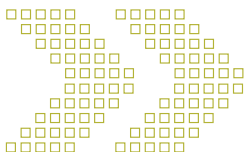
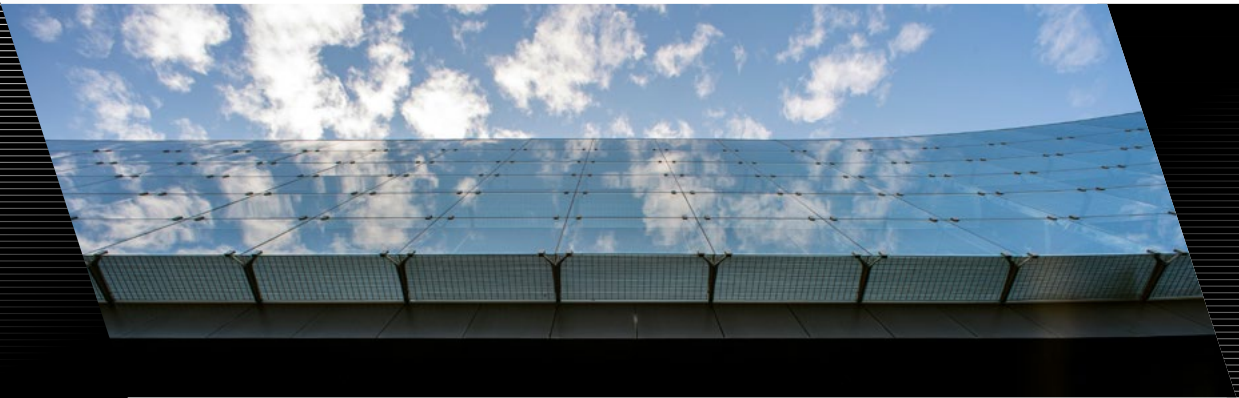




Australian Government

Australian Security
Intelligence Organisation

ASIO Report to Parliament 2014–2015



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

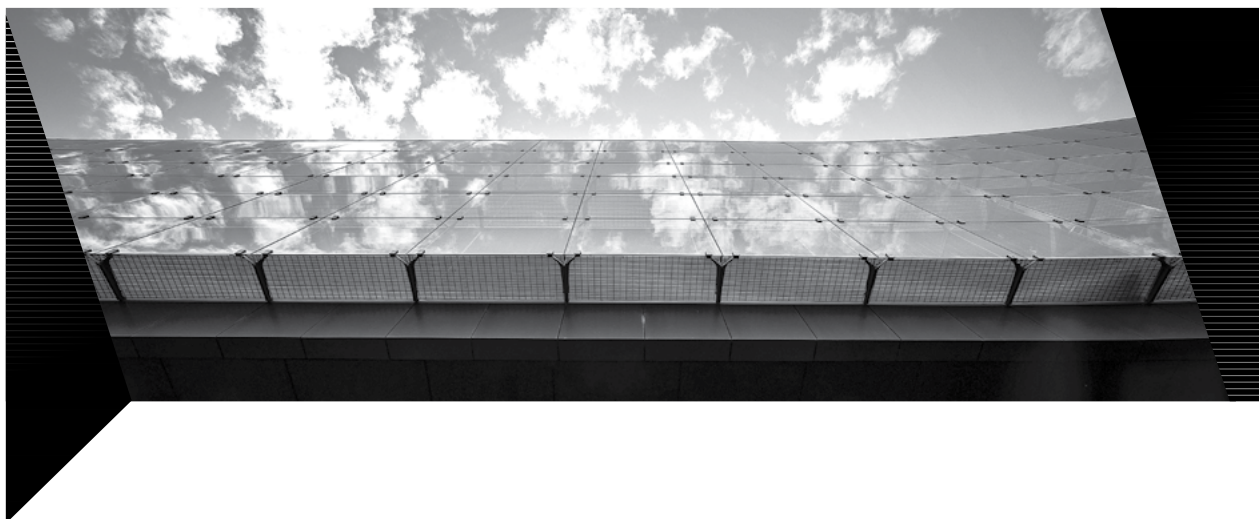
Being responsible for what we do and for our outcomes.
Being accountable to the Australian community through the government and the parliament.

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

2014–2015



ISSN 0815-4562 (print)
ISSN 2204-4213 (online)

© Commonwealth of Australia
(Australian Security Intelligence Organisation) 2015



All material presented in this publication is provided under a Creative Commons (CC) BY Attribution 3.0 Australia Licence (<http://creativecommons.org/licenses/by/3.0/au/deed.en>).

The details of the relevant licence conditions are available on the Creative Commons website (<http://creativecommons.org/licenses/>) as is the full legal code for the CC BY Attribution 3.0 Australia Licence (<http://creativecommons.org/licenses/by/3.0/legalcode>).

Commonwealth Coat of Arms

The Commonwealth Coat of Arms is used in accordance with *Commonwealth Coat of Arms: information and guidelines*, provided by the Department of the Prime Minister and Cabinet, dated November 2012, viewed 22 July 2014, (http://www.dpmc.gov.au/guidelines/docs/CCoA_guidelines.pdf).

Image use

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 inviting staff to submit images evocative of Australia. The winning image was included in this year's report.



Australian Government

Australian Security
Intelligence Organisation

24 September 2015

Director-General of Security

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

Dear Attorney,

In accordance with section 94 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), I am pleased to present to you ASIO's Annual Report for the year ending 30 June 2015.

As required by the ASIO Act, a copy of the *Report to Parliament 2014-2015* – 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 placed appropriate fraud control mechanisms that meet the organisation's needs and comply with the guidelines.

Yours sincerely,
Duncan Lewis

Duncan Lewis

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

FOI WARNING:
Exempt document under
Freedom of Information Act 1982
Refer related FOI requests to
Attorney-General's Department, Canberra.



Table of contents

Director-General's review	vii
The year at a glance	xiii
Guide to the report	xiv
ASIO's role and functions	xv
Organisational structure	xvi

Part 1

The security environment and outlook.....	1
Terrorism	2
Espionage and clandestine foreign interference	7
Communal violence and violent protest	9
Border integrity	12

Part 2

Program performance.....	13
Outcome 1	14
Security intelligence analysis and advice	15
Protective security advice	26
Security intelligence investigations and capabilities	29
Foreign intelligence collection in Australia	34

Part 3

Outcomes and highlights	35
--------------------------------------	-----------

Part 4

ASIO and accountability.....	39
Attorney-General	40
Parliamentary oversight	41
Independent oversight	44
Legal assurance and capability protection	47
Internal audit and fraud control	52
Security in ASIO	54

Part 5

Corporate management 55

Corporate strategy and governance 56

People 62

Property 70

Financial services 72

Information and technology services 73

Part 6

Financial statements 75

Part 7

Appendices and indices 117

Appendix A 118

Appendix B 119

Appendix C 120

Appendix D 121

Appendix E 123

Appendix F 124

Appendix G 125

Additional ASIO reporting requirements under the
Australian Security Intelligence Organisation Act 1979 128

Abbreviations 129

Glossary 131

Index 132



Director-General's review

This *Report to Parliament* is my first as the Director-General of Security. Since my appointment I have been impressed by the professionalism and commitment of the officers of ASIO. I come to the position as Australia faces a most challenging and complex security environment.

During this reporting period ASIO has continued its demanding job of identifying and investigating threats to Australia and Australians wherever they may be. ASIO operates as a security intelligence service and we continue to work in strict accordance with the *Australian Security Intelligence Organisation Act 1979*, other legislation which applies to the organisation, and within a thorough and comprehensive accountability and oversight framework.

Terrorism is the most obvious and immediate challenge, it poses a direct and ongoing threat to the safety and wellbeing of our people. In particular, the threat is associated with violent extremist ideologies that have aims hostile to Australia's interests. It requires a coordinated, considered and comprehensive response.

Espionage and foreign interference directed against Australia by foreign powers also present a first order challenge. While the impact of such activity might not be as obvious to our community as that of terrorism, it has the potential to undermine our sovereignty. It can impact our ability to further our national interests and to defend ourselves against others.

Sitting under these major threats, and sometimes connected to them, are ongoing issues of communal violence, violent protest and other activities that can affect the safety or wellbeing of Australians. ASIO's role is to identify and understand these threats and issues. ASIO provides intelligence and advice to help government manage threats while ensuring that, in protecting Australians' democratic freedoms, those freedoms are not themselves infringed.

Terrorism

Never before has terrorism been such a direct and immediate threat to our nation and our people. ASIO's counter-terrorist efforts are operating at a high tempo. The resourcing required to manage this ever-increasing workload is significant. Despite our most strenuous efforts there can be no absolute guarantee that every threat can be identified and mitigated.

The Syrian and Iraq conflict continues to play directly into the terrorism threat to Australia. An increasing number of Australians offshore are participating in the conflict, and it is unlikely we know the identities of all who are fighting or who have participated in the conflict. Some foreign fighters have returned and others have expressed interest in returning to Australia. While the question of prosecution of returning foreign fighters is a matter for law enforcement, ASIO's interest is in assessing the threat they might present should they return.

A number of Australians are actively supporting violent extremist groups in Syria and Iraq from Australia—providing funding, recruiting for them and facilitating the travel of others to join the conflict.

In September 2014, the Terrorism Public Alert Level was elevated by the Australian Government from Medium to High, reflecting ASIO's assessment of the terrorist threat in Australia. This was the first increase of the alert level since it was introduced following the September 11 attacks in the United States.

Two terrorist attacks occurred in Australia during the reporting period. The first attack, which took place in Melbourne on 23 September 2014 (the Endeavour Hills police station attack) resulted in the injury of two police officers and the death of the attacker. The second, which occurred in Sydney on 15–16 December 2014 (the Lindt Café siege in Martin Place), resulted in the deaths of two hostages and the hostage taker. In addition, and in the same reporting period, six separate terrorist plots were disrupted. Each of the six disrupted terrorist plots was initially identified and investigated by ASIO, prior to being handed over to law enforcement.

These Australian attacks, or planned attacks, come against a backdrop of global terrorist activity. Internationally, similar relatively crude lone-actor attacks are becoming all too common. The United Kingdom, Canada, Denmark, France, Belgium, Libya, Kenya, Tunisia and the United States have all been targeted. We must not, however, leap to the conclusion that this mode of terrorism has replaced the threat of larger scale and more organised attacks. Unsophisticated attacks add another, more readily realised strand to the ongoing threat. The old and more sophisticated threats persist. Importantly threats do not originate from a single source: terrorist threats emanate from Australia, from the Middle East, Africa, Europe, South Asia and South-East Asia.

While the rapid growth and capability of the Islamic State of Iraq and the Levant (ISIL) has brought new energy and urgency to the violent extremist agenda, other jihadist groups such as al-Qa'ida and al-Qa'ida in the Arabian Peninsula (AQAP) remain a threat to the West. Importantly, lone-actor attacks have long been advocated by a variety of terrorist organisations, including al-Qa'ida and AQAP. The military-styled activities and appalling atrocities of ISIL in Syria and Iraq have captured the attention of the world, but ISIL is not the sole focus of the terrorist threat. Other violent extremist organisations—groups that are not affiliated with either al-Qa'ida or ISIL but that share a willingness to use violence to achieve their objectives—are also active and have links to Australia. Politically motivated violence from sources other than violent extremists also persists, occasionally involving Australians or touching on Australia's interests.

Since the alert level in Australia was elevated, the factors contributing to the assessment that we face an increased threat have persisted. When describing the global security environment, the Hon. James Clapper, the US Director of National Intelligence, stated that 'unpredictable instability is the new normal'. In 2014, there were 13 000 terrorist attacks around the world, resulting in 32 727 fatalities—the highest rate of attacks since records were first kept 45 years ago. Locally we have seen actual and planned attacks, ongoing growth in the numbers attracted to the violent extremist cause, and active encouragement from overseas for attacks to be conducted in Australia. More than ever, violent extremist groups and individuals see Australia as a legitimate target for a terrorist attack.

Recruiters for violent extremist groups are always seeking—and finding—new would-be violent extremists. This includes some who wish to travel overseas to join terrorist organisations or have aspirations to undertake attacks in Australia. Some who have been prevented from travelling overseas to engage in terrorist activity have refocused their attack efforts on Australia. Several Australians involved in disrupted attack plans already had their passports cancelled to prevent them from travelling to Syria or Iraq.

The steady stream of new recruits poses a significant challenge. It means individuals who are already known to authorities or whose passports have been cancelled are not the only ones who pose a credible threat. Perhaps the most alarming trend is that the age of the individuals targeted is becoming younger. Recruiters are increasingly using social media to actively groom young people who are more vulnerable to these advances. In some cases children in their early teens are being groomed and recruited.

The increase in frequency of lone-actor attacks by hitherto unknown individuals using easily obtained weapons demonstrates the adaptability of violent extremists. These terrorists constantly adjust their methods to combat our evolving response. In this respect, they have been aided by the continuing emergence of new and readily available technologies—with the internet and mobile communications being two good examples. This means new ways of understanding, investigating and combating threats must be added to the capability of ASIO.

Notwithstanding the strenuous and resolute action in legislative amendment, resource allocation and capability development, neither the government nor ASIO can provide the whole solution to the terrorist threat. I have previously stated that families and local communities have a greater role to play, particularly in cases where young people are involved. Security and law enforcement agencies need assistance from the families and carers of these individuals to keep them out of harm's way. This issue has become as much a social phenomenon as a security one. Countering terrorism is increasingly a whole-of-society concern, and it requires a coordinated, whole-of-society response. Of note is the effort currently being placed on countering violent extremism by the Australian community.

Counter-espionage

The threat from espionage and foreign interference in or against Australia continues to be challenging and remains a major focus for ASIO. It is a fact of life that some nations seek to advantage themselves over other nations, using clandestine, deceptive or illegal means. We are aware of a constant array of foreign intelligence activity directed against Australian interests here and around the world. While mostly these activities, and ASIO's efforts to counter them, necessarily remain secret and outside public view, the actual and potential harm caused to Australia should not be underestimated.

One component of ASIO's work in countering espionage threats that has become a growing priority is collaboration with other government agencies and the commercial sector. ASIO is working with both sectors to build awareness of the nature of the espionage threat to Australia from hostile entities. A further area of concern is of course cyber security, where ASIO continues to play a significant role. During the reporting period, ASIO contributed to Australia's defences against covert actions by foreign powers, including completing 23 073 personnel security assessments of people proposed to be given access to Australian national security classified material.

Resourcing and capabilities

ASIO's budget and resourcing have come under growing pressure over the last few years as a result of a significant increase in the number of security investigations and also rising costs of doing business. The increase in investigations is, in part, due to the Syrian conflict, but increases have also been seen in espionage and cyber investigations.

The Foreign Fighters New Policy Proposal funding that ASIO was allocated in 2014 will bring \$196.8 million over four years, consisting of \$139.7 million in operating funding and \$57.1 million in capital funding. At the end of this reporting period, ASIO employed 1715.5 full-time equivalent staff. Through this additional resourcing, and over those four years, ASIO will recruit a further 326 staff, of which 314 will be ongoing. The increase in staff numbers led ASIO to consider necessary structure adjustment—decisions were made in the reporting period to undertake this work, with the adjustment to be realised during the 2015–16 financial year.

Budget supplementation is integral to ASIO increasing its capability to perform its functions, but it is not the whole story. Two other critical components are our ability to attract staff with the requisite skills, abilities and qualities; and our ability to adapt in a world of constantly changing and evolving technologies. ASIO's information and technical capabilities require constant updating as technology changes and the type of work required of them evolves.

To maintain our capability, we also have to constantly update the legislative framework that enables us to use that technology. To fail to do so would leave us lagging behind our adversaries and the threat they present.

Legislation

The suite of legislative reforms undertaken by the Australian Government over the reporting period has helped ensure that national security laws better address the challenges Australia faces. Some of these reforms were responses to changes in the threat environment or directed towards improving the ability of government agencies to collaborate and cooperate. Others were intended to allow ASIO and other agencies to maintain existing capabilities that had been compromised by changes in technology.

ASIO has utilised the new provisions introduced through legislative reform, and the new measures have already contributed to some major investigations, including the disruption of attack plans. For example, and as already mentioned, ASIO has issued warrants using its updated warrant powers, including the amended computer access and surveillance devices warrants and the new 'identified person' warrants. Since the power came into force on 1 December 2014 and during this reporting period, I have recommended to the Minister for Foreign Affairs the suspension (or temporary surrender) of travel documents belonging to nine Australians to prevent them from travelling to join violent extremist groups.



A new home for ASIO

In March 2015, the headquarters of ASIO moved to the new Ben Chifley Building. This wonderful new building will serve as a launching platform for our operations for many years to come, and the positive impact it is having on both the efficiency and effectiveness of our operations is already apparent.

Outlook

Australia faces ongoing threats of terrorism and clandestine foreign activity. The impact of the conflict in Syria and Iraq will be felt in Australia for many years to come. Clandestine foreign targeting of Australian government and business information will also persist, as will the threat from the actions of malicious insiders. Australia's defence must be multidimensional and will include raising awareness of the consequences for individuals who betray the trust associated with access to highly sensitive government information.

I would like to conclude by acknowledging the work being undertaken by ASIO employees, sometimes at personal risk to themselves. These men and women are working tirelessly to keep our community safe. While none of us can guarantee the outcome, I can attest that they are making every effort possible to reduce the risk.

In addition, I would like to acknowledge ASIO's partner organisations both within Australia and overseas—government and private sector alike. The cooperation being demonstrated by all agencies within the Australian Intelligence Community, state and territory law enforcement, and the private sector—and extending to our overseas partners—has not before been as close and effective as is currently the case.

Finally, I would like to thank the Australian people for the support given to ASIO. It is a challenging time in the global and domestic security environment—the support and reporting provided by all Australian communities remains vital in our coordinated effort to protect our country.

Duncan Lewis
Director-General of Security



The year at a glance

OUTCOMES AND ACHIEVEMENTS

During the reporting period, ASIO:

- ▶ Provided advice to government which led to an elevation of the Terrorism Public Alert Level from Medium to High.
- ▶ Initiated and continued security investigations into terrorism, espionage, foreign interference, communal violence and border integrity threats.
- ▶ Investigated two terrorist attacks and actively engaged in thwarting six other planned attacks in Australia.
- ▶ Managed an increased counter-terrorism case load—from 200 to 400 higher-priority investigations since the previous reporting period.
- ▶ Issued adverse security assessments in relation to 93 passports (compared to 45 in 2013–14).
- ▶ Further issued the following security assessments:
 - ▶ 17 628 visa security assessments
 - ▶ 171 203 counter-terrorism security assessments
 - ▶ 23 073 personnel security assessments.
- ▶ Provided assistance and advice in relation to over 50 litigation matters.
- ▶ Completed 811 requests for ASIO records, requiring 52 829 pages to be examined.

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* (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 Commonwealth Parliament, 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. It allows ASIO to share information with the parliament and public.

Part

The Overview provides the Director-General of Security's review of the 2014–15 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. This part informs the Parliament of Australia about the performance of ASIO against the outcomes and deliverables set out in the Portfolio Budget Statements 2014–15.

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 Commonwealth.

4

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

5

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

6

Part 6 details ASIO's audited financial statements for the 2014–15 financial year.

7

Part 7 is a set of appendixes and indexes 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, Australian Government agencies, 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 also responsible for providing security advice in the form of security assessments to government agencies to inform their decision making in relation to prescribed administrative action, including:

- ▶ people seeking entry to Australia
- ▶ people seeking access to classified material and designated security-controlled areas
- ▶ people seeking access to hazardous chemical substances regulated by licence.

Section 17(1)(e) of the ASIO Act also authorises ASIO to obtain foreign intelligence within Australia, including 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

UNCLASSIFIED organisational structure as at 30 June 2015.



Duncan Lewis
DIRECTOR-GENERAL OF SECURITY

DEPUTY DIRECTOR-GENERAL

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

INTERNAL AUDIT

DEPUTY DIRECTOR-GENERAL

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



Part 1

THE SECURITY ENVIRONMENT AND OUTLOOK

ASIO's security intelligence remit is defined by reference to a set of activities that could or would cause harm if directed against Australia, Australians and countries to which Australia has international obligations. ASIO is to identify, investigate, assess and advise on those activities wherever they might occur in the world: its remit is not limited to Australia. Almost all security threats that Australia and Australians face have their origin in, or are linked to, events, people and organisations overseas. Therefore, the security environment described is global, albeit with a strong focus on what is happening in Australia.

Terrorism

The principal terrorist threat to Australia, Australians and Australian interests continues to come from those who adhere to a violent extremist ideology. This ideology is associated with a range of groups that share the single ultimate objective of driving 'apostates' and non-Muslims from Muslim lands and establishing an Islamic state ruled in accordance with their deviant interpretation of Islam. At times these groups are also rivals, seeking to lead and dominate the violent extremist cause. These groups include al-Qa'ida and its affiliates, and the Islamic State of Iraq and the Levant (ISIL). ISIL is separate from, and 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 against the citizens and interests of those countries are not only legitimate but also obligatory.

While the public profile of some groups has waned with the high level of attention garnered by ISIL, multiple groups continue to maintain a high degree of intent and capability, including the capacity to effect or direct a large-scale, complex attack. Al-Qa'ida and its affiliates maintain the desire to strike at the West, and Australia continues to be identified in their propaganda as a legitimate target and location for attack.

The terrorist threat to Australia both domestically and overseas has increased over the past year. On 12 September 2014, the former Director-General of Security, Mr David Irvine AO, increased Australia's general terrorism threat level to High, meaning a terrorist attack was assessed as likely. For the first time, this level was declassified to ensure the public had as much relevant advice as possible. The same day, based on that revised threat level, the Australian Government increased the Terrorism Public Alert Level from Medium to High.

The initial raising of the general terrorism threat level was not in response to any intelligence of specific terrorist attack planning. Rather, it took into account a range of factors, including an increasing number of individuals adopting a violent extremist ideology; more profound and specific discussion among violent extremists of attack planning; encouragement from and direction by violent extremists in Syria and Iraq to conduct terrorist attacks in Australia; and a recognition that the capability required to conduct such attacks was negligible.

Subsequently, two terrorist attacks occurred in Australia and six terrorist plots were disrupted. The first attack took place in Melbourne on 23 September 2014, when Ahmad Numan Haider stabbed uniformed police officers outside the Endeavour Hills police station. The second attack occurred in Sydney on 15–16 December 2014, when Mohammad Hassan Manteghi (also known as Man Haron Monis) took 17 people hostage inside the Lindt cafe in Martin Place. This incident resulted in the deaths of two hostages and Manteghi. Each of the six disrupted terrorist plots was initially identified and investigated by ASIO, prior to being handed over to law enforcement for disruption.

A small minority of people in Australia adhere to a violent extremist ideology. They tend to be linked by informal personal networks rather than through an identifiable, structured or formal terrorist group, although some of these people have personal links to individuals overseas associated with organised terrorist groups. Those links have been used to facilitate radicalisation and recruitment, and to organise the travel of Australians to conflict zones.

