of Finance and leased to ASIO. It will also house the Australian Cyber Security Centre (ACSC).

Construction of the building is substantially complete. As at the end of 2013–14, the building was undergoing final testing and commissioning. ASIO had begun installing corporate information and communications technology equipment, and the fit-out of the ACSC was nearing completion. Preparations for transitioning staff and systems to the building are well advanced. Based on the current program, ASIO will commence relocating to the building in the second half of 2014, and staff moves will be completed by mid-2015.

Project delays, the collapse of key subcontractors and costs relating to the rectification of problems identified during commissioning have continued to put pressure on the project's budget, with cost overruns increasing to $61 million by the end of 2013–14. This equates to 10.3 per cent of the project budget approved in 2008, up from 7.5 per cent as at the end of 2012–13.

Environmental performance

ASIO has continued its commitment to reduce its carbon footprint. Initiatives undertaken in 2013–14 have resulted in:

- a reduction of approximately 426 000 kilowatt hours (2.1 per cent) in our total energy consumption compared to the previous year
- a total of 65 per cent of waste committed to recycling, including paper products, printer toner cartridges, scrap metal and fluorescent light tubes
- ongoing refinements to operating times for building lighting and air conditioning to meet staffing and seasonal requirements.

In addition, ASIO again participated in the seventh consecutive Earth Hour event, on 29 March 2014.

Financial services

Purchasing

Throughout 2013–14 ASIO adhered to the Commonwealth Procurement Rules and associated policy and guidelines. This involved exercising contemporary procurement advice and methodology in order to ensure ASIO's procurement activities are effectively managed and deliver value for money.

Details of ASIO's agreements, contracts and standing offers are available to members of the Parliamentary Joint Committee on Intelligence and Security (PJCIS), who have oversight of ASIO's administration and expenditure.

ASIO does not manage any expenditure types that require reporting under the Australian Government Spatial Reporting Framework.

Consultants

ASIO entered into 50 new consultancy contracts during 2013–14, resulting in total actual expenditure of $796 231. In addition, 11 ongoing consultancy contracts were active during the reporting period, involving total actual expenditure of $401 066. Total consultancy expenditure has decreased by $101 082 from 2012–13.

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

Competitive tendering and contracting

ASIO participated in 54 open tenders during 2013–14. Other approaches to market were not advertised publicly for reasons of national security, in accordance with clause 2.6 of the Commonwealth Procurement Rules.

Information and technology services

Release of ASIO records

ASIO is an exempt agency under the *Freedom of Information Act 1982* but is subject to release of records under the *Archives Act 1983,* which allows public access to Australian Government records in the 'open period'. In accordance with changes to the Archives Act in 2010, the open period is transitioning from 30 to 20 years. The open period currently covers all records created in or before 1987.

All public requests for ASIO records are made to the National Archives of Australia (NAA). The application is forwarded to ASIO, although the identity of the applicant is not provided by the NAA.

Due to the increasing number of requests for access to records and despite permanently allocating a significant number of officers to service public requests, ASIO faces challenges in meeting the 90-day legislated turnaround time. The Organisation prioritises requests in accordance with a 1992 direction from the then Parliamentary Joint Committee on ASIO; the direction was endorsed in 2008 by the Inspector-General of Intelligence and Security.

In accordance with this direction, ASIO categorises requests into 'fast track' and 'bulk access'. Fast-track requests for information include those that are family related and/or not resource intensive. Bulk-access requests are those of a more complicated nature, including research-related requests for access to a broad range of material. A number of researchers make substantial requests for access to ASIO records, and all need to be treated equitably.

Table 6: Public requests for access to ASIO records over 2012–14

	2012–13	2013–14
Applications for record access	441	773
Requests completed	357	532
Number of pages examined	44 141	56 261

In 2013–14 there was a 75 per cent increase in the number of applications made for access to records. A total of 532 requests were completed in the reporting period.

Applicants dissatisfied with exemptions claimed by ASIO can request a reconsideration of the decision by the NAA. In 2013–14 there were two reconsiderations. In both cases, the NAA upheld the ASIO exemptions. An applicant may appeal to the Administrative Appeals Tribunal (AAT) if the NAA upholds an exemption or if a request for access is not completed within 90 days.

One new appeal against exemptions claimed by ASIO was lodged with the AAT in 2012–13. The applicant later withdrew his application, and the AAT issued formal dismissal advice. An outstanding application from 2012–13 was also processed by the AAT during the reporting period. These requests were not completed within 90 days and are considered a 'deemed refusal' under section 40(8)(c) of the *Archives Act 1983*. The various hearings on these matters led to some reprioritisation of other requests.

Part 6

FINANCIAL STATEMENTS

'What is certain is my trust in the high-quality work done by the people within the national intelligence community. Their respect for the rule of law, regard for fairness and proportionality, and ability to conduct themselves in a non-partisan way are central to our business and its future success.'

David Irvine, Director-General of Security
Security in Government Conference 2013, 13 August 2013

Image: © iStock.com / Kokkai Ng

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2014 are based on properly maintained financial records and give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*, as amended.

David Irvine
Director-General of Security

26 August 2014

Australian National Audit Office

INDEPENDENT AUDITOR'S REPORT

To the Attorney-General

I have audited the accompanying financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2014, which comprise: a Statement by the Director-General of Security; Statement of Comprehensive Income; Statement of Financial Position; Statement of Changes in Equity; Cash Flow Statement; Schedule of Commitments; Schedule of Contingencies; and Notes to and forming part of the Financial Statements comprising a Summary of Significant Accounting Policies and other explanatory information.

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

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

Auditor's Responsibility

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

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

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

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

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

Independence

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

Opinion

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

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

(b) give a true and fair view of the matters required by the Finance Minister's Orders including the Australian Security Intelligence Organisation's financial position as at 30 June 2014 and its financial performance and cash flows for the year then ended.

Australian National Audit Office

David Gray
Executive Director

Delegate of the Auditor-General

Canberra

26 August 2014

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2014

	Notes	2014 $ '000	2013 $ '000
EXPENSES			
Employee benefits	3A	**218,724**	213,075
Suppliers	3B	**137,911**	132,843
Depreciation and amortisation	3C	**49,107**	56,421
Finance costs	3D	**153**	179
Write-down and impairment of assets	3E	**631**	11,058
Losses from asset sales	3F	**294**	161
Foreign exchange losses		**3**	(1)
Total expenses		**406,823**	413,736
Less:			
OWN-SOURCE INCOME			
Own-source revenue			
Sale of goods and rendering of services	4A	**13,513**	27,565
Total own-source revenue		**13,513**	27,565
Gains			
Rental income	4B	**660**	1,007
Other gains	4C	**145**	490
Total gains		**805**	1,497
Total own-source income		**14,318**	29,062
Net cost of services		**392,505**	384,674
Revenue from Government	4D	**346,181**	329,743
Deficit attributable to the Australian Government		**(46,324)**	(54,931)
OTHER COMPREHENSIVE INCOME			
Changes in asset revaluation surplus		**-**	9,828
Total comprehensive loss attributable to the Australian Government		**(46,324)**	(45,103)

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

STATEMENT OF FINANCIAL POSITION
as at 30 June 2014

	Notes	2014 $ '000	2013 $ '000
ASSETS			
Financial assets			
Cash and cash equivalents		**17,101**	14,217
Trade and other receivables	6A	**200,750**	205,048
Other financial assets	6B	**5,453**	6,178
Total financial assets		**223,304**	225,443
Non-financial assets			
Land and buildings	7A,D	**269,049**	265,258
Property, plant and equipment	7B,D	**84,264**	78,744
Intangibles	7C,E	**26,110**	19,359
Other non-financial assets	7F	**22,641**	14,640
Total non-financial assets		**402,064**	378,001
Total assets		**625,368**	603,444
LIABILITIES			
Payables			
Suppliers	8A	**15,647**	14,026
Lease incentives	8B	**1,674**	2,201
Other payables	8C	**24,813**	20,314
Total payables		**42,134**	36,541
Provisions			
Employee provisions	9A	**56,537**	58,086
Restoration obligations	9B	**6,088**	10,024
Other provisions		**8,000**	-
Total provisions		**70,625**	68,110
Total liabilities		**112,759**	104,651
Net assets		**512,609**	498,794
EQUITY			
Parent equity interest			
Contributed equity		**614,046**	553,907
Reserves		**17,930**	17,930
Retained surplus (deficit)		**(119,367)**	(73,043)
Total equity		**512,609**	498,794