A consequence of the conflict in Syria and Iraq has been an increase in the number of Australians drawn to and motivated by the violent extremist narrative, particularly following ISIL's declaration of a caliphate on 29 June 2014. ISIL has been particularly successful in galvanising support through the innovative use of social media.

It has been able to influence and recruit new members, with young males and, to a lesser extent, young females being particularly susceptible. Of particular concern is the resonance of ISIL's social media with teenagers aged 14 to 19. This phenomenon presents a broad challenge. Appropriate and effective interventions in these cases need to be far broader and more sustained than simply a security and law enforcement response. But Australians are not only drawn to ISIL; they are also attracted to other terrorist groups active overseas. ASIO had over 400 higher-priority counter-terrorism investigations at the end of the reporting period—a two-fold increase compared to the previous reporting period.

The number of Australians participating in the conflict in Syria and Iraq increased across the reporting period. At the end of June 2015, ASIO was aware of approximately 120 Australians directly participating in the conflict—a significant increase from the previous reporting period. Most were involved with either ISIL or the Syria-based, al-Qa'ida-linked group Jabhat al-Nusra. Some undertook suicide attacks during the reporting period, including two Australians. Overall, ASIO assesses that at least 25 Australians—and possibly as many as 35 Australians—have been killed fighting in the conflict. In addition, approximately 160 Australians have been identified as actively supporting the conflict from Australia.

ASIO is seeing an unprecedented number of young Australians (aged 20 years or younger) engaging with, or travelling to join, violent extremists active in Syria and Iraq. The reasons young Australians are attracted to ISIL vary; it is likely that they are driven by a number of factors. ISIL's online propaganda includes extremely violent and brutal images, a slickly packaged ideological message calling on 'true believers' to support and defend the caliphate, and an apocalyptic strand implying cosmic significance to ISIL's actions. ISIL's social media effort, which is directly targeted at the young, delivers a constant and insistent message in a form that will appeal to them, and direct contact with radicalisers and radicalised peer groups also plays a significant role.

Over the reporting period, ASIO worked with local and overseas partners to disrupt the travel of would-be extremists, with travel mostly but not entirely related to the conflict in Syria and Iraq. The disruption of travel through such means as passport cancellations is one way Australia meets its international obligation not to export terrorism. Disruption of travel also limits Australian violent extremists' exposure to, and experience of, terrorism overseas, and this can contain their capability and commitment. In 2014–15, legislation was passed allowing ASIO to recommend the temporary suspension of passports and the seizure of travel documents. In the reporting period, ASIO issued 93 adverse security assessments in respect of passports.

ASIO cannot know with any certainty whether individual Australians involved with terrorist groups overseas will pose a terrorist threat in Australia should they return. But past experience suggests that some will—19 of 25 Australians who travelled to fight or train with violent extremist groups in the 1990s were involved in terrorist attack planning within five years of their return. Some of those returning are likely to exhibit a reinforced commitment to violent jihad, including holding greater hostility towards Australia, our way of life, our values and our society. Some will be inured to the use of extreme violence and may have acquired new capabilities—most will have fought with a range of violent extremists from across the globe, building enduring networks. Past experience suggests returnees from the current conflict will present a long-term security issue and some will pose a direct threat to Australian interests both here and overseas.

Some of the Australians who have been prevented, through passport cancellation or other prevention measures, from travelling to the conflict in Syria and Iraq also pose an onshore threat. Some of these thwarted travellers have transferred their focus to onshore activities in support of violent extremist groups in Syria and Iraq—especially ISIL and Jabhat al-Nusra—acting as radicalisers, recruiters and facilitators. A persistent risk is that these individuals will refocus their commitment to violent extremism into planning an attack in Australia, especially if they exhaust their options for travel. Already ASIO has seen that some thwarted travellers have considered undertaking attacks at home using simple weapons and tactics.

While the more likely scenario for any attack in Australia is a low-capability attack against a 'soft' target, perpetrated by a lone actor or a small group—as seen in the two terrorist attacks in Australia—the threat of a complex attack, such as a coordinated mass shooting or a large, sophisticated explosive device, also persists.

The surge in extremist support and activity experienced in Australia has occurred globally. Transnational terrorist groups continue to present a real and credible threat to Australians and Australian interests in other countries. Australians and Australian interests overseas have been the specific targets of attacks or have been caught up in attacks directed against others. As the threat increases globally, the threat to Australians and Australian interests overseas also increases.

Over the past year there has been a marked trend in Western countries towards low-capability attacks inspired by exhortations from ISIL. Many of these attacks were by lone actors who either were unknown to authorities or were on the periphery of investigations; most of the attacks were conducted with little planning or preparation.

The conflict in Syria and Iraq resonated strongly with people in South-East Asia, and there have been large, overt demonstrations in support of ISIL. Hundreds of individuals from South-East Asia have trained and fought with militant groups, including ISIL. These individuals may pose a terrorist threat to Australians and Australian interests, particularly in Malaysia and Indonesia, where strong anti-Australian sentiment among violent extremists endures. Of concern is the potential for South-East Asians fighting

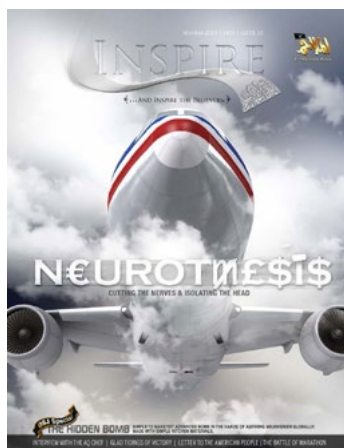
with ISIL to encourage anti-Western attacks in our region. Here, as in other parts of the world, social media is playing an important role in disseminating ISIL propaganda.

In Europe and North America, the security environment also deteriorated over the reporting period, driven largely by the same factors experienced in Australia and evident in a spike of low-capability attacks, disrupted plots and hoaxes. Terrorist attacks included incidents in Canada in October 2014, targeting the military and parliament; in Paris in January 2015, targeting Jewish interests and the media, in particular the satirical magazine *Charlie Hebdo*; in Denmark in February 2015, targeting a free speech event and Jewish interests; and in the United States.

In the Middle East, the security environment remained unstable but deteriorated considerably in Egypt and Yemen. Al-Qa'ida in the Arabian Peninsula (AQAP), Jabhat al-Nusra, and ISIL and its affiliates were responsible for the majority of attacks. Sectarian violence in Syria and Iraq continued unabated. Terrorist groups continued to use tried and tested attack methods, including mass-casualty attacks. In Egypt, violent extremists and revolutionary groups have used violence against primarily Egyptian Government interests, but ASIO remains alert to a potential shift to the deliberate targeting of Western interests.

In Africa, the security environment in the north of the continent also deteriorated. The most prominent groups were Somalia-based al-Shabaab, Nigeria-based Boko Haram, Mali/Algeria-based al-Qa'ida in the Lands of the Islamic Maghreb, and Libya-based militia groups. While ISIL's growing influence was of major concern, al-Qa'ida and locally driven violent extremist groups continued to present the pre-eminent threat. The growing influence of ISIL in Africa was reflected in attacks such as the March 2015 attack on the Bardo Museum in Tunisia, in which an Australian–Colombian national was killed, and the Garissa University attack in Kenya. The kidnapping threat to Westerners remains of particular concern in Africa and the Middle East. The brutal example set by ISIL suggests that kidnap victims are now just as likely to be executed as exchanged for a ransom.

Areas of instability, including Syria, Yemen and Libya, provided permissive environments and conditions for terrorist groups to train members, recruit new members and plan attacks. However, geographic areas are not the only permissive environments for terrorist groups. The internet is a pivotal mechanism through which terrorists communicate, network and disseminate propaganda. Over the reporting period, online terrorist propaganda increased in both volume and sophistication. While difficult to quantify, this increase is likely to have accelerated radicalisation and strengthened already held extremist views. Online propaganda may have also appealed to those with no prior ideological predisposition.



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

Through its Al-Hayat Media Centre, ISIL published a wide range of materials, some in English. It exploited a variety of technologies and featured a small number of Australians. AQAP continued to release its English-language magazine *Inspire*—the highly polished publication remained AQAP's primary method for interaction with Western followers.

Lebanese Hizballah retains a support base in Australia. While Australians have been associated with the group, Hizballah remains focused on supporting the Assad regime in Syria, and there was little security-relevant activity in Australia during the reporting period. Violent rhetoric continued from extreme right-wing and left-wing individuals in Australia; however, acts of violence by either side were rare and largely opportunistic.

More broadly, the terrorism environment is likely to remain fluid and will be affected by nationalist and ethnic tensions, acts of violence overseas and an increased propensity and ability for violence-prone individuals to move to action.

Espionage and clandestine foreign interference

Espionage and other forms of foreign interference are used by many foreign powers to gain information, achieve an advantage, protect or progress their national interests or cause damage to the interests of their adversaries. Clandestine foreign interference activity and espionage against Australian interests is extensive. These activities incorporate a number of techniques and capabilities, including human intelligence, technical collection methods and exploitation of the internet and information technology. Cyber attacks can be used to obtain intelligence or disrupt capability and access.

Competing national interests drive clandestine 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.

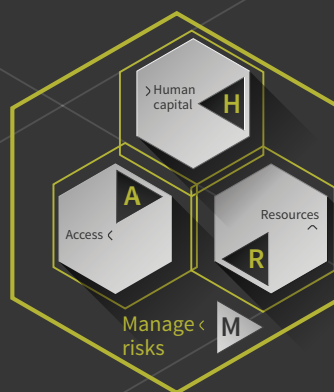
The consequences of espionage and foreign interference are not fixed but will change as circumstances change—as international tensions increase, the stakes tend to become higher. Insofar as Australia can never predict where circumstances might take its relationships, all clandestine foreign activity against Australia must be taken seriously.

ASIO's approach to managing the threat presented by the hostile activities of foreign intelligence services has three key objectives: to discover the most harmful clandestine activity; to degrade its adverse impact on Australia; and to defend against future harmful clandestine activity, including by contributing to security policies and practices. ASIO continues to allocate substantial resources to defensive outreach and advice to heighten awareness of the threat environment and to drive appropriate security policy responses.





HARM



ASIO looks at the espionage and foreign interference threat through the concept of H.A.R.M.—Human capital (H), access (A), resources (R) and managing the risk (M).

- ▶ Foreign intelligence services target people (human capital) who have access to the resources they are interested in, or in an effort to covertly influence them and their activities.
- ▶ Foreign intelligence services seek to generate access to restricted or compartmentalised areas.
- ▶ Foreign intelligence services seek to obtain resources not publicly available to enhance their strategic objectives.
- ▶ Australian Government and industry must seek to understand the threat and translate it into their effective risk management systems and practices to strengthen and protect their organisation from foreign intelligence services and insider threats.

Foreign powers are not only interested in obtaining classified or protected information; any Australian information that is not publicly accessible and might offer an advantage to another country is potentially of value. Foreign espionage activities may be detrimental to Australia's intelligence, scientific, technical and defence capabilities, our economy and trade, and our international relationships.

Foreign interference in Australia by foreign powers is pervasive. It spans community groups, business and social associations and is directed against all levels of Australian Government and the community. 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. ASIO is focused on discovering harmful foreign interference activities to ensure they do not undermine fundamental principles of Australia's democratic freedoms.

In 2014–15, Australian Government and private sector systems experienced an increase in the range, scale and sophistication of hostile cyber activity by foreign state actors. Cyber espionage is attractive to foreign powers because it has the potential to provide access to large aggregations of valuable information and it is easy for the foreign power to deny its involvement. Other forms of hostile cyber activity include accessing and affecting Australia's cyber systems to advantage a foreign power at Australia's expense, as well as cyber sabotage. It is vital that effective security policies and practices are implemented to assist in discovering hostile cyber activities, degrade the impact of these activities on Australian interests and defend against future activities. Together with the Australian Signals Directorate, and the Computer Emergency Response Team in the Attorney-General's Department, ASIO continues to promote awareness of, and defensive responses to, the increasing threat from hostile cyber activity.

Another ongoing threat to Australia's national interests is the risk posed by self-motivated individuals who exploit their privileged access to information to make unauthorised disclosures of classified or privileged information. Such individuals have always been a potential source of harm to Australia's national interests. But the harm these individuals can cause has been greatly increased by modern information technology, which allows large amounts of information to be aggregated and copied, as well as distributed easily to a wide audience. The investigation of actions by individuals who abuse their privileged access to information is complex,

resource-intensive and highly sensitive. ASIO aims to balance an appropriate and proportionate investigative response with individual privacy considerations and the gravity of the potential harm.

It is a fundamental duty of the Australian Government and public servants to preserve and defend the nation's interests. Individuals who have, or have had, access to privileged information have obligations to protect it. It should be noted that ASIO remains focused on unauthorised disclosure, not in preventing individuals from reporting through established mechanisms—including mechanisms established under the *Public Interest Disclosure Act 2013*—what they believe to be wrongdoing and maladministration.

Communal violence and violent protest

Lawful advocacy, protest and dissent are an inherent part of Australia's political and social culture. Most protests are peaceful, and there is little public support for the use of violent or destructive protest tactics. During 2014–15 protests in Australia were mostly peaceful. When violence occurred, it was typically not premeditated and it took place between groups with opposing views on emotive issues. Violence was also used against police attempting to maintain order.

There was increased participation in the activities of Australia-based anti-Islam groups; mostly this was online activity but 'real world' events attracted increased numbers. The conflict in Syria and Iraq, and widespread mainstream and social media coverage of the conflict—in particular, graphic reports of egregious acts—provided a ready stream of material used by anti-Islam activists as evidence that Islam is not compatible with Australian values or the Australian way of life. Anti-Islam groups whose activities were previously mostly limited to online posts and occasional inflammatory publicity stunts began to attract increased numbers to real-world events, such as the Reclaim Australia rallies and the Stop the Mosque protests. The reporting period saw a number of well-attended, coordinated Australia-wide protests with an overt anti-Islam and anti-immigration message; these protests attracted large numbers of supporters and counter-protesters.

Small-scale violence occurred between opposing protesters at the Reclaim Australia rallies in Melbourne in April 2015. Reclaim Australia rallies will continue to be held throughout the next financial year and, due to their potential for violence, will remain of concern. While anti-Islam numbers increased, there was a concurrent increase in counter-protests on platforms of social inclusion, anti-racism and anti-fascism.

In January 2015, members of Sydney's Muslim community and their supporters gathered in a peaceful 'We will not abandon our Prophet' rally organised by Hizb ut-Tahrir, at Sydney's Lakemba train station. The event was held in response to perceptions of anti-Islam sentiment following the terrorist attack on the *Charlie Hebdo* office in Paris. While the event was vocal, it passed without major incident.

Environmental issues, refugee and Indigenous advocacy, animal rights and anti-government policy protests attracted the most significant numbers to protests in 2014–15. While some capital city protests on these issues attracted large, vociferous crowds, most concluded without incident and complied with protest preconditions and directions of police.

The execution of two convicted Australian drug smugglers in Indonesia in late April 2015 prompted small, peaceful vigils outside Indonesian diplomatic facilities in Australia. In late May, letters containing white powder were sent to the Indonesian Embassy in Canberra and three Indonesian consulates in Australia—all letters were assessed as hoaxes.



While some previous Group of Twenty (G20) meetings have been marred by widespread violence and property damage during anti-globalisation and anti-capitalism protests, Australia's G20 hosting commitment—which culminated in the Brisbane Leaders Summit in November 2014—concluded without incident. ASIO assisted the whole-of-government effort through tailored intelligence collection and reporting, the provision of protective security advice to the G20 Taskforce, and the security checking of individuals seeking G20 accreditation. This assistance was aimed at providing forewarning of any potential security-related issues at G20 events and at mitigating any potential threats.

Australia has a low incidence of inter-communal or intra-communal violence, and incidents tend to be in relation to specific local or international events that resonate in Australia and add to or reignite residual communal grievances. In 2014–15 tensions between Sunni and Shia Muslim communities continued but to a lesser extent than in previous years. While this is an enduring issue, and some elements are framing the conflict in Syria and Iraq along sectarian lines, there is little prospect this issue will be a catalyst for wide-scale communal violence.

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 when 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 otherwise coming 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 it already has or which is passed to it by other agencies.

Border integrity

ASIO has contributed to whole-of-government strategies to disrupt and deter people smugglers, including the successful disruption of a sophisticated offshore people-smuggling network responsible for the organisation of multiple illegal maritime ventures to Australia.

The number of people-smuggling ventures and illegal maritime arrivals during the reporting period was very low, continuing the trend from the 2013–14 financial year. The demand among potential illegal immigrants for travel to Australia has fallen. However, Australia's border integrity continues to be challenged by people smugglers, who are motivated by greed. The security environment continues to evolve so that existing and new 'push' factors for illegal travel to Australia will motivate some potential illegal immigrants to consider the risk and expense of an illegal maritime venture to be worthwhile.

ASIO provides staffing for Operation Sovereign Borders and is represented in a number of multi-agency counter-people smuggling groups. During the reporting period, ASIO provided advice to the Australian Government about the threat posed to Australia's territorial and border integrity and security by people smuggling. In addition, ASIO provided information and briefings to support the work of the Australian Government's Independent Reviewer of Adverse Security Assessments, former Federal Court judge the Hon. Margaret Stone, as well as providing support to judicial and administrative reviews of ASIO people smuggling-related security assessments.



Part 2

PROGRAM PERFORMANCE

Outcome 1

ASIO’s appropriation, identified in the 2014–15 Portfolio Budget Statement (PBS), 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.

In 2014–15 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.

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 identify or anticipate emerging national security threats to assist policymakers, decision-makers and responders.

These assessments explore and explain various aspects of the security environment, including ideologies, motivations, patterns of behaviour, events, trends and methodologies. ASIO strategic assessments directly support operational planning, policy development and resource management to help plan effectively for and manage current and future threats.

Performance 2014–15

In 2014–15 terrorism-related assessments dominated ASIO's strategic analysis, particularly in respect of the conflict in Syria and Iraq and the involvement of Australians in that conflict. ASIO provided advice on extremist ideologies, pathways to extremism, the radicalisation process, and indicators and warnings of terrorism. This work was used to underpin the Australian Government's effort to counter violent extremism. ASIO also produced assessments on emerging trends in radicalisation, ramifications of overseas events, counter-intelligence and counter-espionage.

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 visiting foreign dignitaries, domestic violent protest threats, threats to diplomatic premises in Australia, threats to critical infrastructure, 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 to formulate overseas travel advice for its Smartraveller website, www.smartraveller.gov.au.

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 Defence Intelligence Organisation
- ▶ the Department of Foreign Affairs and Trade
- ▶ the Department of Infrastructure and Regional Development
- ▶ the Office of National Assessments.

Performance 2014–15

On 12 September 2014, the Director-General of Security increased Australia's general terrorism threat level to High—terrorist attack is assessed as likely. The decision to raise the level reflected a range of factors, including an increasing number of Australians connected with, or inspired by, overseas terrorist groups, particularly the Islamic State of Iraq and the Levant (ISIL); direction from extremists overseas to conduct attacks here; and the availability of rudimentary or less complex methods of attack, and the willingness of local extremists to consider using such methods. ASIO worked closely with federal and state law enforcement partners to ensure all relevant assessments were shared in a timely manner.

Elsewhere, the continued establishment and growth of terrorist groups in Syria and Iraq, coupled with their ongoing and increasingly sophisticated and targeted propaganda efforts, significantly changed the threat environment. This change developed in parallel to existing and enduring threats from areas of instability such as Afghanistan and Yemen, which still provide permissive operating environments and conditions for established terrorist groups. These developments were reflected in a body of threat assessment reporting.

The terrorist threat in Western countries—and in Europe, in particular—escalated in 2014–15. Reporting provided forewarning of this worsening security environment and continued during rapidly unfolding events. Advice was also provided on the growing threat of ISIL; the potential threat to the West posed by the Syria-based, al-Qa'ida-linked Khorasan Group; and

the deteriorating security environment in North and East Africa. Of particular interest was the threat of ISIL and other extremist groups in South-East Asia, a region where Australians and Australian interests have a significant and visible presence. Threat assessments were used in decision-making by a range of agencies and applied to overseas travel by Australian high-office holders and for major overseas events, such as Anzac Day commemorations.

ASIO also provided assessments and advice to the state and territory law enforcement agencies responsible for providing security responses. ASIO reporting covered the potential use of violence at protests and the specific targeting of high-office holders, including international visitors to high-profile events such as the Group of Twenty (G20) Leaders' Summit, the Asian Football Cup and the Cricket World Cup. Such reporting underpinned an intelligence-led approach to the allocation of security resources, ultimately protecting Australia's reputation as a safe country. Some overseas issues provided a catalyst for protests against the Australian Government; against representatives of foreign governments here; and for and against perceptions of Islam. Most protests were peaceful; however, a range of assessment products highlighted escalating tensions between anti-Islam protesters and counterprotesters at nationwide Reclaim Australia rallies, tensions that culminated in clashes in Melbourne in April 2015.

Counter-espionage threat assessment and advice

During the reporting period, ASIO produced a range of products to advise government partners and industry on the threat posed by foreign espionage and interference activities against Australian interests domestically and overseas. ASIO issued threat assessments and provided an increased number of briefings in relation to foreign intelligence threats to critical infrastructure, the official travel of high-office holders, and special events. In addition, ASIO analytical reports provided critical defensive advice that explained the nature and significance of the threat from foreign intelligence services and augmented the capacity of government partners and industry to manage the risk that emanates from hostile foreign intelligence activity.

ASIO continued its focus on building awareness through targeted engagement across government and industry. The successful establishment of the Counter-Espionage Liaison Officer role saw a significant increase in engagement with security managers during the period, particularly on managing threats when travelling overseas.

Industry engagement and advice

Business Liaison Unit

Most of Australia's national critical infrastructure is privately owned. ASIO works in partnership with the private sector to ensure it has the necessary information to combat national security threats. ASIO's Business Liaison Unit (BLU) is responsible for engaging with the private sector.

The BLU provides an interface between the Australian Intelligence Community and the private sector. It publishes declassified reports, drawn from classified material, on a range of national security issues.

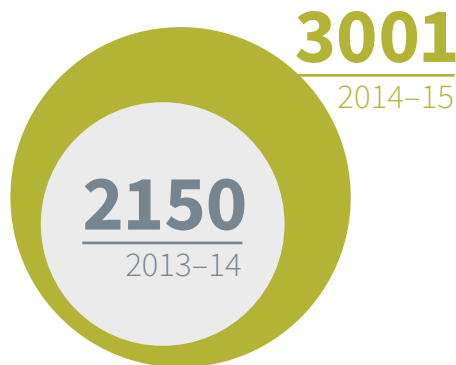
The reports are available on the subscription-based BLU website. The BLU also hosts classified briefings to priority industry sector groups on an invitation-only basis. Further information is on the BLU website, www.blu.asio.gov.au.

Performance 2014–15

In 2014–15 the BLU increased its engagement with priority industry sector groups, working closely with other government departments, industry groups and the Australian Cyber Security Centre (ACSC) to ensure a coordinated approach.

The BLU conducted 265 meetings with corporate security and risk managers across Australia, published 197 reports on its subscriber-based website (including 90 reports from foreign liaison counterparts and 17 reports from other Australian Government agencies) and hosted five dedicated security briefing days for corporate security managers from a range of different sectors, including the energy and resources, banking and finance, and defence sectors.

Figure 1: BLU subscribers



During the reporting period the number of subscribers to the BLU website increased by 39 per cent, from 2150 to 3001.

Cyber security

The number, variety and sophistication of cyber security threats to Australia and Australian interests continue to increase. The establishment of ACSC in November 2014 has brought Australia's cyber security capabilities from across government together in a single location in the Ben Chifley Building (BCB), Canberra. In conjunction with ACSC partners, ASIO has continued its intelligence-led engagement with industry, providing security advice and defensive briefings on cyber espionage. As anticipated, the co-location of the cyber security capabilities has enhanced the Australian Government's integrated response to cyber threats.

Telecommunications Sector Security Reform

During the reporting period, ASIO continued its contribution to the development of the Telecommunications Sector Security Reform legislation, which seeks to enact a regulatory framework to better protect telecommunications networks from cyber threats. The legislative reform will provide greater clarity regarding security expectations, as well as a framework for greater exchange of information between government and industry that will supplement ASIO's ongoing engagement with industry on these issues.

In 2014–15 ASIO observed an increase in telecommunications companies outsourcing and 'offshoring' significant aspects of their business processes and data management practices—in particular, their managed services. ASIO provided threat briefings and advice to the telecommunications sector to raise awareness of and to mitigate the security risks posed by such business practices.

Proscription-related advice and 'declared areas'

The proscription of an organisation identifies it as a 'terrorist organisation', which establishes a number of terrorist offences in respect of support for or affiliation with it. Under Division 102 of the *Criminal Code Act 1995* (the Criminal Code), before the Governor-General makes a regulation specifying an organisation as a terrorist organisation, the Attorney-General must be satisfied on reasonable grounds that the organisation:

- ▶ is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act; or
- ▶ advocates the doing of a terrorist act.

To inform the Attorney-General's decision-making, ASIO provides the Attorney-General's Department (AGD) with advice about organisations for which ASIO assesses there is a case for proscription. This advice is provided in an unclassified Statement of Reasons, prepared in consultation with other government agencies. Upon an organisation's proscription, the Statement of Reasons is made publicly available via the Australian Government's National Security website. As at 30 June 2015, the Australian Government had proscribed 20 organisations.

A current list of proscribed organisations is on the Australian National Security website, www.nationalsecurity.gov.au.

During 2014–15 the Australian Government introduced legislation on ‘declared areas’. Section 119 of the Criminal Code makes it an offence for a person to enter, or remain in, an area of a foreign country if that area has been ‘declared’ by the Minister for Foreign Affairs.

Before ‘declaring’ an area in a foreign country, the Minister for Foreign Affairs must be satisfied that a listed terrorist organisation is engaging in a hostile activity in that area. To inform the ministers’ decision-making process, ASIO provides advice to AGD in the form of a Statement of Reasons detailing why an area meets the legislative test for declaration. If the Attorney-General agrees to the declaration proceeding, a draft legislative instrument and the Statement of Reasons are provided to the Minister for Foreign Affairs.

Performance 2014–15

During 2014–15, the Attorney-General renewed the proscription of six terrorist organisations; Ansar al-Islam, Hizballah’s External Security Organisation, the Islamic Movement of Uzbekistan, ISIL, Jaish-e-Mohammed and Lashkar-e Jhangvi. The Attorney-General proscribed al-Murabitun for the first time. In each case, ASIO provided advice to help inform the Attorney-General’s decision. ASIO briefed the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in respect of these groups during 2014–15.

During the reporting period, ASIO provided advice that informed the Minister for Foreign Affairs in respect of two ‘declared areas’: the al-Raqqa province in Syria (declared in December 2014) and the Mosul district in Iraq (declared in March 2015). ASIO also briefed the PJCIS on these matters.

Security assessment and advice

Section 17(1)(c) of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) identifies one of ASIO’s functions as advising ministers and authorities of the Commonwealth in respect of matters relating to security, to inform them in performing their functions and responsibilities. Security assessments are a subset of this security advice. ASIO undertakes security assessments in accordance with Part IV of the ASIO Act, either at the request of other government agencies or of its own volition.

Part IV of the ASIO Act regulates the provision of advice relating to the taking of prescribed administrative action by Commonwealth agencies and state authorities and imposes an accountability regime on both ASIO and the relevant Commonwealth agency. Security assessments are predictive in nature and identify people who pose a threat to national security. By way of example, security assessments may inform:

- ▶ a decision by the Department of Immigration and Border Protection (DIBP) in relation to a person’s suitability to hold a visa or be granted Australian citizenship
- ▶ a decision by the Minister for Foreign Affairs in relation to the granting of an Australian passport
- ▶ the exercise of specified powers within the *Telecommunications Act 1997* in relation to the granting of carrier licences
- ▶ a decision to take action that relates to or affects a person’s access to national security-classified information

- ▶ a decision in relation to access to certain security-controlled areas (such as airports or ports) or certain security-controlled substances.

Complex security assessments may require extensive investigation, while other assessments may require more limited checking against intelligence holdings. There are three possible types of security assessment outcomes:

- ▶ A non-prejudicial assessment—ASIO does not have security concerns about the proposed action.
- ▶ Qualified security assessment—ASIO does not make a prejudicial recommendation but does communicate information, an opinion or advice that is or could be prejudicial to the interests of the person in relation to the contemplated prescribed administrative action.
- ▶ An adverse security assessment—ASIO recommends that a particular prescribed administrative 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

Certain security assessments made by the Director-General of Security can, in accordance with Part IV of the ASIO Act, be challenged in the Administrative Appeals Tribunal (AAT). The AAT, ‘standing in the shoes of the decision-maker’, conducts merits review of the assessment and can remit it for reconsideration or substitute its own decision. Because of the sensitivity of the information typically underlying an assessment, the AAT hears ASIO matters—

along with any merits review of the resulting decision, such as a decision to deny a passport or a national security clearance—in its Security Appeals Division, now the Security Division. Most assessments relating to migration-related decisions are excluded from this review provision.

As is the case for all decisions of the executive arm of government, ASIO’s administrative decision-making processes may also be subject to judicial review in the Federal Court and 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 2005*, the Director-General of Security 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. The Department of Foreign Affairs (DFAT) can issue temporary documents to facilitate the return of an Australian citizen whose passport has been cancelled while the holder is overseas.

Table 1: Number of passports subject to adverse security assessments or suspension provisions, by financial year

Financial Year	Number of passports subject to adverse security assessments	Number of Australian passports subject to temporary suspension
2014–15	93	9
2013–14	45	<i>not applicable</i>
2012–13	18	<i>not applicable</i>
2011–12	7	<i>not applicable</i>
2010–11	7	<i>not applicable</i>
2009–10	8	<i>not applicable</i>

With the introduction of the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*, a new provision was introduced that enables the Minister for Foreign Affairs to suspend a person's Australian travel documents for a period of 14 days if recommended by the Director-General of Security. Unlike a passport refusal or cancellation, the ASIO Act has been amended so that a person is not required to be notified of a security assessment requesting suspension of the person's Australian travel documents, nor can the person seek AAT review of the security assessment. Administratively, a passport suspension can be undertaken within a shorter time-frame than a passport cancellation—it allows ASIO to be more responsive to the movement of would-be travellers' intent on departing the country to undertake activities of security concern.

Performance 2014–15

During the reporting period, ASIO issued adverse security assessments in respect of 93 passports, in relation to individuals located both in Australia and offshore. The overwhelming majority of these assessments related to the conflict in Syria and Iraq.

The sharp increase from the previous reporting year was primarily due to the respective increase in potential travellers.

Citizenship

ASIO may issue security assessments in relation to applications for Australian citizenship under the *Australian Citizenship Act 2007*. In 2014–15 ASIO did not issue any adverse assessments in relation to citizenship applications.

Visa security assessments

ASIO furnishes security assessments to the DIBP to inform its decision-making. Where ASIO assesses that an individual is directly or indirectly a threat to security, it may issue an adverse security assessment. DIBP is required to act on the security assessment in accordance with its legal framework—for example, to refuse to grant a visa, or to cancel a visa, on security grounds. Visa security assessments may be initiated through a referral from DIBP or at ASIO’s own volition.

ASIO’s visa security assessment activities are conducted in cooperation with other border security agencies, particularly DIBP. Visa security assessment caseloads are aligned with DIBP’s priorities and with national security considerations.

Performance 2014–15

In 2014–15 ASIO undertook a major revision of its visa security assessment model in order to focus resources on the cases of greatest complexity and potential highest threat. As a result, the number of DIBP referrals requiring ASIO assessment declined. Additionally, DIBP referred fewer illegal maritime arrival cases,

resulting in a continuing reduction in the number of visa security assessments for the reporting period.

Counter-terrorism security assessments

ASIO provides counter-terrorism focused security assessments for applicants seeking to access sensitive air or maritime port areas, or security sensitive chemical, biological or 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 would pose a threat to national security should they have access to sensitive areas. AusCheck, located within AGD, coordinates the larger suite of background checks, including criminal history checks, and assesses an applicant’s overall suitability to hold an ASIC or MSIC.

Table 2: Total numbers of immigration-related assessments conducted by ASIO over the past two financial years

Type of entry	Number of assessments completed 2013–14	Number of assessments completed 2014–15 ¹
Temporary visas	17 516	11 052
Permanent residence and citizenship	6120	4638
Onshore protection (air)	326	340
Offshore refugee / humanitarian	2310	1316
Illegal maritime arrivals	877	282
TOTAL	27 149	17 628

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

ASIO provides, via the Australian Federal Police (AFP), counter-terrorism security assessment advice to inform the licensing process run by Australian states and territories for access to security-sensitive ammonium nitrates (SSANs). SSANs 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 (COAG).

Similar ASIO checks are provided to the Department of Health for individuals requiring access to security-sensitive biological agents (SSBAs), 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 by individuals to the Australian Nuclear Science and Technology Organisation nuclear facility at Lucas Heights, New South Wales.

During the reporting period, ASIO provided security assessment advice regarding workforce access to G20, Asian Football Cup and Cricket World Cup events.

Performance 2014–15

In 2014–15 ASIO completed 171 203 counter-terrorism security assessments; this compares to 159 288 counter-terrorism security assessments in 2013–14. One adverse assessment and no qualified assessments were issued during the 2014–15 reporting period.

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.

A critical element in protecting the integrity of government business is ensuring that access to nationally classified, sensitive and privileged information is provided to individuals who are suitable to hold a security clearance.

Table 3: Number and type of national security clearance assessments completed, by financial year

Type of access	2013–14	2014–15
Positive Vetting	1367	428
Negative Vetting Level 2	6668	6619
Negative Vetting Level 1	15 482	16 020
Other	5	6
Total	23 522	23 073

Border integrity investigations and analysis

ASIO helps inform an intelligence-led, risk-managed approach to border security through its reporting and analysis on border-related issues, through the provision of visa security assessments and through its support to whole-of-government measures to counter people-smuggling.

Performance 2014–15

In 2014–15 ASIO's contribution to the whole-of-government effort to counter serious threats to Australia's border and territorial integrity was supported by an ongoing analytical program. ASIO also continued to provide information to the Independent Reviewer of Adverse Security Assessments, the Hon. Margaret Stone, and to address the findings of her reviews.

Support to security intelligence-related prosecutions and litigation

ASIO's involvement in legal proceedings in courts, tribunals and other forums continued at a high tempo; matters included terrorism prosecutions, other prosecutions and civil lawsuits. ASIO's focus remained on defending prejudicial security assessments and providing, with appropriate protection, intelligence to the prosecution to be used as evidence; and to the accused, pursuant to disclosure obligations, in criminal prosecutions.

The AAT reviewed a number of security assessments, primarily concerning the cancellation of passports held by people who had travelled, or intended to travel, overseas for the purpose of engaging in politically motivated violence.

Separately, review proceedings were brought by current and former ASIO employees challenging Comcare decisions.

AAT decisions are reported on the website of the Australasian Legal Information Institute, Austlii, www.austlii.gov.au.

Working with law enforcement agencies, ASIO provided information to be used as evidence in terrorism prosecutions. ASIO also supported the coronial inquest into the deaths arising from the Lindt Café siege and contributed to the settlement of International Court of Justice proceedings brought against Australia by Timor-Leste relating to the seizure and detention of documents and data following the execution of ASIO search warrants in December 2013.

Another important area of national security litigation involved challenges to ASIO's assessments that the people-smuggling activities of particular individuals constituted a serious threat to Australia's territorial and border integrity. These challenges, which were heard at the AAT and the Federal Court, resulted in favourable decisions to the Commonwealth.

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 provides protective security advice to the Australian Government, state and territory governments and Australian businesses.

This advice, provided by ASIO's T4 Protective Security Directorate, relates to the protection of people, information and property from the threats to 'security' set out in section 4 of the ASIO Act. However, section 17(1)(d) of the ASIO Act allows T4 to also consider risks outside those matters defined as 'security' in the ASIO Act.

T4 works with operators of Australian Government-owned national critical infrastructure to provide risk and vulnerability assessment advice. T4, on approval from the Attorney-General, also provides such advice regarding state and territory government and privately owned critical infrastructure.

Protective security risk reviews and vulnerability assessments

T4 advice often takes the form of either a vulnerability assessment, a protective security risk review (PSRR) or a security design evaluation.

- ▶ Vulnerability assessments identify weaknesses in protective security arrangements and seek to provide a vital component of a client's security risk assessment.
- ▶ A PSRR follows a risk assessment methodology and assesses physical, information, administrative and personnel security risks. Risk treatment options are provided for consideration and application as determined by the client.

- 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 and, where applicable, achieve relevant minimum standards (for example, Zone 5 certification requirements).

Physical security certifications

The Australian Government Protective Security Policy Framework (PSPF) identifies T4 as the certification authority for Zone 5 facilities. Zone 5 facilities are facilities that hold information classified as Top Secret. On behalf of Defence and Intelligence Security Group, T4 also certifies the physical security of sensitive compartmented information facilities (SCIFs).

This provides assurance to the Australian Government that agencies are constructing facilities that meet the minimum standards required for the protection of the Australian Government's most sensitive information. 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 helps to reduce the risk of technical compromise of highly classified or sensitive discussions.

TSCM inspections include electronic surveys, the monitoring of premises for possible covert electronic activity, and physical security inspections. As with previous years, demand for ASIO's TSCM services remained high during the reporting period.

Security services and equipment evaluation

T4 conducts the Security Equipment Evaluation Program on behalf of the Australian Government's Security Construction and Equipment Committee (SCEC). This program evaluates security products such as locks, alarms and security containers to determine whether they are suitable for use by government. Products assessed as being fit for purpose are listed in the Security Equipment Evaluated Product List (SEEPL).

T4 also evaluates and endorses couriers, locksmiths, data destruction facilities and security consultants who work with, or provide services for, the Australian Government.

Protective security training

An important aspect of T4's outreach program is educating agency security staff on their security obligations under the PSPF. This is achieved through T4's own protective security training courses, as well as through courses conducted in partnership with AGD's Protective Security Training College.

T4 also regularly delivers training to enable commercial security consultants and locksmiths to meet the requirements of SCEC programs.

For further information on T4, visit the ASIO website at www.asio.gov.au.
 For further information on SCEC, visit the SCEC website at www.scec.gov.au.

Performance 2014–15

In 2014–15, T4 met its objective of providing protective security advice to its clients by delivering the following outputs:

Advice	Performance 2014–15
Protective security risk reviews and vulnerability assessments	<ul style="list-style-type: none"> ▶ 2 protective security risk reviews ▶ 7 design evaluations ▶ 7 vulnerability assessments
Physical security certifications	<ul style="list-style-type: none"> ▶ 32 Zone 5 site certifications ▶ 9 destruction service approvals ▶ 1 lead agency gateway facility certification ▶ 67 physical security inspections
Technical surveillance countermeasures	<ul style="list-style-type: none"> ▶ ASIO does not comment publicly on the details of this work program
Security services and equipment evaluation	<ul style="list-style-type: none"> ▶ 35 security equipment evaluations ▶ 7 courier evaluations, including 4 endorsements ▶ 1 locksmith bulletin ▶ 2 protective security circulars ▶ 2 security equipment guides ▶ 1 Security Equipment Evaluated Product List (SEEPL 2015) ▶ 1 technical note
Protective security training	<ul style="list-style-type: none"> ▶ 2 protective security training courses ▶ 3 SCEC-approved locksmith briefings

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 engagement
- ▶ contribution to policy development.

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 with sufficient accuracy to prevent such threats eventuating. ASIO's work is predictive and advisory, an exercise in informing risk management and enabling government to take preventative actions.

Counter-terrorism investigations and analysis

ASIO undertakes counter-terrorism 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.

Performance 2014–15

In the reporting period, Australia suffered two terrorist attacks and authorities disrupted six terrorist plots. ASIO was managing over 400 higher-priority counter-terrorism security investigations at the end of the reporting period—working to identify, investigate and analyse terrorist threats and act with law enforcement agencies to thwart those threats.

Further detail on ASIO's performance relating to counter-terrorism operations and capabilities is provided in the classified Part 3 of the *ASIO Annual Report 2014-15*. Part 1 provides an overview of the current assessment of the threat from terrorism.

Counter-terrorism strategy

The Australian Government's counter-terrorism strategy was agreed to by the Coalition of Australian Governments (COAG) and released in August 2015, following the reporting period. It is characterised by a focus on strong, intelligence-led collaboration.

ASIO has continued to contribute to Australia's security through a number of multi-agency initiatives and governance arrangements, including participation in the Australian – New Zealand Counter-Terrorism Committee (ANZCTC). ASIO provides security intelligence advice to the ANZCTC and to its subcommittees and individual capability forums, which ensures there is a common understanding among the member agencies of the threat environment facing both Australia and New Zealand.

ASIO also participates in the National Counter-Terrorism Exercise Program, a range of annual counter-terrorism exercises that test, maintain and strengthen counter-terrorism capabilities and interoperability across and between all levels of government and their agencies. ASIO helps develop, conduct and refine the program 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.

Australian Counter-Terrorism Centre

On 4 August 2014, the National Security Committee of Cabinet (NSC) agreed that the Department of the Prime Minister and Cabinet (PMC) would lead a review of Australia's counter-terrorism arrangements to ensure they are well organised and targeted and as effective as possible. The report of the review was released in February 2015 and drives the work undertaken by the Australian Counter-Terrorism Centre (ACTC) in coordinating the Australian Government's counter-terrorism efforts.

The ACTC is responsible for providing assurance to government that Australia's counter-terrorism effort is coordinated, and government agencies work together closely on operations, policy challenges and capability development. The ACTC is a multi-agency, whole-of-government capability. Housed in the BCB, the ACTC is staffed by embedded officers from intelligence, law enforcement, policy and border protection agencies.

On 25 May 2015 the then Prime Minister, the Hon. Tony Abbott MP, announced structural changes across the Australian Government to better coordinate Australia's national counter-terrorism efforts. The Minister for Justice, Mr Michael Keenan, was appointed the Minister assisting the Prime Minister on Counter-Terrorism. Mr Greg Moriarty was appointed as Australia's first Counter-Terrorism Coordinator, situated in PMC.

Counter-espionage and foreign interference investigations and analysis

ASIO's outreach to government and the private sector has led to an increased output of security intelligence advice and an enhanced role in policy development and implementation.

ASIO relies heavily on strong and collaborative partnerships. ASIO's objectives are to proactively discover the sources of threat and to build defences, spanning the spectrum of personnel, technical and communications technology security policies.

Contact Reporting Scheme

The Contact Reporting Scheme (CRS) 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 individuals, including foreign nationals, that appear to be suspicious, where the contact is ongoing, unusual or persistent in any respect.

This contact could be official or social and could occur either in or outside Australia. Employees should also report contact with any person, regardless of nationality, where that person seeks access to information they do not need to perform their duties. Employees are encouraged to report incidents to their respective Agency Security Advisor, or their internal security team.

International engagement

ASIO engages with, and receives support from, a number of international partners. While international partnerships have always been important in the performance of ASIO's functions, the complexity of the 'foreign fighters' issue has made cooperation with foreign security and intelligence agencies even more critical. As a consequence, ASIO expanded its overseas liaison network during the reporting period.

Many security threats are transnational in nature. Liaison relationships enable ASIO to draw on the expertise and capability of overseas partners.

Contribution to policy development

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

In 2014–15, ASIO worked with AGD 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 violent extremist terrorism, both domestically and internationally. ASIO assessments informed policymakers of the implications of the conflicts in Syria and Iraq for Australia's security, including consequences from the involvement of Australian citizens in those conflicts and their impact on radicalisation within Australia. ASIO 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 conflict. ASIO also worked with other agencies to manage the threat posed by individuals who returned to Australia having participated in the conflict.

ASIO supported policy agencies in the development and passage of a number of significant reforms to the national security legislative framework, including the *National Security Legislation Amendment Act (No. 1) 2014*, the *Counter-Terrorism Legislation Amendment (No. 1) Act 2014*, the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* and the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. Further detail about these and other legislative reforms is provided in Part 4 of this report.

ASIO also significantly increased its engagement with the broader Australian Government—at executive levels and with agency security advisers—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. ASIO has identified vulnerabilities and significant weaknesses associated with current Australian personnel security arrangements, in terms of both the current practice and the ability to respond effectively to emerging issues. This creates an unacceptable level of risk for government. As a result of these vulnerabilities, the secure conduct of government business cannot be assured. In addition, the risk to government information, as well as the information provided by our closest partners, carries serious implications for our national sovereignty and our reputation with partners.

In 2014–15, in recognition of the vulnerabilities of the current system for the Australian Government, AGD led a consultative process to develop detailed business models required for the necessary reforms to personnel security arrangements. ASIO has been a key stakeholder and contributor to the AGD-led review, translating our investigative and personnel security assessments experience, and that of our allied partners, to inform the reforms.

In 2014–15, ASIO worked closely with the Department of the Treasury and broader Australian Government agencies on a number of policy issues relating to foreign investment applications to the Foreign Investment Review Board.

ASIO also engaged with and contributed to the Cyber Security Review, led by PMC. ASIO's contribution included membership of the Cyber Security Review Steering Group and participation in a range of workshops.

New national terrorism threat advisory system

The NTAC, a branch within ASIO, worked closely with PMC during the Review of Australia's Counter-Terrorism Machinery on developing workable changes to Australia's national terrorism advisories. The review's report, which was released in January 2015, recommended the development of a new national terrorism threat advisory system, to replace the classified National Threat Level system and the unclassified Public Alert Systems.

At its meeting on 17 April 2015, the Council of Australian Governments agreed to implement the recommendations of the review. The new advisory system is expected to be presented to the Australia – New Zealand Counter-Terrorism Committee on 23 July 2015, with implementation of the new advisory system to take place later in the year.

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 completes this activity in close cooperation with foreign intelligence collection partners the Australian Secret Intelligence Service and the Australian Signals Directorate.