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

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2014

	Retained earnings		Asset revaluation surplus		Contributed equity/capital		Total equity	
	2014	2013	**2014**	2013	**2014**	2013	**2014**	2013
	$'000	$'000	**$'000**	$'000	**$'000**	$'000	**$'000**	$'000
Opening balance	**(73,043)**	(18,112)	**17,930**	8,102	**553,907**	488,079	**498,794**	478,069
Comprehensive income								
Other comprehensive income	**-**	-	**-**	9,828	**-**	-	**-**	9,828
Deficit for the period	**(46,324)**	(54,931)	**-**	-	**-**	-	**(46,324)**	(54,931)
Total comprehensive income	**(46,324)**	(54,931)	**-**	9,828	**-**	-	**(46,324)**	(45,103)
Transactions with owners								
Contributions by owners								
Equity injection — appropriation	**-**	-	**-**	-	**165**	5,062	**165**	5,062
Departmental capital budget	**-**	-	**-**	-	**59,974**	60,766	**59,974**	60,766
Total transactions with owners	**-**	-	**-**	-	**60,139**	65,828	**60,139**	65,828
Closing balance attributable to the Australian Government	**(119,367)**	(73,043)	**17,930**	17,930	**614,046**	553,907	**512,609**	498,794

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

CASH FLOW STATEMENT
for the period ended 30 June 2014

	Notes	2014 $ '000	2013 $ '000
OPERATING ACTIVITIES			
Cash received			
Appropriations		**411,665**	394,815
Sales of goods and rendering of services		**14,061**	24,092
Net GST received		**15,240**	14,263
Other		**15,549**	3,893
Total cash received		**456,515**	437,063
Cash used			
Employees		**219,049**	213,455
Suppliers		**165,618**	153,587
Section 31 receipts transferred to OPA		**31,030**	29,297
Total cash used		**415,697**	396,339
Net cash from operating activities	10	**40,818**	40,724
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		**840**	729
Total cash received		**840**	729
Cash used			
Purchase of property, plant and equipment		**44,593**	44,753
Purchase of intangibles		**14,346**	10,618
Total cash used		**58,939**	55,371
Net cash used by investing activities		**(58,099)**	(54,642)
FINANCING ACTIVITIES			
Cash received			
Contributed equity		**20,165**	15,360
Total cash received		**20,165**	15,360
Net cash from financing activities		**20,165**	15,360
Net increase (decrease) in cash held		**2,884**	1,442
Cash and cash equivalents at the beginning of the reporting period		**14,217**	12,775
Cash and cash equivalents at the end of the reporting period		**17,101**	14,217

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

SCHEDULE OF COMMITMENTS
as at 30 June 2014

	Notes	2014 $ '000	2013 $ '000
BY TYPE			
Commitments receivable			
Sublease rental income		**632**	985
Net GST recoverable on commitments		**60,085**	62,550
Total commitments receivable		**60,717**	63,535
Commitments payable			
Capital commitments			
Land and buildings	A	**5,411**	-
Property, plant and equipment	A	**587**	3,574
Intangibles		**396**	842
Total capital commitments		**6,394**	4,416
Other commitments			
Operating leases	B	**640,319**	664,555
Other		**18,690**	23,649
Total other commitments		**659,009**	688,204
Net commitments by type		**604,686**	629,085

Commitments are GST inclusive where relevant.

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

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

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

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

  Various arrangements apply to the review of lease payments:

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

SCHEDULE OF COMMITMENTS continued

	Notes	2014 $ '000	2013 $ '000
BY MATURITY			
Commitments receivable			
Operating lease			
One year or less		**632**	985
From one to five years		**-**	-
Total operating lease income		**632**	985
Other commitments receivable			
One year or less		**6,283**	6,134
From one to five years		**20,095**	21,259
Over five years		**33,707**	35,157
Total other commitments receivable		**60,086**	62,550
Total commitments receivable		**60,717**	63,535
Commitments payable			
Capital commitments			
One year or less		**6,394**	4,416
From one to five years		**-**	-
Total capital commitments		**6,394**	4,416
Operating lease commitments			
One year or less		**49,437**	48,608
From one to five years		**220,104**	229,223
Over five years		**370,779**	386,724
Total operating lease commitments		**640,320**	664,555
Other commitments			
One year or less		**15,949**	17,254
From one to five years		**2,740**	6,395
Total other commitments		**18,689**	23,649
Total commitments payable		**665,403**	692,620
Net commitments by maturity		**604,686**	629,085

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

SCHEDULE OF CONTINGENCIES
as at 30 June 2014

	2014 $ '000	2013 $ '000
Contingent liabilities		
Claims for damages or costs	**1,125**	210
Total contingent liabilities	**1,125**	210
Net contingent liabilities	**1,125**	210

Details of each class of contingent liabilities and assets, including those not included above because they cannot be quantified or are considered remote, are disclosed in Note 11: Contingent Liabilities and Assets.

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS for the year ended 30 June 2014

Note 1: Summary of significant accounting policies

1.1 Objective of ASIO

ASIO is an Australian Government-controlled entity. It is a not-for-profit entity. The objective of ASIO is to provide advice, in accordance with the *Australian Security Intelligence Organisation Act 1979*, to ministers and appropriate agencies and authorities, to protect Australia and its people from threats to national security.

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

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

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

1.2 Basis of preparation of the financial statements

The financial statements are general purpose and are required by section 49 of the *Financial Management and Accountability Act 1997.*

The financial statements have been prepared in accordance with:

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

The financial statements have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets and liabilities at fair value. 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 Statement of Financial Position when, and only when, it is probable that future economic benefits will flow to ASIO or a future sacrifice of economic benefits will be required and the amounts of the assets or liabilities can be reliably measured.

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

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

1.3 Significant accounting judgements and estimates

In the process of applying the accounting policies listed in this note, ASIO has made the following judgements, which 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.
- Employee provisions include an estimation component in respect of long-term employee benefits measured at the present value of estimated future cash outflows.

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

1.4 New Australian accounting standards

Adoption of new Australian accounting standard requirements

No accounting standard has been adopted earlier than the application date as stated in the standard. New standards and amendments to standards that were issued prior to the signing of the statement by the Director-General of Security 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 AASB but are effective for future reporting periods are not expected to have a future financial impact on the entity.

1.5 Revenue

Revenue from the sale of goods is recognised when:

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

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

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

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

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

Revenue from government

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

Appropriations receivable are recognised at their nominal amounts.

1.6 Gains

Resources received free of charge

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

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

Sale of assets

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

1.7 Transactions with the government as owner

Equity injections

Amounts appropriated which are designated as 'equity injections' for a year (less any formal reductions) and departmental capital budgets are recognised directly in contributed equity in that year.

Distributions to owners

The FMOs require that distributions to owners be debited to contributed equity unless it is in the nature of a dividend.

1.8 Employee benefits

Liabilities for 'short-term employee benefits' (as defined in AASB 119 Employee Benefits) and termination benefits expected within 12 months of the end of the reporting period are measured at nominal amounts.

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

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

Leave

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

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

The liability for leave has been determined by reference to the work of an actuary as at May 2014. The estimate of present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

Separation and redundancy

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

Superannuation

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

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

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

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

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

1.9 Leases

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

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

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

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

1.10 Fair value measurement

ASIO deems transfers between levels of the fair value hierachy to have occurred at the end of the reporting period.

1.11 Cash

Cash is recognised at its nominal amount. Cash and cash equivalents includes:

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

1.12 Financial assets

ASIO classifies its financial assets as 'loans and receivables'. Financial assets are recognised and derecognised upon trade date.

Effective interest method

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

Receivables

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

Impairment of financial assets

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

Financial assets held at cost

If there is objective evidence that an impairment loss has been incurred, the amount of the impairment loss is valued at cost.

1.13 Financial liabilities

ASIO classifies its financial liabilities as 'other financial liabilities'. Financial liabilities are recognised and derecognised upon trade date.

Other financial liabilities

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

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

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

1.14 Contingent liabilities and contingent assets

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

1.15 Acquisition of assets

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

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

1.16 Property, plant and equipment

Asset recognition threshold

Purchases of property, plant and equipment are recognised initially at cost in the Statement of Financial Position, except for purchases costing less than $4000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

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

Revaluations

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 surplus' except to the extent that it reverses a previous revaluation decrement of the same asset class that was previously recognised in the surplus/deficit. Revaluation decrements for a class of assets are recognised directly in the surplus/deficit except to the extent that they reverse a previous revaluation increment for that class.

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

Depreciation

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

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

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

	2014	2013
Buildings on freehold land	**8–60 years**	8–60 years
Leasehold improvements	**lease term**	lease term
Plant and equipment	**2–25 years**	2–21 years

Impairment

All assets were assessed for impairment at 30 June 2014. 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 of disposal and its value in use. Value in use is the present value of the future cash flows expected to be derived from the asset. Where the future economic benefit of an asset is not primarily dependent on the asset's ability to generate future cash flows, and the asset would be replaced if ASIO were deprived of the asset, its value in use is taken to be its depreciated replacement cost.