Performance 2014–15

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 NSC.

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 *ASIO Annual Report 2014–15*.



Part 3

OUTCOMES AND HIGHLIGHTS

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

ASIO fulfils an essential role in the system of government, helping protect Australians and Australian interests from attempts to do harm or cause disadvantage.

In doing so, it contributes to a safe and secure environment in which the nation, individuals and democratic institutions can operate freely and prosper. Having such a security service, operating under not just a strict legislative regime but also comprehensive oversight and accountability frameworks, helps maintain a society in which, as Justice Robert Marsden Hope AC CMC QC said, ‘Public safety and individual liberty sustain each other’.

In order to fulfil its role, ASIO has been given special powers and a remit to investigate activities, including activities within Australia and involving Australians—these activities may not always be against Australian law but they are nonetheless inimical to national interests. With those powers and remit comes a special responsibility to act legally, ethically and with propriety. ASIO adheres to the rule of law and operates under not only a strict legislative regime but also comprehensive oversight and accountability regimes. It engages transparently with the oversight and accountability mechanisms to provide public reassurance of the legality and propriety of ASIO’s actions.

Attorney-General

ASIO’s ministerial accountability is to the Attorney-General, currently Senator the Hon. George Brandis QC.

Functional responsibility

ASIO’s security intelligence activity is conducted in accordance with the *Attorney-General’s Guidelines*, under sections 8A(1) and 8A(2) of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). The *Attorney-General’s Guidelines* stipulate that ASIO’s activities must be conducted in a lawful, timely and efficient manner, applying the principal of proportionality—that is, the methods used to investigate a person must be proportional to the threat posed—to ensure the least intrusion necessary into an individual’s privacy. The Guidelines were last updated in December 2007.

Part III, Division 3 of the ASIO Act provides for warrants allowing ASIO to use ‘special powers’. The Attorney-General issues all ASIO warrants, other than questioning warrants and questioning and detention warrants, which are issued by a ‘prescribed authority’. 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 issue the warrant. For every warrant issued, ASIO must report to the Attorney-General on the extent to which it assisted the organisation in carrying out its functions.



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 347 submissions to the Attorney-General.

Parliamentary oversight

ASIO has been subject to parliamentary joint committee oversight since 1986. In 2014–15 that oversight was performed by the Parliamentary Joint Committee on Intelligence and Security, Senate Estimates hearings and several parliamentary inquiries relating to national security.

Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is a bipartisan statutory committee established under section 28 of the *Intelligence Services Act 2001* (ISA). More information on the role of the committee and its previous inquiries is available on the Parliament of Australia website, www.aph.gov.au.

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 under the ISA 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 and reporting the committee's comments and recommendations to each House of the Parliament of Australia and to the responsible minister.

The PJCIS may also review a regulation that lists an entity as a terrorist organisation under section 102.1A of the *Criminal Code Act 1995* or that lists a declared area.

Review of administration and expenditure

The PJCIS commenced its review of the administration and expenditure of Australian intelligence agencies for the period 2013–14 on 25 September 2014. ASIO provided both a classified and an unclassified submission; the latter is available on the PJCIS website www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security. The submissions provide information on the security environment, as well as ASIO's expenditure, organisational structure, corporate direction and strategic planning, human resource management, legislation, organisational security, relationships and accountability. On 25 March 2015, ASIO attended a private hearing before the PJCIS to inform the committee's inquiry.

Review of national security legislation

During the reporting period, ASIO made a submission to and appeared before the PJCIS in relation to the review of the *Migration Amendment Bill 2013*.

Martin Place siege: Joint Commonwealth – New South Wales review

On 17 December 2014, the then Prime Minister, the Hon. Tony Abbott MP, and the New South Wales Premier, the Hon. Mike Baird MP, announced a review of the Lindt Café siege incident in respect of national and state agencies and the cooperation between them. This review was conducted jointly by the Department of the Prime Minister and Cabinet (PMC) and the New South Wales (NSW) Department of Premier and Cabinet.

ASIO engaged openly and actively with the review. ASIO holdings and actions as they related to Mohammad Hassan Manteghi (also known as Man Haron Monis) informed—and were referenced in—the final report of the joint review, which included a detailed appendix outlining ASIO's prioritisation model.

The report of the joint review was released on 22 February 2015, and made 17 recommendations to improve the system, including laws and government processes. The review made no recommendations with regard to ASIO's conduct, or ASIO's processes and procedures as they related to Manteghi.

Only one recommendation in the report related to ASIO's access to information. It recommended that all states and territories review relevant legislation—particularly with regard to privacy and health—to ensure appropriate access by ASIO.

However, the report noted that ASIO was able to access all relevant information held by government agencies in this case. The final report is available on the PMC website, www.dpmc.gov.au/pmc/publication/martin-place-siege-joint-commonwealth-new-south-wales-review.

The NSW Coroner is conducting an inquest into the deaths of Mr Tori Johnson, Ms Katrina Dawson and Manteghi. The first segment of this inquest was held from 25 May to 5 June 2015, with the inquest to continue in the 2015–16 reporting period.

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 with the Parliament of Australia on 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 2014–15 the Director-General of Security, Mr Duncan Lewis, and Deputy Director-General, Ms Kerri Hartland, appeared before the committee on three occasions: Supplementary Budget Estimates, on 10 December 2014; Additional Estimates, on 24 February 2015; and Budget Estimates, on 28 May 2015.

During these appearances, ASIO responded to questions on topics such as ASIO's budget, security assessments in respect of passports, foreign fighters and the legislative changes to the *Telecommunications (Interception and Access) Act 1979* (TIA Act). 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.

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

The Senate Legal and Constitutional Affairs References Committee completed its inquiry into the comprehensive revision of the TIA Act and tabled its report on 23 March 2015.

The focus of the report was on the mandatory data retention regime, issues on which the committee members were unable to reach an agreed view and which were largely superseded as a result of the passage of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. There was a general recognition by the committee of the need for urgent reform of the TIA Act.

During the reporting period the former Director-General of Security, Mr David Irvine AO, attended a public hearing to supplement ASIO's unclassified submission to the inquiry.

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.

Dr Vivienne Thom held the position of IGIS during the reporting period. Appointed in 2010, Dr Thom concluded her term as IGIS in July 2015. 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.

The independent oversight provided by the IGIS, and compliance recommendations arising from IGIS reviews and inspections, is used by ASIO to improve its processes. More information can be obtained from the IGIS website, www.igis.gov.au.

Independent Reviewer of Adverse Security Assessments

The role of the Independent Reviewer of Adverse Security Assessments, performed during the reporting period by 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 Department of Immigration and Border Protection (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; and to be ineligible for a permanent protection visa, or to have 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 completed. The Independent Reviewer's terms of reference are available on the Attorney-General's Department (AGD) website, www.ag.gov.au/asareview.

By the end of the reporting period, the Independent Reviewer had finalised a total of 46 of the 47 primary reviews within her cohort. Having finalised 22 primary reviews in previous years, in 2014–15 the Independent Reviewer finalised a further 24. Of these:

- ▶ In six cases the Independent Reviewer found the adverse security assessments were appropriate.
- ▶ In two cases the reviews were well advanced when ASIO furnished new assessments—one qualified and the other non-prejudicial. In both cases, the Independent Reviewer completed her review and agreed the new assessments were appropriate.
- ▶ In six cases, the Independent Reviewer found the adverse security assessments had been appropriate at the time they were furnished but were no longer appropriate, and recommended either qualified or non-prejudicial security assessments.
 - ▶ After re-examining the cases, in five cases ASIO furnished either qualified or non-prejudicial assessments in accordance with the Independent Reviewer's recommendation.
 - ▶ In one case, the Independent Reviewer recommended ASIO issue a non-prejudicial security assessment. Following consideration, ASIO furnished a qualified security assessment. The Independent Reviewer completed her report finding the qualified security assessment was not appropriate and maintaining her view that a non-prejudicial security assessment would be an appropriate outcome.
- ▶ In five cases, new (qualified or non-prejudicial) security assessments were furnished by ASIO following new information referred by the Independent Reviewer, and the outcomes of ASIO's own investigations.
- ▶ In two cases, the Independent Reviewer found there were flaws in ASIO's assessment and she was unable to form a view as to the appropriateness of the adverse security assessment. In both cases, ASIO furnished qualified security assessments, which the Independent Reviewer agreed were appropriate.
- ▶ In three cases, the Independent Reviewer found the adverse security assessments were not appropriate. Of these:
 - ▶ In one case, the Independent Reviewer recommended ASIO issue either a non-prejudicial or qualified security assessment, and after re-examining the case ASIO furnished a non-prejudicial security assessment.
 - ▶ In two cases, the Independent Reviewer recommended ASIO issue a non-prejudicial security assessment, and after re-examining the cases ASIO furnished non-prejudicial security assessments.

In addition to the finalised cases, the Independent Reviewer referred new information concerning one case to ASIO, together with an incomplete but advanced draft of her report. The draft summarised all the information before her but did not include any recommendation. ASIO was considering the new information at the end of the reporting period. Under the terms of reference, the review process for this case remains on hold until ASIO concludes its consideration of the new information.

Periodic review

The Independent Reviewer's terms of reference require her to conduct a periodic review of adverse security assessments for eligible persons every 12 months.

For this phase, the Independent Reviewer encouraged applicants to provide any information that they wished to put forward and that would likely be of assistance. This included material that clarified, corrected or added to information previously given, as well as any updated information on family circumstances and mental or physical health. As part of the periodic review, the Independent Reviewer considered closely the overall security environment, informed by ASIO's contemporary assessment of security threats, and the passage of time and, if relevant, any changes to the applicants' circumstances or ideology during their time in detention.

In parallel with the Independent Review process, ASIO undertook a large number of internal reviews of its own volition. A number of legal representatives advised they would await the outcome of the ASIO internal review prior to turning their attention to the Independent Reviewer's periodic review process. The Independent Reviewer decided to proceed with periodic reviews, regardless of the status of the ASIO internal review, and (provided the legal representatives had been given ample notice) regardless of whether or not any additional submissions had been provided to her office. This approach was in the best interests of applicants as it was anticipated that the opinion expressed in the Independent Reviewer's draft report would be of assistance to ASIO in its internal review. A number of periodic reviews ceased in the reporting period due to ASIO's furnishing of non-prejudicial or qualified security assessments of its own volition.

There were 14 extant adverse security assessments at the end of the reporting period which were eligible for periodic review. By the end of the reporting period, the Independent Reviewer had provided four draft periodic review reports to ASIO. In one of those four cases, just after the reporting period, on the basis of the Independent Reviewer's draft finding and its own investigation, ASIO furnished a non-prejudicial security assessment.

Independent National Security Legislation Monitor

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.

The Hon. Roger Gyles AO QC was appointed as the acting INSLM on 7 December 2014.

Mr Gyles is currently conducting an inquiry into section 35P of the ASIO Act in relation to special intelligence operations. ASIO has appeared at private and public hearings as part of the review and provided classified and unclassified submissions in response to requests for information.

Legal assurance and capability protection

ASIO's legal division (Office of Legal Counsel) provides legal advice on organisational compliance and risk in carrying out operational activities. In particular, the division 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 division 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.

Advice is provided in respect of the proper use of special powers warrants. Examples of assistance include advising 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.

Specifically, during 2014–15 the Division provided advice on operations, investigations, and legal and administrative proceedings, including:

- ▶ developing and implementing a suite of legislative amendments designed to strengthen and improve Australia's legislative counter-terrorism framework
- ▶ providing legal advice to operational planning around the growing threat of radicalised individuals training in or returning from Syria and Iraq
- ▶ 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 Group of Twenty (G20) conferences
- ▶ 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 levels.

The Division also provided capability protection advice to support merits review processes in the Administrative Appeals Tribunal, and judicial review in the Federal and High Courts of Australia.

Legislative change

National Security Legislation Amendment Act (No. 1) 2014

Most provisions in the *National Security Legislation Amendment Act (No. 1) 2014* commenced on 30 October 2014. The Act contains a range of improvements to the legislative framework governing Australia's intelligence agencies, primarily the ASIO Act and the ISA, as well as modernisation measures. These amendments are an important step towards ensuring that ASIO's legislative framework adequately equips and assists it to perform its statutory mandate in a rapidly changing threat environment.

Key measures of direct relevance to ASIO include:

- ▶ addressing problems relating to the scope and effectiveness of ASIO warrants, including amendments to ASIO's computer access warrant legislation to better reflect modern use of technology
- ▶ introducing a new, single 'surveillance device' warrant
- ▶ modernising ASIO's employment provisions
- ▶ introducing a special intelligence operations scheme to protect ASIO employees and other people from civil and criminal liability for certain authorised activities that would otherwise be unlawful

- ▶ introducing an ‘identified person warrant’, which, together with subsequent authorisations by the Attorney-General or the Director-General of Security, enables multiple powers to be exercised against an identified person under one warrant
- ▶ enhancing cooperation between ASIO and ASIS and the private sector
- ▶ creating and updating secrecy offences in the ASIO Act and ISA.

ASIO played a key role in the development of this legislation, in collaboration with the Attorney-General’s Department (AGD) and other intelligence agencies. ASIO made a number of submissions to the PJCIS review of the draft legislation and appeared before the committee on 15 August 2014.

During the reporting period, ASIO also undertook a significant amount of work in relation to the implementation of these legislative reforms. This included developing a suite of internal fact sheets and frequently asked questions on the legislative reform measures; and updating existing warrant templates and developing new warrant templates, in consultation with the AGD.

ASIO has actively utilised the suite of powers introduced under the Act. For example, ASIO has issued warrants in respect of all new warrant powers, including the amended computer access and surveillance device warrants and the new identified person warrants.

Counter-Terrorism Legislation Amendment (No. 1) Act 2014

The *Counter-Terrorism Legislation Amendment (No. 1) Act 2014* commenced on 13 January 2015. The Act contains measures to assist intelligence and law enforcement agencies to disrupt terrorist threats.

Key measures of relevance to ASIO include:

- ▶ improving the control order framework, including making control orders available where a person trains with a terrorist organisation, facilitates a terrorist act or engages in foreign incursions
- ▶ making explicit that it is a statutory function of Australian Secret Intelligence Service (ASIS) to assist and cooperate with the Australian Defence Force (ADF)
- ▶ enabling the Minister for Foreign Affairs to give a class authorisation to enable ASIS to support ADF operations
- ▶ enabling the Attorney-General to give agreement to a ministerial authorisation in relation to a class of Australians
- ▶ enabling ASIS, the Australian Signals Directorate and the Australian Geospatial-Intelligence Organisation to obtain ministerial authorisations in emergency situations.

During the reporting period, ASIO worked with the Attorney-General’s Department (AGD) and other Australian Government agencies as part of the development of this legislation.

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014

The *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* received Royal Assent on 3 November 2014. Most of the provisions of the Act that are relevant to ASIO commenced on 1 December 2014. The Act addresses gaps in the counter-terrorism legislative framework, focusing on the threat posed by the return of Australians who have participated in foreign conflicts or trained with extremist groups overseas.

Key measures of relevance to ASIO include:

- ▶ substituting the ‘last resort’ requirement for obtaining ASIO questioning warrants with a requirement for the Attorney-General to be satisfied that the warrant request is reasonable in all the circumstances
- ▶ extending to 2018 the sunset date of the ASIO questioning and questioning and detention warrants
- ▶ introducing an offence for wilfully damaging things required to be produced under questioning and questioning and detention warrants
- ▶ introducing new offences in the *Criminal Code Act 1995* (Criminal Code) (advocating terrorism and entering a declared area without legitimate purpose)
- ▶ introducing the temporary suspension of Australian and foreign travel documents
- ▶ introducing the temporary cancellation of visas
- ▶ introducing the ability to cancel certain welfare benefits for individuals whose visa or passport has been cancelled on security grounds.

ASIO played a key role in the development of this legislation, in collaboration with AGD and other agencies. ASIO made submissions to the PJCIS review of the draft legislation, and it appeared before the committee on 3 October 2014.

ASIO also undertook a significant amount of work in relation to the implementation of these legislative reforms. This included internal training, policy development, the updating of existing security assessment templates and the development of new templates in consultation with both the Department of Foreign Affairs and Trade and AGD.

Since implementation, ASIO has used the temporary suspension of travel documents to assist in preventing the travel of prospective foreign fighters. In addition, ASIO’s advice has informed the declarations by the Minister for Foreign Affairs under the Criminal Code of two areas—al-Raqqa province, in Syria, and Mosul district, in Iraq—making it an offence to travel to those areas without legitimate purpose. Al-Raqqa province was declared on 4 December 2014, and Mosul district was declared on 2 March 2015.

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* received Royal Assent on 13 April 2015. The majority of the provisions in the Act will commence on 13 October 2015.

The Act requires telecommunications service providers to retain and secure specified telecommunications data for a minimum of two years.

The introduction of this obligation is a critical step in ensuring that ASIO can continue to access telecommunications data vital to national security investigations.

During the reporting period, ASIO worked with AGD and other agencies on the development of the legislation. ASIO made a number of submissions to the PJCIS review of the draft legislation, and it appeared before the committee on 17 December 2014 and 30 January 2015.

The legislation includes new record-keeping and reporting requirements for ASIO and law enforcement agencies in relation to accessing retained telecommunications data; and imposes a new oversight regime in relation to the disclosure of telecommunications data for the purposes of identifying the identity of a journalist's source, including a restriction on the ability to authorise the disclosure of such data unless a journalist information warrant is in force.

During the reporting period, ASIO took steps towards ensuring that it will be in compliance with these new statutory obligations when they take effect on 13 October 2015, including the development of new warrant templates for journalist information warrants, and a review of current record-keeping and reporting practices to ensure that they meet new requirements.

Telecommunications and Other Legislation Amendment Bill 2015

On 26 June 2015, the Attorney-General and the then Minister for Communications, the Hon. Malcolm Turnbull MP, released an exposure draft of legislation to amend the *Telecommunications Act 1997* to strengthen the current framework for managing

national security risks to Australia's telecommunications networks. Submissions on the draft legislation closed on 31 July 2015.

The draft Bill includes the following:

- ▶ an obligation for all carriers, carriage service providers and carriage service intermediaries (C/CSPs) to take steps to protect their networks from unauthorised access and interference
- ▶ a requirement for C/CSPs to notify security agencies of key changes to networks and management systems that could affect their ability to protect their networks
- ▶ authority for the Secretary of AGD to request information from C/CSPs and to issue directions to C/CSPs, enforceable by a civil penalty regime.

During the reporting period, ASIO worked with AGD on the development of the draft legislation and associated explanatory material.

Legislation on assumed identities

With the support of AGD, ASIO has been pursuing amendments to state and territory legislation in relation to assumed identities. During the reporting period, this work resulted in the introduction of Northern Territory (NT) legislation on assumed identities. The *Police (Special Investigative and Other Powers) Act 2015* was passed on 19 February 2015 and assists ASIO to obtain evidence of its assumed identities from NT-issuing agencies, including entries in the NT register of births, deaths and marriages.

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

Public interest disclosure

The *Public Interest Disclosure Act 2013* (the PID Act) enables all Commonwealth agencies to facilitate disclosure and investigate wrongdoing and maladministration in the Commonwealth public sector, including within ASIO.

For intelligence agencies, the PID Act works in conjunction with other legislation—such as the ASIO Act, the IGIS Act, 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.

In the reporting period, three disclosures were received and allocated to an investigating authority. All three disclosures were completed, or allocated for investigation under another authority, within the required time frames. The disclosure investigations found no findings of maladministration, wastage of public money or abuse of public trust, but cases did produce recommendations aimed at improving organisational communication, effectiveness and overall accountability.

ASIO complied with public interest disclosure reporting mechanisms by informing the IGIS on the receipt and conclusion of each disclosure matter.

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

Internal audit and fraud control

Fraud control

The ASIO Fraud Management Group comprises senior executive officers who oversee the management of fraud control arrangements and report to ASIO's Audit and Risk Committee. In the reporting period, no serious fraud allegations were referred to the Fraud Management Group for investigation, and both the Fraud Management Group and the Audit and Risk Committee were satisfied with the manner in which minor fraud matters were dealt with through alternative administrative or investigative processes.

The Audit and Risk Committee was satisfied ASIO has the appropriate processes in place to detect, capture and respond to the fraud risks identified in the fraud risk assessment undertaken in early 2013. In accordance with Commonwealth fraud control policy, the committee will require ASIO to undertake another fraud risk assessment in 2015–16.

Fraud awareness training for all new employees and contractors continues to be provided in ASIO's induction training. ASIO also provides a mandatory e-learning training module on fraud awareness, which ASIO personnel must complete every three years. The module recently underwent substantial amendment to ensure it continues to be of benefit for ASIO staff and reflects changes in ASIO and Commonwealth policies.

Audit

ASIO's Internal Audit Directorate undertakes evaluations of all financial and non-financial policies and operations. Internal audits and evaluations may cover any of the programs or activities of ASIO, as provided for in legislation, relevant business agreements, memorandums of understanding or contracts.

In 2014–15 Internal Audit undertook six mandatory compliance audits into the access and use by ASIO personnel of other agency database information.

An audit was conducted into ASIO processes to ensure travel approvals are provided by the appropriate delegate and in accordance with Australian Government Policy Official International Travel—Approval and Use of the Best Fare of the Day. The audit found updates to ASIO's travel guidance met the requirements of the resource management guide but policy advice in this area required updating.

In the reporting period, an audit of ASIO's compliance with the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) framework was undertaken to augment existing compliance activities. The objective of the audit was to assess the suitability of the systems, controls and reporting that ASIO is relying upon in determining compliance or non-compliance with the requirements of the PGPA Act framework. While the audit found there was scope for improvement in some areas, the results attested to the efforts of ASIO in adopting and complying with the legislative framework.

Internal Audit Directorate regularly monitored and sought updates from work areas on the implementation of agreed audit and evaluation recommendations. The Audit and Risk Committee at its quarterly meetings was kept informed of the progress of the implementation of recommendations.

Security in ASIO

ASIO has a holistic and tightly integrated security program, which is overseen and driven by the senior executive. All aspects of security are managed collectively and collaboratively to achieve maximum effect from the interrelated disciplines that form the ASIO security program. As threats and risks evolve, ASIO adapts internal security measures to meet the challenge of protecting ASIO employees, premises, information and assets. ASIO ensures that all employees have access to the training, tools and advice required to actively manage any security risks in a manner consistent with ASIO's strong security culture.

Security policy and coordination

ASIO implements security policies in accordance with Australian Government requirements and develops and maintains additional protective security policies and guidelines to address the specific security environment ASIO employees work within. All ASIO employees must comply with mandatory training requirements, which highlight and explain new or changing security risks and provide tools and advice to address them. ASIO also seeks opportunities to contribute to the maintenance of Australian Government security policy frameworks and policies.

Personnel security

All ASIO employees are required to maintain an appropriate high-level security clearance. ASIO employees are continually assessed for ongoing suitability to hold a clearance. ASIO employees must demonstrate that they are honest, trustworthy, mature, tolerant, resilient and loyal and are not susceptible to influence or coercion. ASIO employees have access to a number of support services to assist them in maintaining the attributes and behaviours required of an ASIO clearance holder.