Derecognition

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

1.17 Intangibles

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

Software is amortised on a straight-line basis over its anticipated useful life. The useful life of ASIO's software is 1–10 years (2012–13: 1–10 years).

All software assets were assessed for indications of impairment as at 30 June 2014.

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
- for receivables and payables.

Note 2: Events after the reporting period

There were no events occuring after reporting date which had an effect on the 2014 financial statements.

On 13 August 2013 the Instrument to Reduce Appropriations (No. 1 of 2013–14) signed by the Minister for Finance and Deregulation took effect. The instrument gave legal standing to the reduction of *ASIO's Appropriation Act (No. 1)* 2012–2013 by $10 226 000. The result of this reduction is reflected in the Statement of Comprehensive Income and Statement of Financial Position. As required by the FMOs, the reduction is not included in Notes 15A Annual Appropriations and 15C Unspent departmental annual appropriations.

The instrument would have the effect of reducing:

- In Note 6A: *Appropriations receivable for existing programs* and the corresponding Trade and Other Receivables in the Statement of Financial Position by $10 226 000.
- In Note 8C: *Payable to Government (appropriation)* and the corresponding *Other Paybles* in the Statement of Financial Position by $10 226 000.
- In Note 15A: *Departmental ordinary annual services* by $10 226 000.
- In Note 15C: *Appropriation Act (No. 1)* 2012–13 by $10 226 000.

if it had been executed in the 2012–13 financial year.

Note 3: Expenses

	2014	2013
	$ '000	$ '000
Note 3A: Employee benefits		
Wages and salaries	**166,121**	164,117
Superannuation:		
Defined contribution plans	**13,070**	13,355
Defined benefit plans	**17,998**	18,219
Leave and other entitlements	**14,436**	13,737
Separation and redundancies	**7,099**	3,647
Total employee benefits	**218,724**	213,075

	2014 $ '000	2013 $ '000
Note 3B: Suppliers		
Provision of goods — related entities	**314**	285
Provision of goods — external entities	**11,457**	6,647
Rendering of services — related entities	**21,218**	22,072
Rendering of services — external entities	**82,402**	80,280
Operating lease rentals — related entities:		
minimum lease payments	**3,879**	3,943
Operating lease rentals — external entities:		
minimum lease payments	**17,027**	17,631
Workers' compensation premiums	**1,614**	1,985
Total supplier expenses	**137,911**	132,843
Note 3C: Depreciation and amortisation		
Depreciation:		
Property, plant and equipment	**24,356**	28,465
Buildings	**17,156**	21,295
Total depreciation	**41,512**	49,760
Amortisation — intangibles — computer software	**7,595**	6,661
Total depreciation and amortisation	**49,107**	56,421
Note 3D: Finance costs		
Unwinding of discount — restoration obligations	**153**	179
Note 3E: Write-down and impairment of assets		
Asset write-downs and impairments from:		
Impairment of receivables	**2**	6,858
Revaluation decrement of property, plant and equipment	**-**	1,622
Write-down of property, plant and equipment	**629**	2,540
Write-down of intangible assets	**-**	38
Total write-down and impairment of assets	**631**	11,058
Note 3F: Losses from asset sales		
Property, plant and equipment		
Proceeds from sale	**(840)**	(729)
Carrying value of assets sold	**1,134**	890
Total losses from asset sales	**294**	161

Note 4: Income

	2014 $ '000	2013 $ '000
OWN SOURCE REVENUE		
Note 4A: Sale of goods and rendering of services		
Provision of goods — related entities	**6**	8
Provision of goods — external entities	**1**	4
Rendering of services — related entities	**13,256**	25,341
Rendering of services — external entities	**250**	2,212
Total sale of goods and rendering of services	**13,513**	27,565
GAINS		
Note 4B: Rental income		
Rental income - operating lease	**660**	1,007
Note 4C: Other		
Resources received free of charge	**120**	115
Other	**25**	375
Total other gains	**145**	490
REVENUE FROM GOVERNMENT		
Note 4D: Revenue from Government		
Appropriation — Departmental appropriations	**346,181**	329,743

Note 5: Fair value measurements

The following tables provide an analysis of assets and liabilities that are measured at fair value. The different levels of the fair value hierarchy are defined below.

Level 1: Quoted prices (unadjusted) in active markets for identical assets or liabilities that the entity can access at measurement date.

Level 2: Inputs other than quoted prices included within Level 1 that are observable for the asset or liability, either directly or indirectly.

Level 3: Unobservable inputs for the asset or liability.

Note 5A: Fair value measurements

Fair value measurements at the end of the reporting period by hierarchy for non-financial assets

	Fair value measurements at the end of the reporting period using			
	Fair value	Level 1 inputs	Level 2 inputs	Level 3 inputs
	$'000	$'000	$'000	$'000
Non-financial assets				
Land	1,565	-	-	1,565
Buildings on freehold land	5,092	-	-	5,092
Leasehold improvements	29,611	-	-	29,611
Other property, plant and equipment	82,644	-	43,946	38,698
Total non-financial assets	**118,912**	**-**	**43,946**	**74,966**
Total fair value measurements of assets in the statement of financial position	**118,912**	**-**	**43,946**	**74,966**
Assets not measured at fair value in the statement of financial position				
Non-financial assets [1]				
Leasehold improvements – work in progress	232,781	-	-	-
Other property, plant and equipment – work in progress	1,620	-	-	-
Intangibles	26,110	-	-	-
Total assets not measured at fair value in the statement of financial position	**260,511**	**-**	**-**	**-**

[1] ASIO did not measure any non-financial assets at fair value on a non-recurring basis as at 30 June 2014.

Fair value measurements

ASIO's assets are held for operational purposes and not held for the purposes of deriving a profit. The current use of the assets is considered the highest and best use.

Note 5B: Level 1 and level 2 transfers for recurring fair value measurements

There have been no transfers between levels of the hierarchy during the year.

The entity's policy for determining when transfers between levels are deemed to have occurred can be found in Note 1.

Note 5C: Valuation technique and inputs for level 2 and level 3 fair value measurements

Level 2 and 3 fair value measurements – valuation technique and the inputs used for assets in 2014

	Category (Level 2 or Level 3)	Fair value $'000	Valuation technique(s) [1]	Inputs used	Range (weighted average) [2]
Non-financial assets					
Land	3	1,565	Market Approach	Price per square metre	(10.00%) - 10.00%
Buildings on freehold land	3	1,361	Market Approach	Price per square metre	(10.00%) - 10.00%
Buildings (specialised)	3	3,731	Depreciated Replacement Cost	Replacement Cost New	N/A
				Consumed economic benefit/ Obsolescence of asset	2.93% - 13.33% (3.29%) per annum
Leasehold	3	29,611	Depreciated Replacement Cost	Replacement Cost New	N/A
				Consumed economic benefit/ Obsolescence of asset	6.67% - 20.00% (10.44%) per annum
Plant and equipment	2	43,946	Market Approach	Adjusted market transactions	N/A
Plant and equipment (specialised)	3	38,698	Depreciated Replacement Cost	Replacement Cost New	N/A
				Consumed economic benefit/ Obsolescence of asset	10.00% - 33.33% (16.97%) per annum

[1] There has been no change to valuation techniques.

[2] Significant unobservable inputs only. Not applicable for assets or liabilities in the Level 2 category.

There were no significant inter-relationships between unobservable inputs that materially affect fair value.

Recurring and non-recurring Level 3 fair value measurements – valuation processes

ASIO procured the services of an appropriately qualified valuer to undertake a materiality review of all non-financial assets as at 30 June 2014. ASIO tests the procedures of the valuation model at least once every 12 months (as obtained at least once every three years). The valuer provided written assurance to ASIO that the models developed are in compliance with AASB 13.

There is no change in the valuation technique since the prior year.

Significant Level 3 inputs used by ASIO are derived and evaluated as follows:

Land and buildings – price per square metre

The market approach utilises market transactions of similar assets to determine fair value. Due to the sensitive nature of the assets within this class, precise locations have not been disclosed. Fair value measurements have been developed based on analysed prices in the asset's general locality. The prices per square metre rates are based on sales evidence and applied using professional judgement.

Buildings (specialised), leasehold, plant and equipment – consumed economic benefit / obsolescence of asset

Assets that do not transact with enough frequency or transparency to develop objective opinions of value from observable market evidence have been measured utilising the depreciated replacement cost approach. Under the depreciated replacement cost approach the estimated cost to replace the asset is calculated and then adjusted to take into account the consumed economic benefit/obsolescence. The consumed economic benefit/obsolescence has been determined based on professional judgement regarding physical, economic and external obsolescence factors relevant to the asset under consideration.

Recurring level 3 fair value measurements – sensitivity of inputs

Land and buildings – price per square metre

The significant unobservable inputs used in the fair value measurement of ASIO's land and buildings asset classes relate to the adopted price per square metre. A significant increase (decrease) in this input would result in a significantly higher (lower) fair value measurement.

Buildings (specialised), leasehold, plant and equipment – consumed economic benefit / obsolescence of asset

The significant unobservable inputs used in the fair value measurement of ASIO's Buildings (specialised), Leasehold and Plant and equipment assets classes relate to consumed economic belefit/obsolescence. A significant increase (decrease) in this input would result in a significantly lower (higher) fair value measurement.

Note 5D: Reconciliation for recurring level 3 fair value measurements

Recurring level 3 fair value measurements – reconciliation for assets

	Non-financial assets				
	Land	Buildings	Leasehold	Plant and equipment (specialised)	Total
	2014	**2014**	**2014**	**2014**	**2014**
	$'000	**$'000**	**$'000**	**$'000**	**$'000**
Opening balance [1]	1,565	5,526	46,028	39,760	92,879
Total gains/(losses) in accumulated depreciation	-	(434)	(16,722)	(14,013)	(31,169)
Purchases	-	-	306	13,132	13,438
Sales	-	-	-	(181)	(181)
Issues	-	-	-	-	-
Settlements	-	-	-	-	-
Transfers into Level 3 [2]	-	-	-	-	-
Transfers out of Level 3 [2]	-	-	-	-	-
Closing balance	1,565	5,092	29,611	38,698	74,966
Changes in unrealised gains/(losses) recognised	-	-	-	-	-

[1] Open balance as determined in accordance with AASB 13.

[2] There have been no transfers between levels of the hierarchy during the year.

ASIO's policy for determining when transfers between levels are deemed to have occurred can be found in Note 1.

Note 6: Financial assets

	2014 $ '000	2013 $ '000
Note 6A: Trade and other receivables		
Goods and services receivables in connection with:		
Related entities	**2,175**	1,406
External entities	**384**	663
Total receivables for goods and services	**2,559**	2,069
Appropriations receivable for existing programs	**195,805**	200,676
GST receivable from the Australian Taxation Office	**2,386**	2,303
Total trade and other receivables (net)	**200,750**	205,048
All receivables are expected to be recovered in no more than 12 months.		
Receivables are aged as follows:		
Not overdue	**199,486**	203,957
Overdue by:		
less than 30 days	**127**	358
31 to 60 days	**75**	149
61 to 90 days	**136**	98
more than 90 days	**926**	486
Total receivables (gross)	**200,750**	205,048
Credit terms for goods and services were within 30 days (2013: 30 days).		
Note 6B: Other financial assets		
Accrued revenue	**5,453**	6,178
All accrued revenue is expected to be recovered in no more than 12 months.		

Note 7: Non-financial sssets

	2014 $ '000	2013 $ '000
Note 7A: Land and buildings		
Land at fair value	**1,565**	1,565
Buildings on freehold land		
fair value	**5,635**	5,635
accumulated depreciation	**(543)**	(109)
Total buildings on freehold land	**5,092**	5,526
Leasehold improvements		
work in progress	**232,780**	212,140
fair value	**50,315**	50,010
accumulated depreciation	**(20,703)**	(3,983)
Total leasehold improvements	**262,392**	258,167
Total land and buildings	**269,049**	265,258

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

Note 7B: Property, plant and equipment

Property, plant and equipment		
work in progress	**1,620**	1,615
fair value	**111,507**	83,706
accumulated depreciation	**(28,863)**	(6,577)
Total property, plant and equipment	**84,264**	78,744

No indicators of impairment were found for infrastructure, plant and equipment.
Property, plant and equipment of an immaterial value only is expected to be sold or disposed of within the next 12 months.

	2014 $ '000	2013 $ '000
Revaluations of non-financial assets		
All revaluations were conducted in accordance with the revaluation policy stated in Note 1. On 31 March 2013, an independent valuer conducted the revaluations.		
Revaluation amounts were:		
Land and buildings – increment transferred to asset revaluation surplus	-	10,441
Property, plant and equipment – decrement transferred to asset revaluation surplus	-	(449)
Property, plant and equipment – decrement expensed	-	(1,622)
Total revaluations of non-financial assets	-	8,370

Note 7C: Intangibles

Computer software		
purchased	**26,743**	21,486
internally developed — in progress	**8,481**	1,831
internally developed — in use	**26,396**	24,606
accumulated amortisation	**(35,428)**	(28,482)
accumulated impairment	**(82)**	(82)
Total computer software	**26,110**	19,359
Total intangibles	**26,110**	19,359

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

Note 7D: Reconciliation of the opening and closing balances of property, plant and equipment

	Land	Buildings	Buildings - leasehold improvement	Property, plant & equipment	Total
	$'000	$'000	$'000	$'000	$'000
2014 **As at 1 July 2013**					
Gross book value	**1,565**	**5,635**	**262,150**	**85,321**	**354,671**
Accumulated depreciation and impairment	**-**	**(109)**	**(3,983)**	**(6,577)**	**(10,670)**
Net book value 1 July 2013	**1,565**	**5,526**	**258,167**	**78,744**	**344,002**
Additions by purchase	**-**	**-**	**20,945**	**31,637**	**52,582**
Depreciation expense	**-**	**(434)**	**(16,722)**	**(24,356)**	**(41,512)**
Disposals – other	**-**	**-**	**-**	**(1,761)**	**(1,761)**
Net book value 30 June 2014	**1,565**	**5,092**	**262,392**	**84,264**	**353,313**
Net book value 30 June 2014 represented by:					
Gross book value	**1,565**	**5,635**	**283,095**	**113,127**	**403,422**
Accumulated depreciation and impairment	**-**	**(543)**	**(20,703)**	**(28,863)**	**(50,110)**
	1,565	**5,092**	**262,392**	**84,264**	**353,313**

	Land	Buildings	Buildings - leasehold improvement	Property, plant & equipment	Total
	$'000	$'000	$'000	$'000	$'000
2013 **As at 1 July 2012**					
Gross book value	1,515	7,746	228,213	126,852	364,326
Accumulated depreciation and impairment	-	(1,192)	(23,587)	(48,073)	(72,852)
Net book value 1 July 2012	1,515	6,554	204,626	78,779	291,474
Additions by purchase	-	-	63,421	33,932	97,353
Revaluations and impairments recognised in other comprehensive income	50	210	10,181	(450)	9,991
Revaluations recognised in the operating result	-	-	-	(1,622)	(1,622)
Depreciation expense	-	(1,239)	(20,056)	(28,465)	(49,760)
Disposals – other	-	-	(4)	(3,683)	(3,687)
Depreciation Adjustment	-	-	-	254	254
Net book value 30 June 2013	1,565	5,525	258,168	78,744	344,002
Net book value 30 June 2013 represented by:					
Gross book value	1,565	5,635	262,150	85,321	354,671
Accumulated depreciation and impairment	-	(109)	(3,983)	(6,577)	(10,669)
	1,565	5,525	258,168	78,744	344,002

Note 7E: Reconciliation of the opening and closing balances of intangibles

	Computer software		
	Internally developed	Purchased	Total
	$'000	$'000	$'000
2014 **As at 1 July 2013**			
Gross book value	**26,437**	**21,486**	**47,923**
Accumulated amortisation and impairment	**(15,503)**	**(13,061)**	**(28,564)**
Net book value 1 July 2013	**10,934**	**8,425**	**19,359**
Additions by purchase or internally developed	**8,738**	**5,609**	**14,347**
Amortisation expense	**(4,159)**	**(3,436)**	**(7,595)**
Net book value 30 June 2014	**15,513**	**10,598**	**26,110**
Net book value 30 June 2014 represented by:			
Gross book value	**34,878**	**26,743**	**61,621**
Accumulated amortisation and impairment	**(19,365)**	**(16,145)**	**(35,510)**
	15,513	**10,598**	**26,110**
2013 **As at 1 July 2012**			
Gross book value	25,205	16,827	42,032
Accumulated amortisation and impairment	(14,669)	(11,923)	(26,592)
Net book value 1 July 2012	10,536	4,904	15,440
Additions by purchase or internally developed	4,618	6,001	10,619
Amortisation expense	(4,220)	(2,441)	(6,661)
Disposals – other	-	(38)	(38)
Net book value 30 June 2013	10,934	8,426	19,359
Net book value 30 June 2013 represented by:			
Gross book value	26,437	21,486	47,923
Accumulated amortisation and impairment	(15,503)	(13,061)	(28,564)
	10,934	8,426	19,359

	2014 $ '000	2013 $ '000
Note 7F: Other non-financial assets		
Prepayments	**22,641**	14,640
Total other non-financial assets	**22,641**	14,640
Total other non-financial assets are expected to be recovered in:		
No more than 12 months	**14,578**	9,290
More than 12 months	**8,063**	5,350
	22,641	14,640

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

Note 8: Payables

Note 8A: Suppliers

Trade creditors and accruals	**15,647**	14,026
Supplier payables expected to be settled within 12 months:		
Related entities	**1,430**	513
External entities	**14,217**	13,513
	15,647	14,026

Settlement is usually made within 30 days.