Physical and information security

ASIO complies with Australian Government physical and information security requirements. ASIO undertakes scheduled reviews of premises to ensure continuing compliance with required security standards, as well as addressing any changing threats or risks. ASIO information security requirements are met in a combination of both procedural and technical security measures and ensure that information ASIO holds is protected from compromise.

Information technology security

ASIO's information technology systems are subject to stringent security requirements. All ASIO IT systems are subject to ongoing monitoring and audit activities to ensure that usage is both appropriate and secure. Review of systems' security is continuous, and system owners are responsive to evolving security challenges.



Part 5

CORPORATE MANAGEMENT

Corporate strategy and governance

ASIO Strategic Plan 2013–16

ASIO's Strategic Plan 2013–16 provides the overarching direction for the organisation. This financial year ASIO built on the foundation set by the strategic plan since its introduction.

In 2014–15, ASIO focused intently on several of its strategic goals, particularly the following two:

- ▶ 'We manage risk in a constantly evolving security environment'—more than ever ASIO has needed to respond to the evolving security environment. As expected, there has been an evolution in the security threat environment; at the same time, there has been an evolution in the legislative foundation upon which ASIO operates.
- ▶ 'Attract, develop and retain a professional and highly competent workforce'—in response to the New Policy Proposal funding received during the reporting period, ASIO has committed additional resources to the effective recruitment of new talent. Maintaining a security-cleared and professional workforce is a great challenge; expanding that workforce is an even greater challenge.

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

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 information and advice to support the Director-General of Security in his responsibilities.

During the reporting period and consistent with ASIO's new risk management policy and the requirements of the *Public Governance, Performance and Accountability Act 2013*, the ASIO committees changed the way they consider and manage risk.

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. Up until May 2015, Ms Jenet Connell, a highly experienced and distinguished public servant serving at the time as the Chief Operating Officer of the Department of Finance, was the board's external member. Mr John Lonsdale, Chief Operating Officer of the Department of the Treasury, has since taken on the role of external board member.

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 outcomes of the Executive Board are visible to the Australian National Audit Office (ANAO) as part of its governance audit.

Over the reporting period, the Executive Board received regular reporting from ASIO's committees on corporate outcomes and issues, key security issues—including the conflict in Syria, developments in the domestic security environment, and espionage threats—the organisation's budget, the counter-terrorism New Policy Proposal, and risks.

Intelligence Coordination Committee

The Intelligence Coordination Committee (ICC) provides strategic direction and ensures formal and effective coordination of ASIO's investigative and assessment priorities, allocating resources to these priorities on a risk management basis. The ICC approaches its responsibilities by dividing ASIO's work into thematic work programs, including counter-terrorism, counter-espionage and interference, border security, and security intelligence capabilities. It also regularly reviews ASIO's performance against the objectives of both the National Intelligence Priorities and the key risks identified by the ICC programs.

Workforce Capability Committee

ASIO's ability to both respond to and prepare for challenges in the security environment relies 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 progress of recruitment activities to increase ASIO's capacity in relation to the counter-terrorism New Policy Proposal, a review of ASIO's language capabilities, results from the ASIO staff survey, and policy changes in relation to internal transfer processes. The WCC reported to the Executive Board on the external and internal recruitment outcomes against the New Policy Proposal recruitment targets.

Security Committee

The ASIO Security Committee (ASC) reports directly to the Executive Board, providing assurance of sound and secure practices in ASIO. The ASC considers the evolving security environment and reviews and addresses key issues relevant to the security of ASIO people, property, operational activities and information technology. It also approves security policy and procedures and reviews ASIO's compliance in meeting legislative and policy responsibilities specific to Australian Government mandatory standards.

Finance Committee

The Finance Committee (FC) monitors ASIO's financial performance and provides advice to the Executive Board on ASIO's financial management and strategy. The New Building Committee is a subcommittee of the FC and is responsible for ensuring the Ben Chifley Building (BCB) meets ASIO's requirements.

The core FC responsibilities are:

- ▶ reviewing ASIO's operating budget, its asset replacement activities and the ASIO Investment Program
- ▶ providing strategic advice, including future budget management strategies, to the Executive Board.

Two significant issues during 2014–15 were the injection of operating and capital funds associated with the counter-terrorism New Policy Proposal; and financial implications as the BCB became fully operational.

Audit and Risk Committee

The role of the ASIO Audit and Risk Committee is to provide independent assurance and advice to the Director-General of Security and the Executive Board on ASIO's financial and performance reporting responsibilities, risk oversight and management, and system of internal control.

Members of the committee, including the Chair, are appointed for an initial period not exceeding three years. The Chair of the Audit and Risk Committee, Ms Lynelle Briggs AO, was appointed by the Director-General of Security on 6 February 2012, and her tenure was extended for a further 12 months. In 2014–15, the independence of the committee was strengthened through the inclusion of a third external member. Over the reporting period, six ASIO officers and three external members served as committee members; the committee currently comprises three ASIO officers and three independent members.

In 2014, the committee oversaw the rapid maturation of ASIO's Enterprise Risk Management Framework and began reviewing enterprise risk reporting from the other ASIO governance committees for risks requiring Executive Board attention.

The committee also oversaw the development of the business continuity framework, and future work by the committee is expected in this area through the review of divisional business continuity plans and supporting documentation.

The committee considered all audits undertaken by ASIO's Internal Audit Directorate during the period and monitored and reviewed ASIO's response and action against recommendations. It also reviewed ASIO's response and action in relation to any significant issues raised in external audit and review reports and better practice guides. The committee anticipates ASIO will make greater use of external providers to undertake performance—and management-initiated audits in 2015–16.

Communication and leadership meetings

Distinct from ASIO's corporate committees are ASIO's communication and leadership meetings. They do not represent decision-making points; instead, they focus on communicating current and emerging issues. The Senior Executive Meeting is a weekly meeting of all officers at ASIO Senior Executive Service (SES) Band 2 and above. The Senior Executive Service Meeting is a monthly meeting of all officers at SES Band 1 and above.

ASIO Consultative Council

The ASIO Consultative Council was established to enable ASIO management and staff to meet regularly, in a structured way, to discuss and resolve issues of interest and concern. The council is recognised by the Attorney-General. Two representatives from ASIO's Staff Association and two representatives from ASIO's management group constitute a quorum for the meeting, which occurs monthly.

Over the reporting period, the ASIO Consultative Council reviewed and updated its charter and membership, discussed and resolved issues relating to the relocation of staff to the BCB and transitional arrangements, received information and provided input into the organisation's efforts to comply with the Australian Government Employment Bargaining Framework, received feedback on the outcomes of the 2014 ASIO Staff Survey, and contributed to the review and development of numerous human resources policies and initiatives.

Government and public engagement

ASIO is committed to engaging with the government and business sectors, the media and the Australian public. While ASIO's outreach is often the provision of classified security-related advice, ASIO also delivers an appropriate level of public information. ASIO is the only Australian intelligence agency that tables an unclassified Report to Parliament.

ASIO can be contacted on the ASIO public line: **1800 020 648**.

ASIO Partnership Forums

The ASIO Partnership Forums are an important part of ASIO's government engagement. The forums are designed to provide participants from across government with a better understanding of ASIO's role, structure and priorities.

During the reporting period, ASIO held separate programs for the SES and senior officers (Executive Level 1, Executive Level 2 and equivalent military and police levels) from a range of Australian Government and state and territory agencies. Feedback from the forums was overwhelmingly positive, with attendees remarking on the high level of detail and contemporary information provided.

Stakeholder Satisfaction Survey

The Stakeholder Satisfaction Survey is undertaken by ASIO annually and provides a valuable insight into the levels of satisfaction of key partners. It also gives ASIO an understanding of the extent to which ASIO supports the attainment of partner agency outcomes. The survey has a focus on strategic and administrative issues.

Specifically, the survey seeks feedback from partners regarding their engagement experience with ASIO. 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 engaged an external consultant with extensive experience in the Australian Intelligence Community (AIC) to prepare and conduct the survey to ensure feedback was forthright. Preparations for the next survey, scheduled for July–August 2016, will be presented to senior management in late 2015.

Public statements and the media

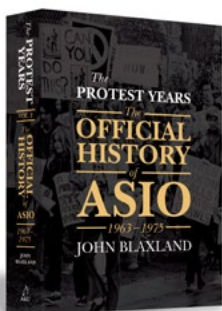
ASIO has a publicly listed media contact number and email address. ASIO routinely responds to media enquiries but does not comment on operations, investigations or individuals, nor does it comment on operational capabilities.

Attributable public statements are occasionally provided by the Director-General of Security through media responses, public speeches, or appearances at parliamentary or senate hearings. The Director-General of Security occasionally speaks at public seminars or conferences.

ASIO's media effort includes, where possible, assisting the media in its reporting of national security matters. For ASIO, it is an opportunity to clarify information and to inform the Australian public about matters of security concern. ASIO appreciates the value of accurate media reporting on national security.

Official History of ASIO

The Spy Catchers: The Official History of ASIO 1949–1963, volume 1 of the official history of ASIO, was launched by the Attorney-General on 7 October 2014 at the Museum of Australian Democracy, Old Parliament House, Canberra. The book was written by Professor David Horner AM of the Australian National University's (ANU) Strategic and Defence Studies Centre. Overall responsibility and direction for the project at the ANU lies with Professor Horner.



During the reporting period *The Spy Catchers* sold over 7000 copies, and a paperback version will be released in November 2015. *The Spy Catchers* was awarded the St Ermin's Hotel Intelligence Book of the Year Award 2015 in the United Kingdom.

The second volume in the series, titled *The Protest Years: The Official History of ASIO 1963-1975*, has been written by Dr John Blaxland and will be published by Allen & Unwin in October 2015.

The third volume, co-authored by Dr Blaxland and Dr Rhys Crawley, will undergo a similar clearance process as previous volumes to ensure it contains no information prejudicial to national security, while maintaining academic integrity.

The ANU researchers have viewed over 7000 unredacted ASIO files. Progress of the project is monitored by the History of ASIO Advisory Committee. The committee meets every six months and comprises Mr Geoff Gallop AC, Mr Jim Carlton AO, the Director-General of Security and a Deputy Director-General.

People

Overview

The counter-terrorism New Policy Proposal announced in August 2014 by the Australian Government dramatically shifted ASIO's people strategy. Consequently, in 2014-15 ASIO's people strategy changed from a previous focus on reducing and consolidating, to one of expanding capabilities and growth. This shift brings challenges in terms of recruitment, vetting and training.

The recruitment work undertaken has contributed towards all four goals 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 it to meet increasingly diverse and complex security challenges.

Workforce management and reporting

At the start of the 2014-15 reporting period, ASIO's workforce management focus was on downsizing activities, a result of recommendations from the internal *Review of the Staffing and Resource Allocation (2012-13)*. As the year progressed, the workforce management focus transitioned to increasing staffing numbers. This was necessary to fill existing critical vacancies and to grow capabilities to meet the requirements outlined in the counter-terrorism New Policy Proposal.

Activity throughout the reporting period focused on meeting growth targets and increasing capability. The initial period of growth in response to the counter-terrorism New Policy Proposal was particularly focused on increasing ASIO's corporate capability, such as recruitment and vetting functions to support the increased recruitment activity and to service the increased size of the organisation.

The Organisational Capability Program provides ASIO with mechanisms to deploy staff around ASIO in an effort to deliver on its mission. In 2014–15, ASIO continued to build on an expanded program, which was successful in providing staff with the ability to access opportunities to expand their own capability development, while ensuring that ASIO deploys staff to respond to the changing security environment. At the end of the reporting period, ASIO employed 1715.5 full-time equivalent staff.

Recruitment and staff movements

In 2014–15 recruitment remained a primary challenge. The focus was on growth, following the counter-terrorism New Policy Proposal, with a particular emphasis on the difficult-to-fill roles of intelligence officers, technical officers and information and communications technology (ICT) positions.

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. As university graduates are a target audience for intelligence officer and junior technical and ICT roles, ASIO attended 20 university career fairs around the country and conducted information sessions for targeted disciplines at a number of universities. This direct engagement with university students promoted ASIO and employment opportunities. It also provided the opportunity to explain the security-related requirements expected of applicants.

An online employment register was established during the reporting period, supported by a national recruitment awareness campaign. The register allows those interested in ongoing opportunities with ASIO to lodge their interest. As at 30 June 2015, over 4900 applications had been submitted. ASIO's expenditure on recruitment advertising for difficult-to-fill roles increased from \$599 739 in 2013–14 to \$871 902 in 2014–15, with both greater participation in university career fairs and the employment register national campaign attributing to the majority of the increase.

A recruitment agency panel was established during the reporting period, and this has broadened the organisation's capability and capacity in relation to recruitment.

OUTCOMES AND ACHIEVEMENTS

During the 2014–15 reporting period, ASIO:

- ▶ Had a strong focus on increasing recruitment intakes, including through the establishment of an online employment register, the promotion of ASIO, and employment opportunities at universities and career fairs. These activities increased ASIO's candidate pool. A panel of recruitment agencies was established to further broaden capability and capacity in recruitment.
- ▶ Continued the redevelopment of its employment relations framework. Extensive resources were focused on meeting the Australian Government Employment Bargaining Framework and working towards the establishment of a new workplace agreement, the last having expired in June 2014.
- ▶ Conducted a staff survey, the results of which were very positive. Focus groups were conducted to further discuss specific areas of concern, and the results from these sessions will be incorporated into the future people strategy program.
- ▶ Continued to work in close collaboration with partner agencies to meet a shared-services approach to areas across the AIC where potential efficiencies were identified.
- ▶ Actively engaged in the issue of gender equality across the broader AIC and led the development and implementation of a Gender Equity Strategy.
- ▶ Significantly strengthened relationships with international partner agencies on corporate and human resources matters, sharing corporate strategies and resources to build capability.
- ▶ Increased the focus of early intervention management practices when dealing with both performance and injury matters, encouraging management to engage early and prevent long-term injury or performance issues. This follows through to the active management of underperformance and misconduct matters, and the development of supporting policy and training to enable such management.

Human resources programs

In October 2014, all ASIO employees were invited to participate in the biannual Staff Satisfaction Survey, with 62.3 per cent of staff submitting a response. The majority of respondents expressed positive views about working for ASIO, with results exceeding the outcomes from past surveys in many areas, as well as exceeding Australian Public Service averages in several categories covered by the survey. Despite the overall results being very high, the favourable outcome did not extend to all categories captured by the survey. In an effort to better understand the various issues affecting these results, ASIO facilitated a number of focus groups with staff across the organisation. The outcomes of these focus groups have now been provided to ASIO's executive, and a range of strategies are being developed in an attempt to address the related issues.

The Director-General of Security is a member of the Heads of Intelligence Agency Meeting (HIAM). During 2014, HIAM initiated an investigation into the causes and implications of the existing gender imbalance across the AIC, noting that only 40 per cent of the AIC workforce is female, with the majority sitting within positions at the lower end of the organisational hierarchy. To help inform this conversation and ensure an accurate understanding of the current situation, ASIO participated in an AIC-wide gender equity survey and facilitated focus groups with both male and female members of staff. In recognition of the importance of this issue and the extensive evidence demonstrating the link between a diverse and inclusive workforce and improved

business performance, HIAM established a Gender Equity Steering Committee. Three SES members of ASIO's management team have been selected to represent ASIO on this committee and to lead the development and implementation of a Gender Equity Strategy.

Employment relations

Throughout the reporting period, ASIO devoted extensive resources to the development of a submission to the Australian Public Service Commissioner seeking approval for ASIO's proposed bargaining position on terms and conditions of employment. The submission was prepared in accordance with the Australian Government Public Sector Workplace Bargaining Policy, with the Public Service Commissioner's approval being a prerequisite to the commencement of formal workplace bargaining with employees. ASIO continues to liaise with representatives of the Australian Public Service Commission to refine its submission and demonstrate that any proposed wage increase is both affordable and offset by genuine productivity improvements.

ASIO Ombudsman

A functional review of the role of the ASIO Ombudsman was undertaken during the reporting period to ensure the role met business requirements, supported employment legislation and provided adequate staff and management support. A limited tender was advertised in appointing the role to ensure it remains a position of impartiality.

The role of the ASIO Ombudsman will continue to include the provision of impartial and confidential services to staff and management. The position is a vehicle to address staff-related concerns through advice, consultation and mediation—and as a reporting mechanism to management on trends or themes to enable appropriate remedial action. The Ombudsman role has a limited capacity to undertake complex formal investigations.

Throughout the coming year, the role of the Ombudsman will be increasingly promoted to ensure staff and management are aware that it is an avenue available to them.

In 2014–15 the ASIO Ombudsman provided advice in relation to 35 general queries. It provided more substantial advice on nine occasions on matters connected with performance, bullying and harassment.

The Ombudsman undertook four formal investigations: two investigations into allegations of inappropriate conduct in the workplace, one Public Interest Disclosure investigation, and one process inquiry into the advertising of internal job vacancies.

During this period, the ASIO Ombudsman provided input to a wide range of presentations relating to the role and the importance of the ASIO Values and Code of Conduct in establishing a proper and respectful workplace culture.

The Ombudsman continued to meet regularly with ASIO senior management and with representatives of the Staff Association to discuss the health of the workplace.

ASIO staff 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 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 internal audits conducted in 2013 and 2014 to determine ASIO's compliance with the WHS Act, ASIO implemented a number of projects, which have demonstrated:

- ▶ an increase in incident reporting by staff on work health and safety incidents and near misses
- ▶ a continued embedding of work health and safety principles in management training across the organisation.

ASIO's rehabilitation management system is audited annually in accordance with the requirements of the *2012 Guidelines for Rehabilitation Authorities*, issued by Comcare. The audit conducted during the reporting period identified two non-conformances, relating to the measuring of rehabilitation provider performance. Both non-conformances were addressed, by 30 June 2015, through the development and implementation of appropriate tools and mechanisms.

During the reporting period, health and safety representatives (HSRs) continued to actively engage with their work groups on the benefits of maintaining a safe work environment.

The First Aid Officer Program continued to be reviewed to ensure that ratios across ASIO relating to first aid are legislatively compliant.

ASIO's Work Health and Safety Committee meets quarterly to discuss relevant issues and to endorse work health and safety policies and procedures. Attendance is strong: HSRs, worker representatives and management meet with the mutual goal of ensuring safe working environments for all workers and visitors.

ASIO's HealthINT program continued to promote a healthy work-life balance. During the reporting period, staff were given the opportunity to undertake annual flu vaccinations, as well as appraisals to monitor their level of health in areas such as blood pressure, blood glucose and core strength.

ASIO's Comcare premium rate rose from 1.05 per cent of payroll in 2013–2014 to 1.18 per cent of payroll in 2014–15, which was attributed to an increase in the cost of injury claims in ASIO and across the Australian Government. However, Comcare has notified ASIO of a drop in its premium rate to 1.02 per cent, due in part to a reduction in estimated claim frequency based on trends in ASIO's performance over the last four years. ASIO's premium rate remains relatively low, at approximately 50 per cent of the average premium rate for other Australian Government agencies.

Training and development

In 2014–15, the Director-General of Security commissioned a review of ASIO's training needs to ensure that ASIO officers are well positioned to serve the needs of the government and the nation. The results of this review have informed ASIO's training over the final quarter of the reporting period and will continue to provide overarching direction into 2015–16.

Concurrently, increased resources were dedicated to ASIO's training in 2014–15 in recognition of ASIO's growing workforce and the challenges inherent in its operating and security environments.

There was also greater focus on enhancing existing partnerships with close national and international partners to deliver mutual training benefits and ensure best practice through benchmarking.

Intelligence training

The Intelligence Development Program (IDP) is ASIO's program for training and developing new intelligence officers in analytical and operational tradecraft. It was remodelled in late 2014 to provide an enhanced multifaceted program to deliver 'job ready' graduates. The IDP is an intensive program delivered through classroom-based learning and practical exercises, with short-term placements in the workplace to solidify learning outcomes. It also includes a final three 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 Technical Officer Graduate Program, a one-year structured program aimed at university graduates, commenced in 2014–15. It includes placements in a range of technical areas within ASIO's Technical Capabilities Division, including software development, technical development, telecommunications, computer forensics and technical operations. Participants in this program will graduate during the next reporting period. The Technical Officer Graduate Program was established in light of the criticality of ASIO's technical capabilities to achieving its intelligence mission.

During the reporting period, significant focus was also given to refining current, and build advanced and specialised development opportunities for practising intelligence professionals. These initiatives are forward-looking and anticipatory in nature to ensure our officers are well positioned to meet both current and future challenges inherent in the Australian and international security environments.

Personal safety and security

The safety and security of ASIO officers is necessarily the utmost priority, particularly in light of the heightened threat level in Australia. Accordingly, during the reporting period ASIO built on existing training to develop an overarching and comprehensive personal safety and security training continuum for the ASIO workforce. A diverse range of training opportunities are available to all staff within this continuum, with more advanced modules delivered to staff based on role requirements.

Core capability development

ASIO's investment in core capability development continued to deliver best-practice training in response to diverse business needs.

In 2014–15, ASIO's new starter induction program was refreshed and remodelled to provide an effective introduction to ASIO's security intelligence role, security culture and practices and a comprehensive understanding of ASIO's Values and Code of Conduct.

ASIO also conducted a review of its e-learning capability, resulting in the removal of obsolete modules and the republishing of in-house developed content, commencing with the mandatory training modules. Twelve new e-learning modules were published, including seven for personal safety and security and four relating to record-keeping, ensuring ASIO adheres to its obligations under relevant legislation. During the reporting period, ASIO recorded 3320 instances of mandatory and 1362 instances of non-mandatory e-learning completions.

During the reporting period, ASIO approved 3426 instances of face-to-face training, attended by 1752 employees across 60 training courses. This represents more than double the instances of face-to-face training that occurred in the previous reporting period. Such training includes management and leadership development (detailed below), corporate programs such as project management and financial management, personal safety and security training, and information technology courses.

Management and leadership development

Implementation of ASIO's Management and Leadership in Security Intelligence Strategy continued in 2014–15, including ASIO's shared-services approach to strengthening management and leadership capability across the AIC. The strategy includes three primary pathway programs:

- ▶ Management Skills in ASIO Workshop—aimed at new or current supervisors and managers requiring foundational skills and/or knowledge refresh at ASIO Employee (AE) 5–6 to ASIO Executive Employee (AEE) 3 levels.
- ▶ Introduction to Management Program—aimed at high-potential and aspiring frontline managers or new managers from the AE6 to AEE1 levels.
- ▶ Mastering Management Program—aimed at high-potential and high-performing AEE2 employees.

ASIO's continuous evaluation processes have identified clear evidence that the strategy's programs have had a positive impact. Through these evaluations, participants highlighted the significant development of new knowledge and skills over time, a positive impact in the workplace by applying these skills, and an increase in sharing resources and heightened collaboration across agencies in the AIC.

Study support and language development programs

Over the reporting period, 10 per cent of ASIO staff received support to undertake study or language development. In 2014–15, 119 officers participated in ASIO-supported study programs, at a cost of \$301 794. These programs included some 89 courses across a range of disciplines, including security and policy, conflict and strategic studies, business management, project management and information technology.

ASIO's Language Skills Development Program is aimed at building language capability, and ASIO employees are encouraged to apply for the program where relevant to their role. During the reporting period, ASIO spent \$432 335 on language training for 46 employees across 15 languages, following 54 language development business cases.

Rewards and recognition

ASIO acknowledges the exceptional work of staff through its Recognition Framework. The framework includes the provision of Director-General's medallions, which are awarded to teams and individuals in the categories of innovation, exceptional leadership, significant contribution and modelling ASIO Values. Staff commitment is recognised through the Foundation Day awards ceremony, with awards presented for service over 10, 20, 30 and 40 years.

Property

Ben Chifley Building

ASIO took possession of its new central office, the Ben Chifley Building (BCB), on 7 August 2014. The building is named after Australia's 16th Prime Minister, Joseph Benedict 'Ben' Chifley, Prime Minister at the time of ASIO's establishment. The BCB has been designed and built from the ground up to provide a purpose-built, high-security facility. The building is owned by the Department of Finance and leased to ASIO. It also houses the Australian Cyber Security Centre and the Australian Counter-Terrorism Centre.



*Australia's 16th Prime Minister,
Joseph Benedict 'Ben' Chifley*

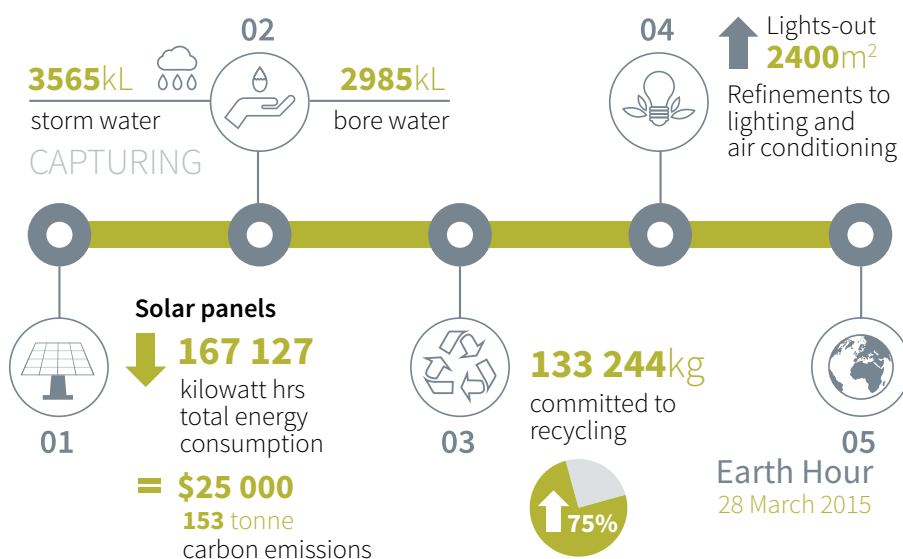
On possession of the building, security screening and the installation of ASIO ICT systems commenced. Relocation of staff into the BCB began in October 2014. The BCB effectively became ASIO's new central office in February 2015, when the Director-General of Security relocated from Russell. ASIO's relocation is now complete. The decommissioning of the previous headquarters in Russell is under way, and it is projected that the building will be returned to the Department of Finance late 2015.

Environmental performance

ASIO has continued its commitment to reduce its carbon footprint. Initiatives undertaken in 2014–15 have resulted in the following:

- ▶ a reduction of 167 127 kilowatt hours in ASIO's total energy consumption, through the installation and use of solar panels, saving approximately \$25 000 and 153 tonnes of carbon emissions
- ▶ a saving of approximately \$33 800 of potable water by capturing 3565 kilolitres of stormwater and using 2985 kilolitres of bore water
- ▶ the commitment to recycling of 133 244 kilograms of waste—an increase of 75 per cent compared to the previous year—including paper products, printer toner cartridges, batteries, scrap metal and fluorescent light tubes
- ▶ the extension of lights-out data centre operations by 2400 metres squared
- ▶ ongoing refinements to operating times for building lighting and air conditioning to meet staffing and seasonal requirements
- ▶ participation in the eighth consecutive Earth Hour event, on 28 March 2015.

Figure 2: Environmental performance



Financial services

Purchasing

Throughout 2014–15, ASIO adhered to the Commonwealth Procurement Rules and associated policy and guidelines. This involved exercising contemporary procurement advice and methodology in order to ensure that 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 29 new consultancy contracts during 2014–15, resulting in total actual expenditure of \$802 821. In addition, 17 ongoing consultancy contracts were active during the reporting period, involving total actual expenditure of \$496 194. Total consultancy expenditure has increased by \$101 718 from 2013–14.

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 69 open tenders during 2014–15. 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 subject to the release of records under the *Archives Act 1983* (Archives Act), which allows the public to request access to Australian Government records in the open period. The open period currently covers all records created in or before 1989.

All public requests for ASIO records are made to the National Archives of Australia (NAA) in the first instance, and the NAA passes the request to ASIO. ASIO assesses relevant records and then provides advice to the NAA about whether the records contain information that should be exempt from public release under section 33(1) of the Archives Act. Exemption decisions are based on whether the information is sensitive now, not whether it was sensitive at the time the record was created.

ASIO continues to face challenges in meeting the 90-day legislative turnaround time. ASIO prioritises requests to provide equitable access and gives greater priority to requests from those seeking records on themselves or family members.

This is in accordance with the 1992 direction from the Parliamentary Joint Committee on ASIO, endorsed in 2008 by the Inspector-General of Intelligence and Security. Currently 10 individual applicants are responsible for 50 per cent of requests for access.

In 2014–15 requests for access to ASIO records continued to increase, with a total of 811 requests completed.

Applicants dissatisfied with exemptions claimed by ASIO may request that NAA reconsider the decision. In 2014–15, there was one reconsideration by NAA, which upheld the ASIO exemptions.

Applicants may also appeal to the Administrative Appeals Tribunal (AAT) regarding ASIO exemptions or if their request is not completed within 90 days. One application from 2012–13 continues to be the subject of action under the auspices of the AAT; this matter concerns ‘deemed refusal’ of multiple requests. During the reporting period, hearings on this matter led to some reprioritisation by the applicant of other access requests to ASIO. There were no new AAT appeals in this reporting period.

Table 4: Release of ASIO records

	2012–13	2013–14	2014–15
Applications for record access	441	773	790
Requests completed	357	532	811
Number of pages examined	44 141	56 261	52 829

Transfer of information holdings to Ben Chifley Building

ASIO completed the audit and secure transport of hard-copy information holdings to the BCB through the Records Audit and Migration Project. This program included consultation with external agencies and NAA inspection of records repositories.



Part 6

FINANCIAL STATEMENTS

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2015 comply with subsection 42(2) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and are based on properly maintained financial records as per subsection 41(2) of the PGPA Act.

In my opinion, at the date of this statement, there are reasonable grounds to believe that ASIO will be able to pay its debts as and when they fall due.



Duncan Lewis
Director-General of Security

10 September 2015



INDEPENDENT AUDITOR'S REPORT

To the Attorney-General

I have audited the accompanying annual financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2015, which comprise:

- 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; and
- Notes to and forming part of the Financial Statements including a Summary of Significant Accounting Policies.

Accountable Authority's Responsibility for the Financial Statements

The Director General of Security is responsible under the *Public Governance, Performance and Accountability Act 2013* for the preparation and fair presentation of annual financial statements that comply with Australian Accounting Standards and the rules made under that Act. The Director General of Security is also responsible for such internal control as is necessary to enable the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

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

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

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

Accountable Authority of the entity, 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

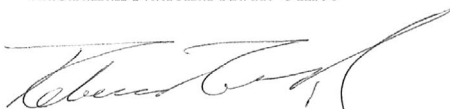
In conducting my audit, I have followed the independence requirements of the Australian National Audit Office, which incorporate the requirements of the Australian accounting profession.

Opinion

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

- (a) comply with Australian Accounting Standards and the *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*; and
- (b) present fairly the financial position of the Australian Security Intelligence Organisation as at 30 June 2015 and its financial performance and cash flows for the year then ended.

Australian National Audit Office



Rebecca Reilly
Executive Director

Delegate of the Auditor-General

Canberra
10 September 2015

STATEMENT OF COMPREHENSIVE INCOME for the period ended 30 June 2015

	Notes	2015 \$ '000	2014 \$ '000
EXPENSES			
Employee benefits	4A	221,554	218,724
Suppliers	4B	179,933	137,911
Depreciation and amortisation	4C	63,800	49,107
Other	4D	759	1,081
Total expenses		466,046	406,823
OWN-SOURCE INCOME			
Revenue			
Sale of goods and rendering of services	5A	16,539	13,513
Other revenue	5B	3,778	660
Gains	5C	810	145
Total own-source income		21,127	14,318
Net cost of services		444,919	392,505
Revenue from government	5D	368,423	346,181
Total comprehensive loss attributable to the Australian Government		(76,496)	(46,324)

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

STATEMENT OF FINANCIAL POSITION

as at 30 June 2015

	Notes	2015 \$ '000	2014 \$ '000
ASSETS			
Financial assets			
Cash and cash equivalents		22,023	17,101
Trade and other receivables	7A	93,975	200,750
Other financial assets	7B	4,998	5,453
Total financial assets		120,996	223,304
Non-financial assets			
Land and buildings	8A,D	175,571	269,049
Property, plant and equipment	8B,D	159,787	84,264
Intangibles	8C,E	36,868	26,110
Other non-financial assets	8F	25,354	22,641
Total non-financial assets		397,580	402,064
Total assets		518,576	625,368
LIABILITIES			
Payables			
Suppliers	9A	16,622	15,647
Lease incentives	9B	1,171	1,674
Other payables	9C	29,451	24,813
Total payables		47,244	42,134
Provisions			
Employee provisions	10A	62,608	56,537
Restoration obligations	10B	6,281	6,088
Other provisions		-	8,000
Total provisions		68,889	70,625
Total liabilities		116,133	112,759
Net assets		402,443	512,609
EQUITY			
Parent equity interest			
Contributed equity		580,376	614,046
Reserves		17,930	17,930
Retained surplus (deficit)		(195,863)	(119,367)
Total equity		402,443	512,609

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

STATEMENT OF CHANGES IN EQUITY for the period ended 30 June 2015

	2015 \$'000	2014 \$'000
RETAINED EARNINGS		
Opening balance	(119,367)	(73,043)
Comprehensive income		
Deficit for the period	(76,496)	(46,324)
Closing balance	(195,863)	(119,367)
ASSET REVALUATION SURPLUS		
Opening balance	17,930	17,930
Closing balance	17,930	17,930
CONTRIBUTED EQUITY/CAPITAL		
Opening balance	614,046	553,907
Transactions with owners		
Distributions to owners		
Returns of capital - reduction of appropriation	(82,877)	-
Contributions by owners		
Equity injection - appropriation	16,028	165
Departmental capital budget	33,179	59,974
Closing balance	580,376	614,046
Closing balance attributable to the Australian Government	402,443	512,609

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

CASH FLOW STATEMENT for the period ended 30 June 2015

	Notes	2015 \$ '000	2014 \$ '000
OPERATING ACTIVITIES			
Cash received			
Appropriations		410,284	411,665
Sales of goods and rendering of services		16,973	14,061
Net GST received		17,004	15,240
Other		-	15,549
Total cash received		444,261	456,515
Cash used			
Employees		212,749	219,049
Suppliers		192,272	165,618
Section 74 receipts		22,055	31,030
Total cash used		427,076	415,697
Net cash from operating activities	11	17,185	40,818
INVESTING ACTIVITIES			
Cash received			
Proceeds from sales of property, plant and equipment		623	840
Total cash received		623	840
Cash used			
Purchase of property, plant and equipment		39,861	44,593
Purchase of intangibles		18,797	14,346
Total cash used		58,658	58,939
Net cash used by investing activities		(58,035)	(58,099)
FINANCING ACTIVITIES			
Cash received			
Contributed equity		45,772	20,165
Total cash received		45,772	20,165
Net cash from financing activities		45,772	20,165
Net increase in cash held		(4,922)	2,884
Cash and cash equivalents at the beginning of the reporting period		17,101	14,217
Cash and cash equivalents at the end of the reporting period		(22,023)	17,101

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

SCHEDULE OF COMMITMENTS

as at 30 June 2015

		2015	2014
	Notes	\$ '000	\$ '000
BY TYPE			
Commitments receivable			
Sublease rental income		18,052	632
Net GST recoverable on commitments		56,764	60,085
Total commitments receivable		74,816	60,717
Commitments payable			
Capital commitments			
Land and buildings	A	7,728	5,411
Property, plant and equipment	A	2,982	587
Intangibles		3,315	396
Total capital commitments		14,025	6,394
Other commitments			
Operating leases	B	606,921	640,319
Other		36,483	18,690
Total other commitments		643,404	659,009
Net commitments by type		582,614	604,686

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 leases for office accommodation and agreements for the provision of motor vehicles to officers.
- Various arrangements apply to the review of lease payments including review based on the consumer price index and market appraisal.

SCHEDULE OF COMMITMENTS

continued

	2015	2014
Notes	\$ '000	\$ '000
BY MATURITY		
Commitments receivable		
Operating lease		
One year or less	1,753	632
From one to five years	9,589	-
Over five years	6,710	-
Total operating lease income	18,052	632
Other commitments receivable		
One year or less	7,119	6,283
From one to five years	19,172	20,095
Over five years	30,473	33,707
Total other commitments receivable	56,764	60,086
Total commitments receivable	74,816	60,717
Commitments payable		
Capital commitments		
One year or less	13,220	6,394
From one to five years	805	-
Total capital commitments	14,025	6,394
Operating lease commitments		
One year or less	51,213	49,437
From one to five years	213,123	220,104
Over five years	342,585	370,779
Total operating lease commitments	606,921	640,320
Other commitments		
One year or less	26,803	15,949
From one to five years	9,680	2,740
Total other commitments	36,483	18,689
Total commitments payable	657,429	665,403
Net commitments by maturity	582,614	604,686

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 2015

- Note 1: Summary of significant accounting policies
- Note 2: Events after the reporting period
- Note 3: Net cash appropriation arrangements
- Note 4: Expenses
- Note 5: Income
- Note 6: Fair value measurements
- Note 7: Financial assets
- Note 8: Non-financial assets
- Note 9: Payables
- Note 10: Provisions
- Note 11: Cash flow reconciliation
- Note 12: Contingent liabilities and assets
- Note 13: Senior management personnel remuneration
- Note 14: Financial instruments
- Note 15: Appropriations
- Note 16: Reporting of outcomes
- Note 17: Budgetary reports and explanation of major variances

Note 1: Summary of significant accounting policies

1.1 Objective of ASIO

ASIO is an Australian Government-controlled not-for-profit entity. As authorised by the *Australian Security Intelligence Organisation Act 1979*, 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.

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 42 of the *Public Governance, Performance and Accountability Act 2013*.

The financial statements have been prepared in accordance with:

- ▶ Financial Reporting Rule (FRR) for reporting periods ending on or after 1 July 2014; and
- ▶ Australian Accounting Standards and Interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial statements have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets and liabilities at fair value. 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 FRR, 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 rising under executory contracts are not recognised unless required by an accounting standard. Liabilities and assets that are unrecognised are reported in the schedule of commitments or the contingencies note.

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

1.3 Significant accounting judgments and estimates

In the process of applying the accounting policies listed in this note, ASIO has made the following judgments that have the most significant impact on the amounts recorded in the financial statements:

- ▶ The fair value of land and buildings has been taken to be the market value of similar properties or depreciated replacement cost of assets 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.
- ▶ Leave provisions involve assumptions based on the expected tenure of existing staff, patterns of leave claims and payouts, future salary movements and future discount rates.

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 ASIO.

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 ASIO.

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 and
- ▶ it is probable that the economic benefits associated with the transaction will flow to ASIO.

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 ASIO.

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.

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. 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 disposal of assets are recognised when control of the asset has passed to the buyer.

1.7 Transactions with the government as owner

Equity injections

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

1.8 Employee benefits

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

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.

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 and Deregulation'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 government. ASIO accounts for the contributions as if they were contributions to defined contribution plans.

Superannuation payable as at 30 June 2015 represents outstanding contributions for the final fortnight of the financial year.

1.9 Leases

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 hierarchy to have occurred at the end of the reporting period.

1.11 Financial assets

Cash

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

- ▶ cash on hand
- ▶ deposits on demand in bank accounts
- ▶ cash held by outsiders.

Loans and receivables

Trade receivables are classified as 'loans and receivables' and recorded at face value less any impairment. Trade receivables are recognised where ASIO becomes party to a contract and has a legal right to receive cash. Trade receivables are derecognised on payment.

Impairment of financial assets

Financial assets are assessed for impairment at the end of each reporting period. Allowances are made when collectability of the debt is no longer probable.

1.12 Financial liabilities

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). Supplier and other payables are derecognised on payment.

1.13 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.

1.14 Acquisition of assets

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.

Purchases of non-financial assets are initially recognised 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).

1.15 Property, plant and equipment

Revaluations

Following initial recognition at cost, property, plant and equipment is carried at fair value less subsequent 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.

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.

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

	2015	2014
Buildings on freehold land	8–60 years	8–60 years
Leasehold improvements	lease term	lease term
Plant and equipment	2–25 years	2–25 years

Impairment

All assets were assessed for impairment at 30 June 2015. 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.

Derecognition

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

1.16 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 (2013–14: 1–10 years).

All software assets were assessed for indications of impairment as at 30 June 2015.

1.17 Taxation

ASIO is exempt from all forms of taxation except fringe benefits tax and the goods and services tax (GST).

Revenues, expenses and assets are recognised net of GST except:

- ▶ where the amount of GST incurred is not recoverable from the Australian Taxation Office; and
- ▶ for receivables and payables.

1.18 Legal

The Australian Government continues to have regard to developments in case law, including the High Court's most recent decision on Commonwealth expenditure in *Williams v Commonwealth [2014] HCA 23*, as they contribute to the larger body of law relevant to the development of Commonwealth programs. In accordance with its general practice, the Government will continue to monitor and assess risk and decide on any appropriate actions to respond to risks of expenditure not being consistent with constitutional or other legal requirements.

Note 2: Events after the reporting period

There was no subsequent event that had the potential to significantly affect the ongoing structure or financial activities of ASIO.

Note 3: Net cash appropriation arrangements

	2015	2014
	\$ '000	\$ '000
Total comprehensive income/(loss) plus depreciation and amortisation expenses previously funded through revenue appropriations	(12,696)	2,783
Less depreciation and amortisation expenses previously funded through revenue appropriation	(63,800)	(49,107)
Total comprehensive loss as per statement of comprehensive income	(76,496)	(46,324)

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.

Note 4: Expenses

Note 4A: Employee benefits

Wages and salaries	169,592	166,121
Superannuation		
Defined contribution plans	14,156	13,070
Defined benefit plans	17,084	17,998
Leave and other entitlements	20,300	14,436
Separation and redundancies	422	7,099
Total employee benefits	221,554	218,724

	2015	2014
	\$ '000	\$ '000

Note 4B: Suppliers

Provision of goods

Related entities	722	314
External entities	10,206	11,457

Rendering of services

Related entities	16,585	21,218
External entities	108,133	82,402

Operating lease payments

Related entities	33,990	3,879
External entities	7,718	17,027

Workers' compensation premiums	2,579	1,614
--------------------------------	-------	-------

Total supplier expenses	179,933	137,911
--------------------------------	----------------	----------------

Note 4C: Depreciation and amortisation

Depreciation

Property, plant and equipment	38,147	24,356
Buildings	17,614	17,156
Total depreciation	55,761	41,512

Amortisation - intangibles - computer software	8,039	7,595
---	--------------	--------------

Total depreciation and amortisation	63,800	49,107
--	---------------	---------------

Note 4D: Other expenses

Finance costs

Unwinding of discount - restoration obligations	193	153
---	-----	-----

Write-down and impairment of assets from

Impairment of receivables	4	2
Write-down of property, plant and equipment	376	629

Losses from asset sales	186	294
-------------------------	-----	-----

Foreign exchange losses	-	3
-------------------------	---	---

Total other expenses	759	1,081
-----------------------------	------------	--------------

Note 5: Income

	2015	2014
	\$ '000	\$ '000

OWN SOURCE REVENUE

Note 5A: Sale of goods and rendering of services

Sale of goods

Related entities	24	6
External entities	13	1

Rendering of services

Related entities	14,704	13,256
External entities	1,798	250

Total sale of goods and rendering of services	16,539	13,513
--	---------------	---------------

Note 5B: Other revenue

Rental income – operating lease	3,283	660
Royalties	19	-
Other	476	-
Total other revenue	3,778	660

GAINS

Note 5C: Gains

Resources received free of charge

Remuneration of auditors	130	120
Other	632	-
Other gains	48	25
Total gains	810	145

REVENUE FROM GOVERNMENT

Note 5D: Revenue from government

Appropriation – Departmental appropriations	368,423	346,181
--	----------------	----------------

Note 6: Fair value measurements

The levels of the fair value hierarchy are:

- Level 1: Quoted prices (unadjusted) in active markets for identical assets that ASIO can access at measurement date.
- Level 2: Inputs other than quoted prices included within level 1 that are observable for the asset, either directly or indirectly.
- Level 3: Unobservable inputs for the asset.

Fair value measurements – valuation technique and the inputs used for assets 2015

	Category	Fair value		Valuation technique	Inputs used	Range [weighted average] ¹
		2015 \$'000	2014 \$'000			
Land	Level 3	1,565	1,565	Market approach	Price per square metre	10.0% [10.0%]
Buildings on freehold land	Level 3	1,321	1,361	Market approach	Price per square metre	10.0% [10.0%]
Buildings (specialised)	Level 3	3,509	3,731	Depreciated replacement cost	Replacement cost new	N/A
					Consumed economic benefit/obsolescence of asset	2.9% – 12.5% [3.2%] per annum
Leasehold improvements	Level 3	159,540	29,611	Depreciated replacement cost	Replacement cost new	N/A
					Consumed economic benefit/obsolescence of asset	6.4% – 25.5% [7.0%] per annum
Plant and equipment	Level 2	36,461	43,946	Market approach	Adjusted market transactions	N/A
Plant and equipment	Level 3	15,841	-	Market approach	Adjusted market transactions	15.0% [15.0%]
Plant and equipment (specialised)	Level 3	104,046	38,698	Depreciated replacement cost	Replacement cost new	N/A
					Consumed economic benefit/obsolescence of asset	50.0% – 33.33% [18.2%] per annum
Total		322,283	118,912			

¹ Significant unobservable inputs only. Not applicable for assets or liabilities in the Level 2 category.

A reconciliation of movements in property, plant and equipment has been included in Note 8D.

Fair value measurement

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

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

ASIO did not measure any non-financial assets at fair value on a non-recurring basis as at 30 June 2015.