Note 8B: Lease incentives

Lease incentives	**1,674**	2,201
Lease incentives are expected to be settled in:		
No more than 12 months	**502**	601
More than 12 months	**1,172**	1,600
	1,674	2,201

Note 8C: Other payables

Salaries and wages	**5,710**	4,559
Superannuation	**933**	861
Unearned income	**13,400**	115
Fringe benefits tax	**757**	69
Rent payable	**4,013**	4,484
Payable to Government (appropriation)	**-**	10,226
Total other payables	**24,813**	20,314

	2014 $ '000	2013 $ '000
Rent payable is expected to be settled in:		
No more than 12 months	**503**	478
More than 12 months	**3,510**	4,006
	4,013	4,484
Unearned income is expected to be settled in:		
No more than 12 months	**2,510**	115
More than 12 months	**10,890**	-
	13,400	115

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

Note 9: Provisions

Note 9A: Employee provisions

Leave	**56,206**	57,643
Superannuation	**331**	442
Total employee provisions	**56,537**	58,085
Employee provisions are expected to be settled in:		
No more than 12 months	**41,112**	39,921
More than 12 months	**15,425**	18,164
	56,537	58,085

	2014 $ '000	2013 $ '000

Note 9B: Restoration obligations

Restoration obligations	**6,088**	10,024
Restoration obligations are expected to be settled in:		
No more than 12 months	**2,322**	4,127
More than 12 months	**3,766**	5,897
	6,088	10,024
Carrying amount 1 July 2013	**10,024**	9,979
Additional provisions	**5**	38
Lease expiry	**-**	(336)
Extinguish obligation for restoration	**(4,094)**	-
Revaluations	**-**	164
Unwinding of discount or change in discount rate	**153**	179
Closing balance	**6,088**	10,024

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

	2014 $ '000	2013 $ '000
Reconciliation of cash and cash equivalents as per Statement of Financial Position to cash flow statement		
Cash and cash equivalents as per:		
Cash Flow Statement	**17,101**	14,217
Statement of Financial Position	**17,101**	14,217
Reconciliation of net cost of services to net cash from operating activities:		
Net cost of services	**(392,505)**	(384,674)
Revenue from Government	**346,181**	329,743
Adjustments for non-cash items		
Depreciation/amortisation	**49,107**	56,421
Net write-down of non-financial assets	**629**	2,578
Loss on disposal of assets	**294**	161
Revaluation of property, plant and equipment	**-**	1,622
Revaluation of restoration obligation liabilities	**-**	(164)
Changes in assets/liabilities		
(Increase)/decrease in receivables	**44,109**	29,134
(Increase)/decrease in accrued revenue	**725**	(1,800)
(Increase)/decrease in prepayments	**(8,001)**	863
Increase/(decrease) in employee provisions	**(1,549)**	(781)
Increase/(decrease) in other provisions	**8,000**	-
Increase/(decrease) in restoration obligations	**(3,936)**	45
Increase/(decrease) in lease incentives	**(527)**	(555)
Increase/(decrease) in supplier payables	**(6,208)**	(2,886)
Increase/(decrease) in other payables	**4,499**	11,017
Net cash from/(used by) operating activities	**40,818**	40,724

Note 11: Contingent liabilities and assets

	2014	2013
	$ '000	$ '000

Quantifiable contingencies

The schedule of contingencies reports $1.125m contingent liabilities in respect of claims for damages or costs (2013: $210,000). The amount represents an estimate of ASIO's liability based on precedent in such cases. ASIO is defending the claims.

Contingent liabilities

Balance from previous period	**210**	-
New contingent liabilities recognised	**1,125**	210
Liabilities realised	**(125)**	-
Obligations expired	**(85)**	-
Total contingent liaibilites	**1,125**	210

Unquantifiable contingencies

At 30 June 2014, 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 (2013: Nil).

Significant remote contingencies

ASIO does not have any significant remote contingencies.

Note 12: Remuneration of auditors

	2014 $	2013 $
Financial statement audit services are provided free of charge to ASIO by the Australian National Audit Office. No other services were provided by the Auditor-General.		
Fair value	**120,000**	115,000

Note 13: Senior executive remuneration

Note 13A: Senior executive expense for the reporting period

Short-term employee benefits:		
Salary	**9,853,527**	10,848,113
Motor vehicle and other allowances	**876,899**	913,903
Total short-term employee benefits	**10,730,426**	11,762,015
Post-employment benefits:		
Superannuation	**2,170,662**	2,183,135
Other long-term benefits:		
Annual leave accrued	**788,028**	887,589
Long-service leave accrued	**255,899**	289,391
Termination benefits:		
Voluntary redundancy payments	**631,148**	4,083,979
Total	**14,576,163**	19,206,110

Note 13A excludes acting arrangements and part-year service where total remuneration expensed as a senior executive was less than $195,000.

Note 13B: Average annual reportable remuneration paid to substantive senior executives during the reporting period

Average annual reportable remuneration [1]	Senior executives	Reportable salary [2]	Contributed superannuation [3]	Total [4]
	No.	$	$	$
2014				
Total remuneration:				
$0 to $194,999	**1**	**71,049**	**18,845**	**89,894**
$195,000 to $224,999	**3**	**173,736**	**40,048**	**213,784**
$225,000 to $254,999	**22**	**196,487**	**44,440**	**240,927**
$255,000 to $284,999	**5**	**223,437**	**40,816**	**264,253**
$285,000 to $314,999	**7**	**239,875**	**57,388**	**297,263**
$345,000 to $374,999	**1**	**313,234**	**51,270**	**364,504**
$375,000 to $404,999	**2**	**328,559**	**48,901**	**377,460**
$405,000 to $434,999	**2**	**355,829**	**52,185**	**408,014**
$435,000 to $464,999	**1**	**387,906**	**62,576**	**450,482**
$585,000 to $614,999	**1**	**491,237**	**123,618**	**614,855**
Total	**45**			
2013				
Total remuneration:				
$0 to $194,999	4	214,664	39,021	253,685
$195,000 to $224,999	4	175,908	33,530	209,438
$225,000 to $254,999	21	193,277	48,744	242,021
$255,000 to $284,999	14	219,910	48,908	268,818
$285,000 to $314,999	7	241,820	54,820	296,640
$315,000 to $344,999	4	269,620	56,073	325,693
$345,000 to $374,999	2	314,733	50,253	364,986
$375,000 to $404,999	1	315,307	64,655	379,962
$405,000 to $434,999	1	397,239	32,435	429,674
$555,000 to $584,999	1	446,695	110,067	556,762
Total	59			

[1] This table reports substantive senior executives who received remuneration during the reporting period. Each row is an averaged figure based on head count for individuals in that band.

[2] 'Reportable salary' includes:

- gross payments as per individuals' payment summary (as required by the FMOs; excluding salary sacrificed benefits other than superannuation);
- reportable fringe benefits (as required by the FMOs; not the amount reported on individuals' payment summary, but at the taxable value prior to 'grossing up');
- reportable employer superannuation contributions as per individuals' payment summary (these amounts are salary sacrificed superannuation contributions); and
- exempt foreign employment income (if any).

[3] The contributed superannuation amount is the average cost to ASIO for the provision of superannuation benefits to substantive senior executives in that reportable remuneration band during the reporting period.

[4] There were no reportable allowances or bonuses paid.

Note 13C: Average annual reportable remuneration paid to other highly paid staff during the reporting period

Average annual reportable remuneration [1]	Staff	Reportable salary [2]	Contributed superannuation [3]	Total [4]
	No.	$	$	$
2014 Total remuneration:				
	13	**174,236**	**31,301**	**205,537**
	7	**202,558**	**33,691**	**236,249**
	1	**259,433**	**15,705**	**275,138**
	1	**276,823**	**17,014**	**293,837**
Total	**22**			
2013 Total remuneration:				
	17	167,066	40,087	207,153
	5	188,282	43,231	231,512
Total	22			

[1] This table reports staff:

- who were employed by ASIO during the reporting period;
- whose reportable remuneration was $195,000 or more for the reporting period; and
- were not required to be disclosed in Table B.