ASIO conducts a review of the valuation model as an asset materiality review at least once every 12 months (with a formal revaluation undertaken once every three years). If a particular asset class

experiences significant and volatile changes in fair value (i.e. where indicators suggest that the value of the class has changed materially since the previous reporting period), that class is subject to specific valuation in the reporting period, where practicable, regardless of the timing of the last specific valuation. ASIO engaged Australian Valuation Solutions (AVS) to undertake a valuation materiality review and confirm the models developed comply with AASB 13.

There have been changes to the valuation techniques for assets in the property, plant and equipment class. In instances where sufficient observable inputs, such as market transactions of similar assets, were (not) identified in this financial year, the valuation technique was changed from Depreciated Replacement Cost (Market) approach to a Market (Depreciated Replacement Cost) approach. The changes in valuation technique did not result in a material change to fair value.

Unobservable inputs

Significant level 3 inputs

Sensitivity of the fair value measurement to changes in unobservable 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 the price per square metre would result in a significantly higher/(lower) fair value measurement.

Property, plant & equipment (PPE) – adjusted market transactions

The significant unobservable inputs used in the fair value measurement of PPE assets relates to the market demand and valuer's judgement to determine the fair value measurement of these assets.

A significant increase (decrease) in the lease term associated with the assets would result in a significantly higher (lower) fair value measurement.

Buildings, leasehold improvements, property, 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 (DRC) approach. Under the DRC approach the estimated cost to replace is calculated and then adjusted to take into account its consumed economic benefit/asset obsolescence (accumulated depreciation). Consumed economic benefit/asset obsolescence has been determined based on professional judgement regarding physical, economic and external obsolescence factors relevant to the asset under consideration.

A significant increase/(decrease) in the

- price per square metre (buildings)
- lease term (leasehold improvements)
- consumed economic benefit/obsolescence of plant & equipment

would result in a significantly higher/(lower) fair value measurement.

Note 7: Financial assets

	2015	2014
	\$ '000	\$ '000

Note 7A: Trade and other receivables

Goods and services receivables

Related entities	3,240	2,175
External entities	1,559	384
Total receivables for goods and services	4,799	2,559
Appropriations receivable for existing programs	84,441	195,805
GST receivable from the Australian Taxation Office	4,735	2,386
Total trade and other receivables (net)	93,975	200,750

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

Age of receivables

Not overdue	93,807	199,486
Overdue by		
less than 30 days	17	127
31 to 60 days	55	75
61 to 90 days	3	136
more than 90 days	94	926
Total receivables (gross)	93,975	200,750

Credit terms for goods and services were within 30 days (2014: 30 days).

Financial assets were assessed for impairment at 30 June 2015. No indicators of impairment have been identified.

Note 7B: Other financial assets

Accrued revenue	4,998	5,453
------------------------	--------------	--------------

All accrued revenue is expected to be recovered in no more than 12 months.

Note 8: Non-financial assets

	2015	2014
	\$ '000	\$ '000

Note 8A: Land and buildings

Land at fair value	1,565	1,565
Buildings on freehold land		
Fair value	6,688	5,635
Accumulated depreciation	(1,858)	(543)
Total buildings on freehold land	4,830	5,092
Leasehold improvements		
Work in progress	9,636	232,780
Fair value	190,058	50,315
Accumulated depreciation	(30,518)	(20,703)
Total leasehold improvements	169,176	262,392
Total land and buildings	175,571	269,049

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 8B: Property, plant and equipment

Property, plant and equipment

Work in progress	3,439	1,620
Fair value	219,079	111,507
Accumulated depreciation	(62,731)	(28,863)
Total property, plant and equipment	159,787	84,264

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.

Note 8C: Intangibles

Computer software

Purchased	31,498	26,743
Internally developed – in progress	9,615	8,481
Internally developed – in use	38,170	26,396
Accumulated amortisation	(42,332)	(35,428)
Accumulated impairment	(82)	(82)
Total computer software	36,868	26,110
Total intangibles	36,868	26,110

No additional indicators of impairment were found for intangible assets.

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

Note 8D: Reconciliation of the opening and closing balances of property, plant and equipment

	Land \$'000	Buildings \$'000	Buildings: leasehold improvement \$'000	Property, plant & equipment \$'000	Total \$'000
--	----------------	---------------------	--	---	-----------------

2015

As at 1 July 2014

Gross book value	1,565	5,635	283,095	113,127	403,422
Accumulated depreciation and impairment	-	(543)	(20,703)	(28,863)	(50,110)
Net book value 1 July 2014	1,565	5,092	262,392	84,264	353,313
Additions by purchase	-	1,053	10,424	27,505	38,982
Depreciation expense	-	(1,314)	(16,301)	(38,147)	(55,761)
Disposals - other	-	-	(1)	(1,174)	(1,175)
Reclassification	-	-	(87,338)	87,338	-
Net book value 30 June 2015	1,565	4,830	169,176	159,787	335,358

Gross book value	1,565	6,688	199,694	222,518	430,465
Accumulated depreciation and impairment	-	(1,858)	(30,518)	(62,731)	(95,107)
Net book value 30 June 2015	1,565	4,830	169,176	159,787	335,358

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	262,390	84,264	353,313

Gross book value	1,565	5,635	283,095	113,127	403,422
Accumulated depreciation and impairment	-	(543)	(20,703)	(28,863)	(50,110)
Net book value 30 June 2014	1,565	5,092	262,392	84,264	353,313

Note 8E: Reconciliation of the opening and closing balances of intangibles

	Computer software		
	Internally developed	Purchased	Total
	\$'000	\$'000	\$'000

2015

As at 1 July 2014

Gross book value	34,878	26,743	61,621
Accumulated amortisation and impairment	(19,365)	(16,145)	(35,510)
Net book value 1 July 2014	15,513	10,598	26,110

Additions by purchase or internally developed	13,235	5,592	18,827
Amortisation expense	(3,497)	(4,542)	(8,039)
Disposals – other	(4)	(26)	(31)
Net book value 30 June 2015	25,247	11,622	36,868

Net book value 30 June 2015 represented by:

Gross book value	47,785	31,498	79,283
Accumulated amortisation and impairment	(22,539)	(19,875)	(42,414)
	25,246	11,622	36,868

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

Note 8F: Other non-financial assets

	2015	2014
	\$ '000	\$ '000

Prepayments	25,354	22,641
Total other non-financial assets	25,354	22,641

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

No more than 12 months	19,936	14,578
More than 12 months	5,418	8,063
	25,354	22,641

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

Note 9: Payables

Note 9A: Suppliers

Trade creditors and accruals	16,622	15,647
-------------------------------------	---------------	---------------

Supplier payables expected to be settled within 12 months

Related entities	1,154	1,430
External entities	15,468	14,217
	16,622	15,647

Settlement is usually made within 30 days.

Note 9B: Lease incentives

Lease incentives	1,171	1,674
-------------------------	--------------	--------------

Lease incentives are expected to be settled in

No more than 12 months	427	502
More than 12 months	744	1,172
	1,171	1,674

Note 9C: Other payables

Salaries and wages	6,503	5,710
Superannuation	1,061	933
Unearned income	11,441	13,400
Fringe benefits tax	2,570	757
Rent payable	7,876	4,013
Total other payables	29,451	24,813

	2015	2014
	\$ '000	\$ '000

Rent payable is expected to be settled in

No more than 12 months	1,098	503
More than 12 months	6,778	3,510
	7,876	4,013

Unearned income is expected to be settled in

No more than 12 months	1,651	2,510
More than 12 months	9,790	10,890
	11,441	13,400

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

Note 10: Provisions

Note 10A: Employee provisions

Leave	62,347	56,206
Superannuation	261	331
Total employee provisions	62,608	56,537

Employee provisions are expected to be settled in

No more than 12 months	17,271	16,255
More than 12 months	45,337	40,282
	62,608	56,537

Note 10B: Restoration obligations

Restoration obligations	6,281	6,088
--------------------------------	--------------	--------------

Restoration obligations are expected to be settled in

No more than 12 months	2,401	2,322
More than 12 months	3,880	3,766
	6,281	6,088

Carrying amount 1 July 2014	6,088	10,024
Additional provisions	-	5
Extinguish obligation for restoration	-	(4,094)
Unwinding of discount or change in discount rate	193	153
Closing balance	6,281	6,088

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 11: Cash flow reconciliation

	2015	2014
	\$ '000	\$ '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	(22,023)	17,101
Statement of Financial Position	22,023	17,101

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

Net cost of services	(444,919)	(392,505)
Revenue from government	368,423	346,181

Adjustments for non-cash items

Depreciation/amortisation	63,800	49,107
Net write-down of non-financial assets	376	629
Loss on disposal of assets	186	294

Changes in assets/liabilities

(Increase)/decrease in receivables	27,333	44,109
(Increase)/decrease in accrued revenue	455	725
(Increase)/decrease in prepayments	(2,713)	(8,001)
Increase/(decrease) in employee provisions	6,071	(1,549)
Increase/(decrease) in other provisions	(8,000)	8,000
Increase/(decrease) in restoration obligations	193	(3,936)
Increase/(decrease) in lease incentives	(503)	(527)
Increase/(decrease) in supplier payables	1,845	(6,208)
Increase/(decrease) in other payables	4,638	4,499
Net cash from/(used by) operating activities	17,185	40,818

Note 12: Contingent liabilities and assets

	2015	2014
	\$ '000	\$ '000

Quantifiable contingencies

ASIO's contingent liabilities relate to claims for damages or costs. 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	1,125	210
New contingent liabilities recognised	150	1,125
Liabilities realised	-	(125)
Obligations expired	(1,125)	(85)
Total contingent liabilities	150	1,125

Unquantifiable contingencies

At 30 June 2015, 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. These were not included in the table above.

Significant remote contingencies

ASIO does not have any significant remote contingencies.

Note 13: Senior management personnel remuneration

	2015	2014
	\$	\$

Short-term employee benefits

Salary and allowances	10,647,622	9,255,017
Motor vehicle and other fringe benefits	781,749	874,744

Long-term employee benefits

Annual leave accrued	1,015,082	950,790
Long-service leave accrued	325,437	308,966

Termination benefits

Voluntary redundancy payments	-	631,148
-------------------------------	---	---------

Post-employment benefits

Superannuation	2,257,292	2,190,406
----------------	-----------	-----------

Total senior management personnel remuneration	15,027,181	14,211,070
---	-------------------	-------------------

The total number of senior management personnel included above is 56. (2014: 60)

Note 14: Financial instruments

	2015	2014
	\$'000	\$'000

Note 14A: Categories of financial instruments

Financial assets

Loans and receivables

Cash	22,023	17,101
Trade receivables	4,799	2,559
Accrued revenue	4,998	5,453
Total financial assets	31,820	25,113

Financial liabilities

At amortised cost

Trade creditors and accruals	16,622	15,647
Total financial liabilities	16,622	15,647

The net fair value of the financial assets and liabilities are at their carrying amounts. ASIO derived no interest income from financial assets in either the current or prior year.

There is no net gain or loss from financial assets or liabilities through profit or loss for the period ending 30 June 2015 (2014: Nil).

Note 14B: Credit risk

ASIO is exposed to minimal credit risk with the maximum exposure arising from potential debtor default. This amount is equal to the total amount of receivables for services as indicated in the Statement of Financial Position.

Note 14C: Liquidity risk

ASIO has sufficient available financial assets to meet all financial liabilities at 30 June 2015.

Note 14D: Market risk

ASIO holds basic financial instruments that do not expose it to market risks. ASIO is not exposed to 'Currency risk', 'Other price risk' or 'Interest rate risk'.

Note 15: Appropriations

Note 15A: Annual appropriations (recoverable GST exclusive)

	Departmental	
	Ordinary annual services \$ '000	Other services - equity \$ '000
2015		
Appropriation Act		
Annual appropriation	401,602	16,028
PGPA Act		
Section 74	22,055	-
Total appropriation	423,657	16,028
Appropriation applied (current and prior years)	(442,159)	(21,090)
Variance	(18,502)	(5,062)
Section 51 determination ¹	(32,877)	
2014		
Appropriation Act		
Annual appropriation	417,024	165
Appropriations reduced	(10,869)	-
FMA Act		
Section 30	2,764	-
Section 31 (GST excl.)	31,030	-
Total appropriation	439,949	165
Appropriation applied (current and prior years)	(437,478)	(165)
Variance	2,471	-

Variances in 2014–15 are due to prior year appropriations applied in the current year.

The following entities spend money from the Consolidated Revenue Fund on behalf of ASIO:

- Department of Finance relating to the construction of a new building: \$12.116m (2014: \$17.639m).
- Department of Foreign Affairs and Trade relating to services overseas: \$7.249m (2014: \$8.093m).

¹ Unspent Departmental Capital Appropriation from 2012–13, 2013–14 and 2014–15 was permanently re-profiled with approval of the Expenditure Review Committee of Cabinet.

Note 15B: Departmental Capital Budgets (recoverable GST exclusive)

	Departmental
	Ordinary annual services
	Departmental Capital Budget
	\$ '000

2015

Appropriation Act

Annual capital budget	33,179
Appropriations applied	
Payments for non-financial assets	(24,682)
Variance	8,497

Section 51 determinations¹ (32,877)

2014

Appropriation Act

Annual capital budget	59,974
Appropriations applied	
Payments for non-financial assets	-
Variance	59,974

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.

Variance in 2014–15 is due to prior year appropriations applied in the current year and Section 51 re-profile¹.

¹ Unspent departmental capital appropriation from 2012–13, 2013–14 and 2014–15 was permanently re-profiled with approval of the Expenditure Review Committee of Cabinet.

Note 15C: Unspent departmental annual appropriations (recoverable GST exclusive)

	2015	2014
	\$ '000	\$ '000
Appropriation Act (No. 1) 2014–15	80,218	-
Appropriation Act (No. 1) 2013–14	23,020	160,095
Appropriation Act (No. 1) 2012–13	3,227	47,749
Appropriation Act (No.2) 2012–13	-	5,062
Total	106,465	212,906

Note 16: Reporting of outcomes

	2015	2014
	\$ '000	\$ '000
Departmental		
Expenses	466,046	406,823
Own-source income from		
Non-government sector	(1,878)	(276)
Government sector	(19,249)	(14,042)
Net cost of outcome delivery	444,919	392,505

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

Note 17: Budgetary reports and explanation of major variances

The following tables provide a comparison of the original budget presented in the 2014–15 Portfolio Budget Statements and the 2014–15 actual amounts in the financial statements. The budget is not audited.

	Budget estimate		Variance	Note
	Actual	Original ¹		
	\$ '000	\$ '000	\$ '000	

Statement of Comprehensive Income for the period ended 30 June 2015

EXPENSES

Employee benefits	221,554	217,691	(3,863)	A B
Suppliers	179,933	170,716	(9,217)	A B
Depreciation and amortisation	63,800	64,982	1,182	
Other	759	-	(759)	
Total expenses	466,046	453,389	(12,657)	

OWN-SOURCE INCOME

Revenue

Sale of goods and rendering of services	16,539	15,278	(1,261)	
Other revenue	3,778	2,820	(958)	
Gains	810	115	(695)	
Total own-source income	21,127	18,213	(2,914)	

Net cost of services	444,919	435,176	(9,743)	
-----------------------------	----------------	---------	----------	--

Revenue from government	368,423	357,194	(11,229)	A
-------------------------	----------------	---------	-----------	---

Total comprehensive loss attributable to the Australian Government	(76,496)	(77,982)	(1,486)	
---	------------------	-----------	----------	--

¹ ASIO's original budgeted financial statement presented to parliament in respect of the reporting period; that is, ASIO's Portfolio Budget Statements.

	Budget estimate		Variance	Note
	Actual	Original ¹		
	\$ '000	\$ '000	\$ '000	

Statement of financial position as at 30 June 2015

ASSETS

Financial assets

Cash and cash equivalents	22,023	13,587	(8,436)	
Trade and other receivables	93,975	133,307	39,332	C
Other financial assets	4,998	3,162	(1,836)	
Total financial assets	120,996	150,056	29,060	

Non-financial assets

Land and buildings	175,571	237,369	61,798	D
Property, plant and equipment	159,787	93,502	(66,285)	D
Intangibles	36,868	49,283	12,415	
Other non-financial assets	25,354	15,024	(10,330)	
Total non-financial assets	397,580	395,178	(2,402)	
Total assets	518,576	545,234	26,658	

LIABILITIES

Payables

Suppliers	16,622	11,681	(4,941)	
Lease incentives	1,171	1,548	377	
Other payables	29,451	9,118	(20,333)	D
Total payables	47,244	22,347	(24,897)	

Provisions

Employee provisions	62,608	66,822	4,214	
Restoration obligations	6,281	10,946	4,665	
Other provisions	-	-	-	
Total provisions	68,889	77,768	8,879	
Total liabilities	116,133	100,115	(16,018)	

Net assets	402,443	445,119	42,676	
-------------------	----------------	----------------	---------------	--

EQUITY

Parent equity interest

Contributed equity	580,376	634,993	54,617	A C
Reserves	17,930	17,931	1	
Retained surplus (deficit)	(195,863)	(207,805)	(11,942)	
Total equity	402,443	445,119	42,676	

¹ ASIO's original budgeted financial statement presented to parliament in respect of the reporting period; that is, ASIO's Portfolio Budget Statements.

	Budget estimate		Variance	Note
	Actual	Original ¹		
	\$ '000	\$ '000	\$ '000	

Statement of equity for the period ended 30 June 2015

RETAINED EARNINGS

Opening balance	(119,367)	(129,823)	(10,456)	
Comprehensive income				
Deficit for the period	(76,496)	(77,982)	(1,486)	
Closing balance	(195,863)	(207,805)	(11,942)	

ASSET REVALUATION SURPLUS

Opening Balance	17,930	17,931	1	
Closing balance	17,930	17,931	1	

CONTRIBUTED EQUITY/CAPITAL

Opening balance	614,046	601,446	(12,600)	
-----------------	---------	---------	-----------	--

Transactions with owners:

Distributions to owners

Returns of capital – reduction of appropriation	(82,877)	-	82,877	C
---	-----------	---	--------	---

Contributions by owners

Equity injection – appropriation	16,028	368	(15,660)	A
Departmental capital budget	33,179	33,179	-	
Closing balance	580,376	634,993	54,617	
Closing balance attributable to the Australian Government	402,443	445,119	42,676	

¹ ASIO's original budgeted financial statement presented to parliament in respect of the reporting period; that is, ASIO's Portfolio Budget Statements.

	Budget estimate		Variance	Note
	Actual	Original ¹		
	\$ '000	\$ '000	\$ '000	

Statement of cash flows for the period ended 30 June 2015

OPERATING ACTIVITIES

Cash received

Appropriations	410,284	414,147	3,863	
Sales of goods and rendering of services	16,973	16,367	(606)	
Net GST received	17,004	-	(17,004)	
Other	-	1,224	1,224	
Total cash received	444,261	431,738	(12,523)	

Cash used

Employees	212,749	216,294	3,545	
Suppliers	192,272	171,870	(20,402)	A B
Section 74 receipts	22,055	-	(22,055)	
Total cash used	427,076	388,164	(38,912)	
Net cash from operating activities	17,185	43,574	26,389	

INVESTING ACTIVITIES

Cash received

Proceeds from sales of property, plant and equipment	623	-	(623)	
Total cash received	623	-	(623)	

Cash used

Purchase of property, plant and equipment	39,861	76,166	36,305	C D
Purchase of intangibles	18,797	-	(18,797)	C D
Total cash used	58,658	76,166	17,508	
Net cash used by investing activities	(58,035)	(76,166)	(18,131)	

FINANCING ACTIVITIES

Cash received

Contributed equity	45,772	33,547	(12,225)	A
Total cash received	45,772	33,547	(12,225)	
Net cash from financing activities	45,772	33,547	(12,225)	

Net increase in cash held	4,922	955	(3,967)	
----------------------------------	--------------	------------	-----------------	--

Cash and cash equivalents at the beginning of the reporting period	17,101	12,632		
Cash and cash equivalents at the end of the reporting period	22,023	13,587		

¹. ASIO's original budgeted financial statement presented to parliament in respect of the reporting period; that is, ASIO's Portfolio Budget Statements.

Explanation of major variances

- A The New Policy Proposal—Enhancing security intelligence capabilities to counter Islamist terrorism threat—was announced post budget resulting in an additional \$11.229m revenue from government and \$15.660m in additional capital.
- B The altered security environment resulted in increased activity and expenditure.
- C ASIO's departmental capital budget was re-profiled, appropriations returned to government and reallocated in future years to better reflect forecast asset replacement.
- D Adjustments were required post budget to finalise commissioning of the Ben Chifley Building including the Australian Cyber Security Centre.