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

[2] 'Reportable salary' includes:

- gross payments as per individuals' payment summary (as required by the FMOs; excluding salary sacrificed benefits other than superannuation);
- reportable fringe benefits (as required by the FMOs; not the amount reported on individuals' payment summary, but at the taxable value prior to 'grossing up');
- reportable employer superannuation contributions as per individuals' payment summary (these amounts are salary sacrificed superannuation contributions); and
- exempt foreign employment income (if any).

[3] The contributed superannuation amount is the average cost to ASIO for the provision of superannuation benefits to other highly paid staff in that reportable remuneration band during the reporting period.

[4] There were no reportable allowances or bonuses paid.

Note 14: Financial instruments

	2014 $'000	2013 $'000
Note 14A: Categories of financial instruments		
Financial assets		
Loans and receivables		
Cash	**17,101**	14,217
Trade receivables	**2,559**	2,069
Accrued revenue	**5,453**	6,178
Carrying amount of financial assets	**25,113**	22,464
Financial liabilities		
At amortised cost		
Trade creditors and accruals	**15,647**	14,026
Carrying amount of financial liabilities	**15,647**	14,026

Note 14B: Net gains and losses from financial assets

There is no net gain from financial assets through the profit and loss for the period ending 30 June 2014 (2013: Nil).

Note 14C: Net gains and losses from financial liabilities

There is no net gain or loss from financial liabilities through profit or loss for the period ending 30 June 2014 (2013: Nil).

Note 14D: Fair value of financial instruments

	2014 $'000	2014 $'000	2013 $'000	2013 $'000
	Carrying amount	**Fair value**	Carrying amount	Fair value
Financial assets				
Loans and receivables				
Cash	**17,101**	**17,101**	14,217	14,217
Trade receivables	**2,559**	**2,559**	2,069	2,069
Accrued revenue	**5,453**	**5,453**	6,178	6,178
Total	**25,113**	**25,113**	22,464	22,464
Financial liabilities				
At amortised cost				
Trade creditors and accruals	**15,647**	**15,647**	14,026	14,026

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 Statement of Financial Position.

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.

	2014 $'000	2013 $'000
Financial assets		
Loans and receivables		
Cash	**17,101**	14,217
Trade receivables	**2,559**	2,069
Accrued revenue	**5,453**	6,178
Total financial assets	**25,113**	22,464
Financial liabilities		
At amortised cost		
Trade creditors and accruals	**15,647**	14,026

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

	2014 $'000	2013 $'000	2014 $'000	2013 $'000
	Not past due nor impaired		Past due or impaired	
Loans and receivables				
Cash[1]	**17,101**	14,217	-	-
Trade receivables[2]	**1,295**	977	**1,263**	1,091
Accrued revenue[3]	**5,453**	6,178	-	-
Total loans and receivables	**23,849**	21,372	**1,263**	1,091

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

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

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

Ageing of financial assets that are past due but not impaired:

	0 to 30 days	31 to 60 days	61 to 90 days	90+ days	Total
	$'000	$'000	$'000	$'000	$'000
2014					
Loans and receivables					
Trade and other receivables	**127**	**75**	**136**	**926**	**1,264**
2013					
Loans and receivables					
Trade and other receivables	358	149	98	486	1,091

Note 14F: Liquidity risk

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

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

ASIO manages liquidity risk by ensuring all financial liabilities are paid in accordance with terms and conditions on demand. ASIO's liquidity risk profile has not changed from 2012–13.

The following table illustrates the maturities for financial liabilities.

	On demand	within 1 year	1 to 5 years	> 5 years	Total
	$'000	$'000	$'000	$'000	$'000
2014					
At amortised cost					
Trade creditors and accruals	**-**	**15,647**	**-**	**-**	**15,647**
2013					
At amortised cost					
Trade creditors and accruals	-	14,026	-	-	14,026

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 2012–13. ASIO is not exposed to 'Currency risk', 'Other price risk' or 'Interest rate risk'.

Note 15: Appropriations

Note 15A: Annual appropriations

	Appropriation Act		FMA Act			Appropriation applied	
	Annual appropriation	Appropriations reduced	Section 30	Section 31 (GST excl.)	Total appropriation	(current and prior years)	Variance
	$ '000	$ '000	$ '000	$ '000	$ '000	$ '000	$ '000
2014 Departmental							
Ordinary annual services	**417,024**	**(10,869)**	**2,764**	**31,030**	**439,949**	**(437,478)**	**2,471**
Other services							
Equity	**165**	**-**	**-**	**-**	**165**	**(165)**	**-**
Total Departmental	**417,189**	**(10,869)**	**2,764**	**31,030**	**440,114**	**(437,643)**	**2,471**
2013 **Departmental**							
Ordinary annual services	400,735	-	3,518	29,297	433,550	(460,716)	(27,166)
Other services							
Equity	5,062	-	-	-	5,062	-	5,062
Total Departmental	405,797	-	3,518	29,297	438,612	(460,716)	(22,104)

Note 15B: Departmental capital budgets (recoverable GST exclusive)

	Appropriation Act	Appropriations applied	
	Annual Capital Budget	Payments for non-financial assets	Variance
	$ '000	$ '000	$ '000
2014			
Departmental			
Ordinary annual services			
Departmental Capital Budget	**59,974**	**-**	**59,974**
Total Departmental	**59,974**	**-**	**59,974**
2013			
Departmental			
Ordinary annual services			
Departmental Capital Budget	60,766	(8,360)	52,406
Total Departmental	60,766	(8,360)	52,406

Departmental Capital Budgets are appropriated through Appropriation Acts (No. 1, 3, 5).
They form part of ordinary annual services, and are not separately identified in the Appropriation Acts.

Payments made for non-financial assets include purchases of assets and expenditure on assets which have been capitalised.

Note 15C: Unspent departmental annual appropriations

	2014	2013
	$ '000	$ '000
Appropriation Act (No.1) 2013–14	**160,095**	-
Appropriation Act (No.1) 2012–13	**47,749**	207,952
Appropriation Act (No.2) 2012–13	**5,062**	5,062
Appropriation Act (No.1) 2011–12	**-**	1,879
Total	**212,906**	**214,893**

Note 15D: Disclosure by agent in relation to annual appropriations (recoverable GST exclusive)

	2014		2013	
	DoFD	**DFAT**	DoFD	DFAT
	$ '000	**$ '000**	$ '000	$ '000
Total payments	**17,639**	**8,093**	59,309	11,545

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

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

Note 16: Compensation and debt relief

	2014	2013
	$ '000	$ '000
Compensation and debt relief – Departmental		
Act of Grace payments	**-**	-
Waivers of amounts owing to the Australian Government pursuant to subsection 34(1) of the *Financial Management and Accountability Act 1997*	**-**	-
Payments made under the Compensation for Detriment caused by Defective Administration (CDDA) Scheme	**-**	-
Ex-gratia payments	**-**	-

Note 17: Reporting of outcomes

Expenses		
Departmental	**406,823**	413,736
Income from non-government sector		
Departmental		
Activities subject to cost recovery	**(251)**	(2,216)
Other	**(25)**	(375)
	(276)	(2,591)
Other own-source income		
Departmental	**(14,042)**	(26,471)
Net cost of outcome delivery	**392,505**	384,674

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

Note 18: Net cash appropriation arrangements

	2014 $ '000	2013 $ '000
Total comprehensive income/(loss) plus depreciation and amortisation expenses previously funded through revenue appropriations	**2,783**	11,318
Less depreciation and amortisation expenses previously funded through revenue appropriation	**(49,107)**	(56,421)
Total comprehensive loss as per statement of comprehensive income	**(46,324)**	(45,103)

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

Part 7

APPENDICES AND INDICES

'Let me finish by noting my appreciation and respect for the people across the national intelligence community. The men and women of our national security community work tirelessly to protect our nation—and they are significantly effective at it. They are responsive and flexible. Their abilities to collect and assess information, effectively investigating significant security threats against Australia and Australians, deserve greater acknowledgement.'

David Irvine, Director-General of Security
Security in Government Conference 2013, 13 August 2013

Image: ZRyzner / Shutterstock.com

Appendix A

Agency Resource Statement

	Actual available appropriation for 2013–14 $'000	Payments made 2013–14 $'000	Balance remaining 2013–14 $'000
Ordinary Annual Services			
Departmental appropriation[2]			
Prior year departmental appropriation	195,614 *	137,639	47,749
Prior year departmental appropriation reduction	(10,226)		
Departmental appropriation[1]	417,024 *	263,161	153,863
Departmental appropriation reduction	(10,869)		(10,869)
s31 relevant agency receipts[4]	31,030 *	31,030	-
s30 FMA Act	2,764	2,764	-
Cash on hand		-	17,101
Total ordinary annual services	**625,337**	**434,594**	**207,844**
Other Services			
Departmental non-operating [3]			
Equity injections	5,227	-	5,227
Total other services	**5,227**	**-**	**5,227**
Total net resourcing and payments for ASIO	**630,564**	**434,594**	

[1] Appropriation Bill (No.1) 2013–14 & Appropriation Bill (No. 3) 2013–14

[2] Includes an amount of $47.374m in 2013–14 for the Departmental Capital Budget

For accounting purposes this amount has been designated as 'contributions by owners'

[3] Appropriation Bill (No.2) 2013–14

[4] $17.237m per Portfolio Budget Statement plus $13.793m underestimate at time of PBS

* as per Portfolio Budget Statements

Appendix B

Expenses by Outcomes

	Budget*	Actual Expenses	Variation
	2013–14	2013–14	2013–14
	$'000	$'000	$'000
Outcome 1: To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to Government			
Program 1.1: Security Intelligence			
Departmental expenses			
Departmental appropriation	386,887	406,823	(19,936)
Expenses not requiring appropriation in the Budget year	56,891	49,227	7,664
Total for Program 1.1	**443,778**	**456,050**	**(12,272)**
Total expenses for Outcome 1	**443,778**	**456,050**	**(12,272)**

* as per Portfolio Budget Statements

Appendix C

Mandatory reporting requirements for Questioning Warrants and Questioning and Detention Warrants under section 94 of the *Australian Security Intelligence Organisation Act 1979*

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

Appendix D

Workforce statistics

Table 7: Composition of workforce 2008–09 to 2013–14

	2008–09	2009–10	2010–11	2011–12	2012–13	2013–14
Ongoing full-time (excl. Director-General)	1,452	1,460	1,511	1,546	1,589	**1,490**
Non-ongoing full-time[1]	49	40	50	37	42	**27**
Ongoing part-time	116	134	148	168	193	**204**
Non-ongoing part-time	19	18	16	18	19	**17**
Non-ongoing casual	54	39	42	43	61	**57**
Total	1,690	1,691	1,767	1,812	1,904	**1,795**

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

Table 8: Senior Executive Service–equivalent classification and gender 2008–09 to 2013–14 (does not include the Director-General)

		2008–09	2009–10	2010–11	2011–12	2012–13	2013–14
Band 1	Female	7	6	8	10	8	**8**
	Male	35	35	38	36	27	**25**
Band 2	Female	4	4	4	5	3	**3**
	Male	12	10	10	8	6	**7**
Band 3	Female	0	0	0	0[1]	0[1]	**0[1]**
	Male	2	2	2	1	1	**1**
Total		60	57	62	60	45	**44**

[1] These figures do not include a seconded Band 3.

Table 9: Percentage representation of designated groups within ASIO as at 30 June 2014

Group	Total staff [1]	Women	Non–English speaking background	Aboriginal and Torres Strait Islander	People with a Disability	Available EEO data[2]
SES (excl. DG)	44	11	0	0	1	44
Senior officers[3]	488	185	16	2	6	488
AO5[4]	646	323	51	3	7	639
AO1–4[5]	516	258	26	2	2	509
Information Technology Officers grades 1 and 2	93	14	5	1	3	93
Engineers grades 1 and 2	8	0	0	0	0	8
Total	**1,795**	**791**	**98**	**8**	**19**	**1,781**

[1] Based on staff salary classifications recorded in ASIO's human resource information system

[2] Provision of EEO data is voluntary

[3] Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications

[4] ASIO Officer grade 5 group translates to APS Level 6.

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

Table 10: Percentage of representation of designated groups in ASIO 2008–09 to 2013–14

Group	2008–09	2009–10	2010–11	2011–12	2012–13	**2013–14**
Women[1]	44.6	44.3	44.3	44.3	43.8	**44.1**
Non–English speaking background	5.6	6.9	6.0	5.7	5.8	**5.5**
Aboriginal and Torres Strait Islander	0.2	0.2	0.3	0.4	0.5	**0.4**
People with a disability	1.4	1.2	1.2	1.2	1.3	**1.1**

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

Appendix E

ASIO salary classification structure as at 30 June 2014

ASIO MANAGERS			
SES Band 3	$232,491		minimum point
SES Band 2	$208,888		minimum point
SES Band 1	$170,683		minimum point
AEO3	$126,614		
AEO2	$114,863	to	$126,614
AEO1	$101,283	to	$114,863

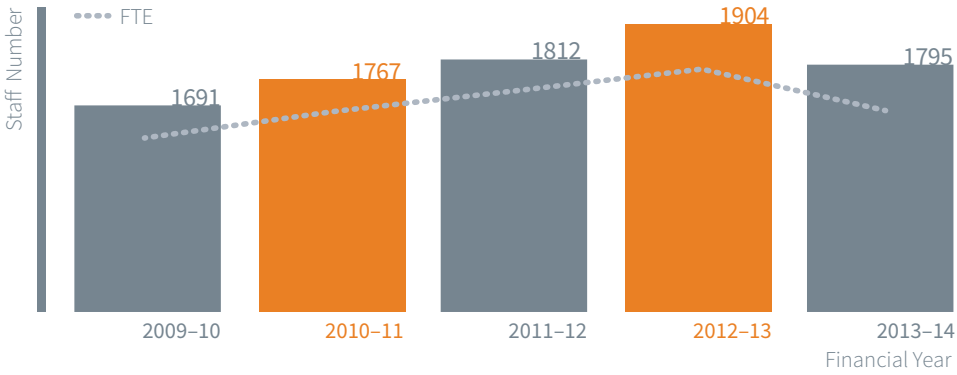
INTELLIGENCE OFFICERS			
IO	$77,337	to	$88,214

ASIO OFFICERS			
ASIO Officer 5	$77,337	to	$88,214
ASIO Officer 4	$63,784	to	$71,694
ASIO Officer 3	$55,623	to	$61,445
ASIO Officer 2	$48,982	to	$54,183
ASIO Officer 1	$43,416	to	$47,859

ASIO ITOs			
SITOA	$126,614		
SITOB	$114,863	to	$126,614
SITOC	$101,283	to	$109,327
ITO2	$77,337	to	$88,214
ITO1	$59,934	to	$69,626

ASIO ENGINEERS			
SIO(E)5	$128,625		
SIO(E)4	$114,863	to	$126,614
SIO(E)3	$101,283	to	$109,327
SIO(E)2	$77,337	to	$88,214
SIO(E)1	$59,934	to	$69,626

ASIO staff numbers 2009–14



Appendix F

Correction of material errors in previous annual report

The following statements in the 2012–13 Report to Parliament are identified as incorrect:

ASIO salary classification structure

On page 121, in Appendix E: ASIO salary classification structure at 30 June 2013, the figures reported for the SES Bands 1 to 3 were effective as at 1 July 2013.

The table below provides the correct information as at 30 June 2013:

ASIO MANAGERS		
SES Band 3	$227,932	minimum point
SES Band 2	$204,792	minimum point
SES Band 1	$167,336	minimum point

Appendix G

Relevance of the images used in the 2013–14 Report to Parliament

The Report to Parliament is one of ASIO's key accountability measures. It is the most significant external publication issued by ASIO each year.

As part of the development of this year's report ASIO held a photography competition and invited all interested staff to submit an image that best represented the theme, 'protecting our way of life'. The winning image was included in this year's report.

Part 1: City

ASIO is responsible for protecting Australia's interests from threats to security. This includes the coordination, management and support for the implementation of ASIO's response to national and international events, both in Australia and overseas. ASIO has dedicated significant focus in this reporting period in support of the government's preparation for the G20 leader's summit in November.

Part 2: Australian industry

ASIO has a proactive, prioritised and targeted outreach program across government and industry designed to build security awareness and resilience. These relationships are integral to ASIO's work in maintaining the security of Australia, its people and its interests.

Part 3: Australian summer at the beach

Australians are friendly democratic decent people and ASIO is committed to protecting the things we value, and our way of life.

Part 4: Travel

ASIO provides security assessments to the Department of Immigration and Border Protection (DIBP) regarding the granting or holding of a visa, and to DFAT in relation to the issuing of a passport. ASIO is also responsible for security assessments on individuals seeking access to designated security-controlled areas (such as airports or ports) or to certain security-controlled substances.

Part 5: Australian passion for sport, culture and events

ASIO provides assessments and advice on security threats to Australian interests at home and abroad, threats to Australian and overseas dignitaries, violent protest threats, threats to diplomatic premises in Australia, threats to critical infrastructure sectors, and threats to major events. The Melbourne Cricket Ground was previously a target under consideration for attack by a terrorist group, a plot jointly disrupted by ASIO and law enforcement agencies.

Part 6: Australia's economic prosperity

Harmful acts of clandestine or deceptive foreign activity against Australian interests continue. ASIO works closely with business, government and key intelligence partners to counter the adverse consequences for Australia's national security posed by espionage.