Part 7

APPENDICES AND INDICES

Appendix A

Agency Resource Statement

	Actual available appropriation for 2014–15 \$'000	Payments made 2014–15 \$'000	Balance remaining 2014–15 \$'000
--	--	---------------------------------------	---

Ordinary Annual Services¹

Departmental appropriation

Prior year appropriation ²	140,743 *	114,496	26,247
2014–15 appropriation ³	368,725 *	310,531	58,194
s74 relevant agency receipts ⁴	22,055 *	22,055	-
Cash on hand		(4,923)	22,023
Total ordinary annual services	531,523	442,159	106,464

Other Services

Departmental non-operating ⁵

Prior year equity injections	5,062 *	5,062	-
Equity injections	16,028 *	16,028	-
Total other services	21,090	21,090	-
Total net resourcing and payments for ASIO	552,613	463,249	

¹ Appropriation Bills (No.1) & Appropriation Bills (No. 3)

² Includes an amount of \$37.780m from 2013–14 and \$4.600m from 2012–13 for the Departmental Capital Budget
For accounting purposes this amount has been designated as 'contributions by owners'

³ Includes an amount of \$0.302m in 2014–15 for the Departmental Capital Budget
For accounting purposes this amount has been designated as 'contributions by owners'

⁴ \$16.367m per Portfolio Budget Statement plus \$5.688m underestimate at time of PBS

⁵ Appropriation Bills (No.2) & Appropriation Bills (No. 4)

* as per Portfolio Budget Statements

Appendix B

Expenses by outcomes

Outcome 1: To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to Government	Budget* 2014–15 \$'000	Actual Expenses 2014–15 \$'000	Variation 2014–15 \$'000
---	------------------------------	---	--------------------------------

Program 1.1: Security Intelligence

Departmental expenses

Appropriation ¹	400,406	423,657	(23,251)
Expenses not requiring appropriation in the Budget year	57,724	64,562	(6,838)
Total for Program 1.1	458,130	488,219	(30,089)
Total expenses for Outcome 1	458,130	488,219	(30,089)

* as per Portfolio Budget Statements

¹ Ordinary annual services (appropriation Act No.s 1 and 3) and Retained Revenue Receipts under section 74 of the *PGPA Act 2013*

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 5: Composition of workforce 2009–10 to 2014–15

	2009–10	2010–11	2011–12	2012–13	2013–14	2014–15
Ongoing full-time ¹	1460	1511	1546	1589	1490	1517
Non-ongoing full time ²	40	50	37	42	27	31
Ongoing part time	134	148	168	193	204	211
Non-ongoing part time	18	16	18	19	17	17
Non-ongoing casual	39	42	43	61	57	53
Total	1691	1767	1812	1904	1795	1829

¹ Does not include the Director-General of Security

² Includes secondees and locally engaged staff held against positions in the structure

Table 6: Senior Executive Service equivalent classification and gender
2009–10 to 2014–15

		2009–10	2010–11	2011–12	2012–13	2013–14	2014–15
Band 1	Female	6	8	10	8	8	13
	Male	35	38	36	27	25	25
Band 2	Female	4	4	5	3	3	3
	Male	10	10	8	6	7	7
Band 3	Female	0	0	0 ²	0 ²	0 ²	0²
	Male	2	2	1	1	1	1
Total		57	62	60	45	44	49

¹ Does not include the Director-General of Security

² These figures do not include a seconded Band 3

Table 7: Representation of designated groups within ASIO at 30 June 2015

Group	Total staff ¹	Women	Non-English speaking background	Aboriginal and Torres Strait Islander	People with a Disability	Available EEO data ²
Senior Executive Service ³	49	16	0	0	1	49
Senior officers ⁴	499	186	18	2	6	499
AE6 ⁵	652	327	56	3	7	641
AE5 ⁶	346	180	17	0	2	346
AE1–4 ⁷	167	84	12	2	1	162
Information Technology Officers Grades 1 and 2	107	16	6	2	3	107
Engineers Grades 1 and 2	9	0	0	0	0	9
Total	1829	809	109	9	20	1813

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

² Provision of equal employment opportunity (EEO) data is voluntary

³ Does not include the Director-General of Security

⁴ Translates to the Australian Public Service (APS) Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications

⁵ ASIO Employee (AE) Grade 6 group translates to APS Level 6

⁶ AE Grade 5 group translates to APS Level 5

⁷ AE Grades 1-4 Translates to span the APS 1 to 4 classification levels

Table 8: Percentage of representation of designated groups in ASIO 2009–10 to 2014–15

Group	2009–10	2010–11	2011–12	2012–13	2013–14	2014–15
Women ¹	44.3	44.3	44.3	43.8	44.1	44.2
Non-English speaking background	6.9	6.0	5.7	5.8	5.5	6.0
Aboriginal and Torres Strait Islander	0.2	0.3	0.4	0.5	0.4	0.5
People with a disability	1.2	1.2	1.2	1.3	1.1	1.1

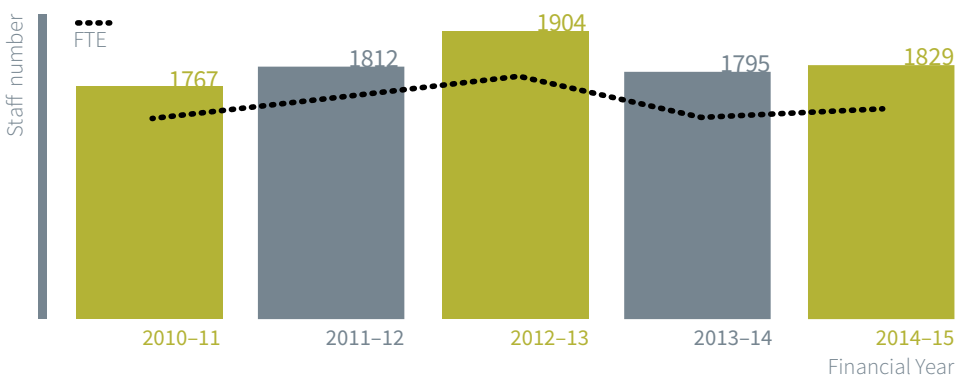
¹ Percentages for women are based on total staff. Percentages for other groups are based on staff for whom EEO data was available.

Appendix E

ASIO Salary Classification Structure at 30 June 2015

ASIO managers			
SES Band 3	\$232 491		minimum point
SES Band 2	\$208 888		minimum point
SES Band 1	\$170 683		minimum point
AEE3	\$137 400		
AEE2	\$116 100	to	\$137 400
AEE1	\$101 300	to	\$113 200
Intelligence employees			
IO	\$79 700	to	\$89 800
ASIO employees			
AE 6	\$79 700	to	\$89 800
AE 5	\$72 100	to	\$77 400
AE 4	\$65 700	to	\$70 500
AE 3	\$58 100	to	\$63 500
AE 2	\$51 100	to	\$56 600
AE 1	\$44 100	to	\$49 000
ASIO information technology officers			
SITEA	\$137 400		
SITEB	\$116 100	to	\$137 400
SITEC	\$101 300	to	\$113 200
ITE2	\$79 700	to	\$89 800
ITE1	\$69 400	to	\$76 300
ASIO engineers			
SIE(E)5	\$137 400		
SIE(E)4	\$116 100	to	\$137 400
SIE(E)3	\$101 300	to	\$113 200
SIE(E)2	\$79 700	to	\$89 800
SIE(E)1	\$69 400	to	\$76 300

Appendix F



Appendix G

Description	Requirement	Page
Letter of transmittal	Mandatory	iii
Table of contents	Mandatory	v–vi
Index	Mandatory	132
Glossary	Mandatory	131
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–xii
Summary of significant issues and developments	Suggested	vii–xii
Overview of department's performance and financial results	Suggested	Part 2
Outlook for following year	Suggested	xii
Significant issues and developments—portfolio	Portfolio departments—suggested	Not applicable
Departmental overview		
Role and functions	Mandatory	xv
Organisational structure	Mandatory	xvi
Outcome and program structure	Mandatory	14
Where outcome and program structures differ from Portfolio Budget Statements (PBS) or Portfolio Additional Estimates 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 PBS or PAES or other portfolio statements	Mandatory	Part 2
Where performance targets differ from the PBS/PAES, details of both former and new targets, and reasons for the change	Mandatory	Not applicable
Narrative discussion and analysis of performance	Mandatory	Part 2
Trend information	Mandatory	Throughout
Significant changes in nature of principal functions/services	Suggested	Not applicable

Description	Requirement	Page
Report on performance (continued)		
Performance of purchaser/provider arrangements	If applicable, suggested	Not applicable
Factors, events or trends influencing departmental performance	Suggested	Part 2
Contribution of risk management in achieving objectives	Suggested	Part 5
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	Not applicable
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	115
Agency resource statement and summary resource tables by outcomes	Mandatory	118–122
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	56–57
Names of the senior executive and their responsibilities	Suggested	Not applicable
Senior management committees and their roles	Suggested	56–60
Corporate and operational planning and associated performance reporting and review	Suggested	56–57
Approach adopted to identifying areas of significant financial or operational risk	Suggested	–
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	–
External scrutiny		
Significant developments in external scrutiny	Mandatory	41–47
Judicial decisions and decisions of administrative tribunals	Mandatory	35
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	62–65
Workforce planning, staff turnover and retention	Suggested	62–69

Description	Requirement	Page
Management of human resources		
Impact and features of enterprise or collective agreements, individual flexibility arrangements (IFAs), determinations, common-law contracts and Australian workplace agreements (AWAs)	Suggested	63–64
Training and development undertaken and its impact	Suggested	67–70
Work health and safety performance	Suggested	66–67
Productivity gains	Suggested	–
Statistics on staffing	Mandatory	121
Enterprise or collective agreements, IFAs, determinations, common-law contracts and AWAs	Mandatory	63–64
Performance pay	Mandatory	Not applicable
Assessment of effectiveness of assets management	If applicable, mandatory	69–71
Assessment of purchasing against core policies and principles	Mandatory	71
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	72
Absence of provisions in contracts allowing access by the Auditor-General	Mandatory	Not applicable
Contracts exempt from AusTender	Mandatory	71
Financial statements	Mandatory	Part 6
Other mandatory information		
Work health and safety (Schedule 2, Part 4 of the <i>Work Health and Safety Act 2011</i>)	Mandatory	58, 66–67
Advertising and market research (section 311A of the <i>Commonwealth Electoral Act 1918</i>) and statement on advertising campaigns	Mandatory	64
Ecologically sustainable development and environmental performance (section 516A of the <i>Environment Protection and Biodiversity Conservation Act 1999</i>)	Mandatory	70
Compliance with the agency's obligations under the <i>Carer Recognition Act 2010</i>	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	122
Information Publication Scheme statement	Mandatory	Not applicable

Additional ASIO reporting requirements under the *Australian Security Intelligence Organisation Act 1979*

Part of report	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	Part 3
The total warrants issued during the year under that division	Mandatory	Part 3
The total number of warrants issued during the year under section 34E and the total of all those hours for all those persons	Mandatory	Part 3
The following numbers:	Mandatory	Part 3
<ul style="list-style-type: none"> ▶ 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 		
The number of times each prescribed authority had persons appear for questioning before him or her under warrants issued during the year	Mandatory	Part 3

Abbreviations

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGSVA	Australian Government Security Vetting Agency
ANU	Australian National University
ANZCTC	Australia – New Zealand Counter-Terrorism Committee
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
BCB	Ben Chifley Building
BLU	Business Liaison Unit
CERT Australia	Computer Emergency Response Team Australia
COAG	Council of Australian Governments
CRS	Contact Reporting Scheme
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	<i>Freedom of Information Act 1982</i>
G20	Group of Twenty
GST	goods and services tax
ICT	information communications technology
IDP	Intelligence Development Program
IGIS	Inspector-General of Intelligence and Security
INSLM	Independent National Security Legislation Monitor

ISA	<i>Intelligence Services Act 2001</i>
JCTT	Joint Counter Terrorism Team
MSIC	Maritime Security Identification Card
NAA	National Archives of Australia
NiTAC	National Interception Technical Assistance Centre
NTAC	National Threat Assessment Centre
PGPA Act	<i>Performance and Accountability Act 2013</i>
PID Act	<i>Public Interest Disclosure Act 2013</i>
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
SSAN	security-sensitive ammonium nitrates
SSBA	security-sensitive biological agents
WHS	work health and safety
WHS Act	<i>Work Health and Safety Act 2011</i>

Glossary

foreign fighters—Australians who have participated in foreign conflicts or undertaken training with extremist groups overseas.

Islamism—A political ideology which holds that Islam provides a complete and self-contained social, political, religious and legal system that should be implemented in existing Muslim societies. Islamism's central principle is that the only legitimate basis for a society's laws, institutions and practices is the tenets of Islam and those laws, institutions and practices inconsistent with the tenets of Islam are not legitimate.

jihadist—Jihadist is commonly used as a noun to refer to a person involved in violent jihad.

lone actor—An individual (or sometimes a close-linked pair) who plans to conduct—or does in fact conduct—an anti-social activity for political or religious motives, or to advance some personal cause. They typically, but not always, use violence; and at the time the action is performed, they act alone and without real-world accomplices.

radicalisation—The process by which an individual's beliefs move from mainstream views (those commonly accepted by the majority within a society) towards more marginal views (those less widely accepted or not accepted by the majority within a society). Radicalisation occurs across a spectrum, and some individuals may become radicalised sufficiently to advocate or use violence to effect societal or political change.

terrorism—Terrorism is a tactic that can be employed by any group or individual determined to use violence to achieve or advance a political goal.

violent extremism—Any ideology or world view that is advanced through the use of violence; violent extremism is unlawful.

Index

A

Abbott MP, the Hon. Tony 30, 42
 accountability 39
 accountability framework xiv, 40
 Administrative Appeals Tribunal (AAT) 21, 25, 73
 adverse security assessments *see also* security assessments 12, 44
 Afghanistan 16–17
 Africa viii, 6
 Al-Murabitun 20
 al-Qa'ida ix, 2–7, 16
 al-Qa'ida in the Arabian Peninsula (AQAP) ix, 5–6
 al-Qa'ida in the lands of the Islamic Maghreb 6
 al-Shabaab 6
 Ansar al-Islam 20
 anti-Islam 10, 17
Archives Act 1983 73
 ASIO Security Committee 57
 assumed identities 51
 Attorney-General iii, xiv, xv, 19–20, 26, 34, 37, 40–43, 47–51, 60–61
 Attorney-General's Department 9, 19, 23, 49
 Attorney-General's Guidelines 40
 audit 52–53
 Audit and Risk Committee 59
 AusCheck 23
 Australia – New Zealand Counter-Terrorism Committee (ANZCTC) 30, 33
Australian Citizenship Act 2007 22
 Australian Counter-Terrorism Centre (ACTC) 30, 70
 Australian Cyber Security Centre (ACSC). *See also* Australian Signals Directorate (ASD) 18, 70, 115
 Australian Defence Force (ADF) 49
 Australian Federal Police (AFP) 16, 24
 Australian Geospatial-Intelligence Organisation (AGO) *see also* Defence Imagery and Geospatial Organisation (DIGO) 49
 Australian Government viii, xi, xii, xv, 2, 8, 9, 12, 15, 17, 18, 19, 20
 Australian National Audit Office (ANAO) 58
 Australian National University (ANU) 61
 Australian Nuclear Science and Technology Organisation (ANSTO) 24
Australian Passports Act 2005 21
Australian Passports Determination 2005 21
 Australian Public Service (APS) 66, 123
 Australian Secret Intelligence Service (ASIS) 34
Australian Security Intelligence Organisation Act 1979 (ASIO Act) iii, vii, xiv, 11, 20, 40, 88, 120, 128
 Australian Signals Directorate (ASD) *see also* Defence Signals Directorate (DSD) 9, 34, 49
 Aviation Security Identification Card (ASIC) 23

B

Ben Chifley Building (BCB) xii, 18, 30, 59, 70, 74, 115
 Blaxland, John Dr 62
 Boko Haram 6
 border integrity 12, 25
 border security *see also* people smuggling 23, 58
 Brandis QC, Senator the Hon. George *see also* Attorney-General 40
 Briggs AO, Ms Lynelle 59
 Business Liaison Unit (BLU) 18

C

Canada viii, 5
 Carlton AO, Mr Jim 62
Charlie Hebdo 5
 Chifley MP, the Hon. Joseph Benedict 'Ben' Chifley (former Prime Minister) 70
 Code of Conduct 66, 68
 Comcare 25, 66–67
 Commonwealth Procurement Rules 73
 communal violence vii–xv, 9–11, 15
 complaints 126
 Computer Emergency Response Team Australia (CERT) 9
 Connell, Ms Jenet 56
 consultants 72
 Contact Reporting Scheme (CRS) 31
 corporate governance 56–59
 corporate strategy 56
 Council of Australian Governments (COAG) 24, 30
 counter-espionage x, 15, 17, 29, 31, 48, 58 *see also* espionage vii, x, xiii, xv, 7–9
 counter-terrorism xiii, 3, 14, 23, 29, 33, 47, 59, 62
 Counter-terrorism Coordinator 30
 counter-terrorism framework 48
Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 22, 32, 50
 counter-terrorism New Policy Proposal 58, 62, 115
 Counter Terrorism Control Centre (CTCC) xvii
 countering violent extremism (CVE) x
Crimes Act 1914 52
Criminal Code Act 1995 (Criminal Code) 19, 42
 critical infrastructure 11, 14, 16–18, 26
 cyber espionage *see also* cyber security *see also* espionage 9, 18
 cyber security *see also* cyber espionage *see also* espionage x, 18, 33
 Cyber Security Review Steering Group 33

D

declared areas 19–20, 42
Defence Imagery and Geospatial Organisation (DIGO) *see also* Australian Geospatial-Intelligence Organisation (AGO) 49
Defence Intelligence Organisation (DIO) 16
Defence Signals Directorate (DSD) *see* Australian Signals Directorate (ASD) 9, 34, 49
Denmark viii, 5
Department of Defence *see also* Minister for Defence 27
Department of Finance 56, 70–71, 91, 108
Department of Foreign Affairs and Trade (DFAT) *see also* Minister for Foreign Affairs 50, 108
Department of Health 24
Department of Immigration and Border Protection (DIBP) 20, 23, 44
Department of the Prime Minister and Cabinet (PMC) 30, 42
Deputy Director-General 43, 56, 58, 62
Director-General of Security vii–xii, 2, 16, 21–22, 40, 43, 49, 56, 65, 77

E

Egypt 5
e-learning 52, 71
engagement xv, 18–19, 32
 government 60
 international 29, 31
 public 60
Endeavour Hills police station vii, 3
environmental performance 71
espionage *see also* cyber espionage *see also*
 cyber security v, vii, x–xi, xiii, xv, 7–9, 15,
 17–18, 29, 31, 48, 58
Europe viii, 5, 16
Executive Board 56–59
extremism *see also* violent extremism 15

F

Federal Court of Australia 12, 21, 25, 44
Finance Committee 59
Financial Management and Accountability Act 1997 (FMA Act) 108
financial statements 41, 76–87
foreign fighters viii, 31, 43, 50, 131
foreign intelligence x, xv, 7, 17
foreign intelligence collection 14, 34
foreign intelligence services 7–8
foreign interference 8, 15, 29, 31
Freedom of Information Act 1982 (FOI Act) 129

G

Group of Twenty (G20) 11, 17, 24, 48
Gallop AC, Mr Geoff 62

H

Hartland, Ms Kerri *see also* Deputy Director-General 43
High Court of Australia 21
Hizballah 6, 20
Hope AC CMC QC, Justice Robert Marsden 40
Horner AM, Professor David 61

I

illegal maritime arrivals 12, 23
Independent National Security Legislation Monitor (INSLM) 47
Independent National Security Legislation Monitor Act 2010 47
Independent Reviewer of Adverse Security Assessments 12, 25, 44–46
industry engagement *see also* engagement 15, 18
information and communications technology 64
information technology 7, 9, 58, 69
information technology security 54
Inspector-General of Intelligence and Security (IGIS) 44, 66, 73
Inspire magazine 6
Intelligence Coordination Committee 58
Intelligence Development Program 68
Intelligence Services Act 2001 (the ISA) 41
International Court of Justice 25
international engagement 31
international partners 29, 31, 57, 67
Iraq viii, ix, xii, 2–5, 10–11, 15–16, 20, 22, 32, 48, 50
Irvine AO, Mr David 43
Islam 2, 17
Islamic Movement of Uzbekistan 20
Islamist 5, 116, 131
Islamic State in Iraq and the Levant (ISIL) ix, 2–6, 16–17, 20

J

Jabhat al-Nusra 3–5
Jaish-e-Mohammed 20
Jewish 5
jihadists ix, 131

K

Kenya viii, 6
Key Performance Indicators 14, 125

L

Lashkar-e-Jhangvi 20
 Lebanese Hizballah 6
 Legal and Constitutional Affairs Committee 43
 Lewis AO, DSC, CSC, Mr Duncan *see also* Director-General of Security iii, v, xii, xiv, xvi, 2, 16, 21–22, 37, 40, 43, 49, 56, 59, 61–62, 65, 67, 71, 77, 89, 121
 Libya viii, 6
 Lindt Café Siege viii, 3, 25
 litigation xiii, 25
 lone actor viii, ix, 5, 131
 Lonsdale, John Mr 56

M

Management and Leadership 69
 Martin Place viii, 3, 42–43
 Maritime Security Identification Card (MSIC) 23
 media 60–61
 Middle East viii, 5, 6
Migration Amendment Bill 2013 42
 Minister for Defence xv, 14, 34
 Minister for Foreign Affairs xi, xv, 14, 20–22, 34, 49–50
 Moriarty, Mr Greg 30
 Muslim 2, 10

N

National Archives of Australia (NAA) 73
 National Counter-Terrorism Exercise Program 30
 National Intelligence Priorities 29, 34, 59
 National Security Committee of Cabinet 30, 34
National Security Legislation Amendment Bill (No.1) 2014 42, 48
 National Threat Assessment Centre (NTAC) 16, 33
 new ASIO building *see also* Ben Chifley Building xii, 86, 108
 New Building Committee 59
 new central office *see also* Ben Chifley Building 70–71
 New South Wales Coroner 43
 New Zealand *see also* Australia – New Zealand Counter-Terrorism Committee 30

O

Office of National Assessments 16
 Official History of ASIO 61–62
 Ombudsman (ASIO) 65–66
 Operation Sovereign Borders 12
 Organisational Capability Program 64
 organisational structure xvi–xvii, 42
 outreach 7, 27, 31, 60

P

Parliamentary Joint Committee on Intelligence and Security (PJCS) 20, 41, 72
 partnership forums 60
 passports ix, xiii, 4, 21–22, 25, 43
 people smuggling *see also* border security 12, 25
 police viii, 3, 9, 10, 16
Police (Special Investigative and Other Powers) Act 2015 [Northern Territory] 51
 politically motivated violence ix, xv, 15, 25, 29
 Prime Minister 30, 42, 44, 70
 Prime Minister and Cabinet 30, 42
 proscription 15, 19–20
 protective security xv, 11, 14, 16, 26–28
 Protective Security Policy Framework (PSPF) 27
 protective security risk reviews (PSRR) 26, 28
 Protective Security Training College 27
 protest activity 11
Public Governance, Performance and Accountability Act 2013 53, 56, 77, 88
Public Interest Disclosure Act 2013 52, 66

Q

questioning and detention warrants 40, 50, 120
 questioning warrants 40, 50, 120

R

radicalisation 3, 6, 15, 32, 131
 records xiii, 44, 72
 recruitment 3, 56, 58, 62, 63, 64
 rewards and recognition 70
 risk management 16, 56, 58, 59

S

security assessments x, xiii, xv, 4, 20–22
Security Construction and Equipment Committee (SCEC) 27
security environment vii, ix, xii, 1–12
Security Equipment Evaluated Product List (SEEPL) 27–28
security-sensitive ammonium nitrates (SSAN) 24
security-sensitive biological agents (SSBA) 24
Senate Estimates 41, 43
Senior Executive Service 60, 121, 122
social media ix, 3–5
Somalia 6
South Asia vii
South-East Asia vii
Stakeholder Satisfaction Survey 61
Stone, the Hon. Margaret 12, 25, 44
Strategic and Defence Studies Centre 61
Strategic plan 56–57
study support 70
suicide attacks 3
Syria viii–xii, 3–6, 10–11, 15–16, 20, 32, 48, 50, 58

T

T4 26–28
technical capabilities xi, 68
technical surveillance countermeasures 26–28
Telecommunications (Interception and Access) Act 1979 32, 43, 50
terrorism *see also* counter-terrorism xii, xiii, 2–6, 15–16, 22, 25, 131
terrorist groups ix, 3–6, 16, 32
terrorist organisations ix, 19–20, 42, 49
Thom, Dr Vivienne 44
threat assessments 11, 14, 16–17
Timor-Leste 25
Tunisia viii, 6

U

United Kingdom viii, 62
United States viii, 5

V

vetting 24, 62, 64
violent extremism x, 4, 15, 131
violent protest vii, 9, 15–16
visa security assessments *see also* security assessments xiii, 23, 25

W

warrants xi, 25, 40, 47, 48, 49, 50, 51, 120, 128
whole-of-government 11, 25, 30–31
Workforce Capability Committee (WCC) 58
Work Health and Safety Act 2011 (WHS Act) 66
Work Health and Safety Committee 58, 67
work health and safety (WHS) 66
workplace agreement 63

Y

Yemen 5–6, 16



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
E: media@asio.gov.au

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

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.