Part 7: Country

Together with private citizens, business and other government agencies, ASIO works to ensure a secure Australia.

Compliance Index

Description	Requirement	Page
Letter of transmittal	Mandatory	iii
Table of contents	Mandatory	v, vi
Index	Mandatory	131
Glossary	Mandatory	129–130
Contact officer(s)	Mandatory	Back cover
Internet home page address and internet address for report	Mandatory	Back cover
Review by secretary [or equivalent]		
Review by departmental secretary [or equivalent]	Mandatory	vii–ix
Summary of significant issues and developments	Suggested	vii–ix
Overview of department's performance and financial results	Suggested	ix
Outlook for following year	Suggested	Part 1
Significant issues and developments – portfolio	Portfolio departments – suggested	Not applicable
Departmental overview		
Role and functions	Mandatory	xii
Organisational structure	Mandatory	xiii–xiv
Outcome and program structure	Mandatory	x, 10
Where outcome and program structures differ from PB Statements/ PAES or other portfolio statements accompanying any other additional appropriation bills (other portfolio statements), details of variation and reasons for change	Mandatory	Not applicable
Portfolio structure	Portfolio departments – Mandatory	Not applicable
Report on performance		
Review of performance during the year in relation to programs and contributions to outcomes	Mandatory	Part 2
Actual performance in relation to deliverables and Key Performance Indicators set out in Portfolio Budget Statements/Portfolio Additional Estimates Statements or other portfolio statements	Mandatory	Part 2
Where performance targets differ from the PBS/PAES, details of both former and new targets, and reasons for the change	Mandatory	Not applicable
Narrative discussion and analysis of performance	Mandatory	Part 2

Description	Requirement	Page
Report on performance continued		
Trend information	Mandatory	Throughout
Significant changes in nature of principal functions/services	Suggested	Not applicable
Performance of purchaser/provider arrangements	If applicable, suggested	Not applicable
Factors, events or trends influencing departmental performance	Suggested	Part 1
Contribution of risk management in achieving objectives	Suggested	52
Social inclusion outcomes	If applicable, mandatory	Not applicable
Performance against service charter—customer service standards, complaints data, and the department's response to complaints	If applicable, mandatory	38, 47, 59–60
Discussion and analysis of the department's financial performance	Mandatory	Part 6
Discussion of any significant changes from the prior year, from budget or anticipated to have a significant impact on future operations	Mandatory	ix
Agency resource statement and summary resource tables by outcomes	Mandatory	116
Management and accountability **Corporate governance**		
Agency heads are required to certify that their agency complies with the Commonwealth Fraud Control Guidelines	Mandatory	iii
Statement of the main corporate governance practices in place	Mandatory	50–52
Names of the senior executive and their responsibilities	Suggested	–
Senior management committees and their roles	Suggested	50–52
Corporate and operational planning and associated performance reporting and review	Suggested	52
Approach adopted to identifying areas of significant financial or operational risk	Suggested	52
Policy and practices on the establishment and maintenance of appropriate ethical standards	Suggested	
How nature and amount of remuneration for SES officers is determined	Suggested	103

Description	Requirement	Page
External scrutiny		
Significant developments in external scrutiny	Mandatory	36–40
Judicial decisions and decisions of administrative tribunals	Mandatory	19–21
Reports by the Auditor-General, a parliamentary committee or the Commonwealth Ombudsman	Mandatory	Not applicable
Management of human resources		
Assessment of effectiveness in managing and developing human resources to achieve departmental objectives	Mandatory	53–59
Workforce planning, staff turnover and retention	Suggested	53–56
Impact and features of enterprise or collective agreements, individual flexibility arrangements (IFAs), determinations, common-law contracts and AWAs	Suggested	59
Training and development undertaken and its impact	Suggested	56, 58
Work health and safety performance	Suggested	60–61
Productivity gains	Suggested	–
Statistics on staffing	Mandatory	119–122
Enterprise or collective agreements, IFAs, determinations, common-law contracts and AWAs	Mandatory	59
Performance pay	Mandatory	Not applicable
Assessment of effectiveness of assets management	If applicable, mandatory	64
Assessment of purchasing against core policies and principles	Mandatory	64
The annual report must include a summary statement detailing the number of new consultancy services contracts let during the year; the total actual expenditure on all new consultancy contracts let during the year (inclusive of GST); the number of ongoing consultancy contracts that were active in the reporting year; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST). The annual report must include a statement noting that information on contracts and consultancies is available through the AusTender website.	Mandatory	64
Absence of provisions in contracts allowing access by the Auditor-General	Mandatory	Not applicable
Contracts exempt from the AusTender	Mandatory	64
Financial statements	Mandatory	Part 6

Description	Requirement	Page
Other mandatory information		
Work health and safety (Schedule 2, Part 4 of the *Work Health and Safety Act 2011*)	Mandatory	60–61
Advertising and market research (section 311A of the *Commonwealth Electoral Act 1918*) and statement on advertising campaigns	Mandatory	56
Ecologically sustainable development and environmental performance (section 516A of the *Environment Protection and Biodiversity Conservation Act 1999*)	Mandatory	62–63
Compliance with the agency's obligations under the *Carer Recognition Act 2010*	If applicable, mandatory	Not applicable
Grant programs	Mandatory	Not applicable
Disability reporting—explicit and transparent reference to agency-level information available through other reporting mechanisms	Mandatory	120
Information Publication Scheme statement	Mandatory	Not applicable
Spatial reporting—expenditure by program between regional and non-regional Australia	If applicable, mandatory	64
Correction of material errors in previous annual report	If applicable, mandatory	Not applicable
Agency resource statements and resources for outcomes	Mandatory	116
List of requirements	Mandatory	Appendix

Additional ASIO reporting requirements (under the ASIO Act)

Description	Requirement	Page
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	Mandatory	136
The total warrants issued during the year under that Division	Mandatory	136
The total number of warrants issued during the year under section 34E and the total of all those hours for all those persons	Mandatory	136
The following numbers: ▸ The number of hours each person appeared before a prescribed authority for questions under warrant issued during the year under section 34G ▸ The number of hours each person spent in detention under such a warrant ▸ The total of all those hours for all those persons	Mandatory	136
The number of times each prescribed authority had persons appear for questioning before him or her under warrants issued during the year	Mandatory	136

Glossary

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
ANAO	Australian National Audit Office
ANU	Australian National University
ANZCTC	Australia and New Zealand Counter-Terrorism Committee
APS	Australian Public Service
AQAP	al-Qa'ida in the Arabian Peninsula
ASD	Australian Signals Directorate
ASIC	Aviation Security Identification Card
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
BLU	Business Liaison Unit
COAG	Council of Australian Governments
CTCC	Counter Terrorism Control Centre
DFAT	Department of Foreign Affairs and Trade
DIBP	Department of Immigration and Border Protection
DIS	Defence Intelligence Security
EMS	Environmental Management System
FOI Act	*Freedom of Information Act 1982*
G20	Group of Twenty
GST	goods and services tax
IDP	Intelligence Development Program
IGIS	Inspector-General of Intelligence and Security
INSLM	Independent National Security Legislation Monitor
ISA	*Intelligence Services Act 2001*
JCTT	Joint Counter Terrorism Team
MSIC	Maritime Security Identification Card
NAA	National Archives of Australia

NiTAC	National Interception Technical Assistance Centre
NSW CCA	New South Wales Criminal Court of Appeal
NTAC	National Threat Assessment Centre
PGPA Act	*Performance and Accountability Act 2013*
PID Act	*Public Interest Disclosure Act 2013*
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PMC	Department of the Prime Minister and Cabinet
PSPF	Protective Security Policy Framework
PSRR	Protective Security Risk Review
SCEC	Security Construction and Equipment Committee
SEEPL	Security Equipment Evaluated Product List
SSAN	security-sensitive ammonium nitrates
SSBA	security-sensitive biological agents
WHS Act	*Work Health and Safety Act 2011*

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Contact and internet details

Written enquiries

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

General enquiries

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

Media enquiries

Tel: (02) 6249 8381
Fax: (02) 6262 9547

Website

www.asio.gov.au

Report a threat

National Security Hotline

Tel: 1800 123 400
Email: hotline@nationalsecurity.gov.au

State and territory offices

Australian Capital Territory	(02) 6249 6299
New South Wales	(02) 8904 0251
Northern Territory	(08) 8981 2374
Queensland	(07) 3831 5980
South Australia	(08) 8223 2727
Tasmania	1800 020 648
Victoria	(03) 9654 8985
Western Australia	(08) 9221 5066

Supplementary information

The *ASIO Strategic Plan 2013–16* provides further information on the activities and management of ASIO, and is available on the ASIO website.