Australian Government

Australian Security Intelligence Organisation

ASIO Annual Report 2015–16

Vision

ASIO's vision is to be trusted and respected as a protector of Australia's national security, to be accessible to partners, to effectively communicate security risks, to be an adaptive and innovative organisation and to have a diverse team of passionate people committed to serve the nation. This vision will drive us forward to achieving our purpose of protecting the nation from security threats.

Purpose

To protect the nation and its interests from threats to security through intelligence collection, assessment, and advice for Government, government agencies, and business.

Values

Our values represent the day-to-day expectations on each person in ASIO in performing our vital work. You will see these values in action when we…

Excellence

- Produce high quality, relevant, timely advice based on the best available information
- Display strong leadership and professionalism
- Improve through innovation and learning

Integrity

- Are ethical and work without bias within the law
- Maintain confidentiality and the security of our work

Respect

- Show respect in our dealings with others

Cooperation

- Build a common sense of purpose and mutual support
- Communicate appropriately in all our relationships
- Foster and maintain productive partnerships

Accountability

- Are responsible for what we do and for our outcomes
- Are accountable to the Australian community through the Government and the Parliament

ASIO ANNUAL REPORT 2015–16

ISSN 0815-4562 (print)
ISSN2204-4213 (online)

Commonwealth Coat of Arms

The Commonwealth Coat of Arms is used in accordance with the April 2014 *Commonwealth Coat of Arms: Information and Guidelines*, published by the Department of the Prime Minister and Cabinet and available online (http://www.itsanhonour.gov.au/coat-arms/index.cfm).

Report a threat

National Security Hotline 1800 123 400
hotline@nationalsecurity.gov.au

Contact us

We welcome feedback on our annual report from any of our readers. Please contact:

Officer: First Assistant Director-General, Executive
Phone: General inquiries: (02) 6249 6299 or 1800 020 648
Business inquiries: (02) 6234 1668
Media inquiries: (02) 6249 8381
Recruitment inquiries: (02) 6257 4916
Email: media@asio.gov.au
Post: GPO Box 2176, Canberra ACT 2601

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

Australian Government

Australian Security
Intelligence Organisation

Director-General of Security

A11298532

27 September 2016

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

Dear Attorney,

In accordance with section 46 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), I am pleased to present to you ASIO's annual report for 2015–16.

The report contains the information required by both section 94 of the *Australian Security Intelligence Organisation Act 1979* and the Public Governance, Performance and Accountability Rule 2014. I certify that fraud risk assessments and fraud control plans have been prepared for ASIO and that we have in place appropriate mechanisms and have taken all reasonable measures for preventing, detecting, investigating, and reporting fraud within the organisation.

The report describes the value ASIO delivered to Australia through protecting the nation and its interests from threats to security. The report necessarily contains some national security classified material. In order to avoid prejudice to ASIO's activities, I have deleted that material from the version to be tabled in parliament (in accordance with determinations made by you and the Minister for Finance under the PGPA Act).

Yours sincerely,

Duncan Lewis

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

Guide to this report

The Director-General's review provides his reflection on the achievements of the organisation during the year and looks ahead to how the organisation will meet future challenges.

PART 1

provides an overview of ASIO, our role and functions, structure, and expectations from government in protecting the nation from threats to security.

PART 2

provides an unclassified overview of Australia's security environment and outlook.

PART 3

is our annual performance statement for 2015–16 against our financial performance and our five key activities of:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders;
- countering serious threats to Australia's border integrity;
- providing protective security advice to government and business; and
- collecting foreign intelligence in Australia.

This part includes both classified and unclassified information.

PART 4

provides additional performance information in support of the annual performance statement.

PART 5

describes our corporate management, including strategy, governance, human resources, financial services, and external scrutiny and accountability.

PART 6

contains classified information about performance and corporate management.

FINANCIAL STATEMENTS AND APPENDICES

The report also contains our audited financial statements and related notes and appendices with information required by the PGPA Act or the ASIO Act (some appendices are classified).

This report is available at www.asio.gov.au/publications-1.html

Contents

Director-General's review

Today's national security challenges are markedly different to those which faced ASIO at the time of its establishment in 1949. The characteristics of the current security environment are a reflection of the nature of our modern, globalised world. The mass movement of people across borders, the ability of the internet to connect people and the prevalence of encrypted mobile communications are part of modern life. At that same time though, these factors also present opportunities for those who wish to do us harm through terrorism, cyber attack, espionage or foreign interference. This means ASIO's intelligence collection and assessment work is now more important than ever; a balanced and trusted security intelligence service is essential.

The threat of violent Islamist terrorism was once something distant or remote; something that affected other parts of the world. Today, the threat is real and unprecedented for Australia—realised by the four attacks and ten disrupted terrorist attacks on our shores since September 2014 (for details see 'Terrorism—the Australian security environment'). The phenomena of radicalisation and the adoption of a commitment to violent Islamist terrorist activities is happening at a speed hitherto unseen. Individuals are also being radicalised at an increasingly young age. The increasing terrorist threat from attacks using basic and more readily available weapons makes it harder for intelligence and law enforcement agencies to protect Australians and Australian interests. In particular we have seen during this reporting period an increase in lone actor attacks both here in Australia and overseas.

The terrorist threat is a concern for many Australians. Polling from the Lowy Institute in 2015 showed fewer than one in four Australians said they felt 'very safe' with the highest-ranked threat being 'the emergence of Islamic State in Iraq and Syria'.[1] The 2016 poll indicated that 'terrorism and national security' ranks as the fifth highest priority for Australians, with 68% regarding this as 'very important.'[2] The community concern is understandable given the increased level of activity on our shores, and that Australian locations have been specifically named in extremist publications.

This year there was a slight decrease in the overall number of ASIO investigations into Australians located in Syria or Iraq, largely due to an increase in the number of Australians assessed to have been killed in the conflict. The number of Australians joining the conflict appears to be plateauing after a steep increase in late 2014 and throughout 2015. Despite over 50 passport cancellations in the past year to prevent travel, there remains a small number of Australians who have succeeded in evading detection and/or border control measures and have departed Australia for Syria or Iraq.

Of great concern is that up to 70 children of Australians have been exposed to extremist groups in Syria or Iraq. These children have either travelled to Syria or Iraq, or a surrounding country, with their Australian parents, or have been born to Australian parents while in the conflict zone. They have been exposed to events in a

[1] Oliver, A. Lowy Institute for International Policy 'The Lowy Institute Poll 2015' available from www.lowyinstitute.org.au

[2] Oliver, A. Lowy Institute for International Policy 'The Lowy Institute Poll 2016' available from www.lowyinstitute.org.au

brutal war zone, undoubtedly traumatised and growing desensitised to such extreme violence. They are also subject to the indoctrination efforts of these extremist groups. The long-term effect of this will be a security concern for Australian intelligence and law enforcement agencies for many years to come.

The international security situation has highlighted the importance of intelligence advice on cross-border movements. Our tailored reporting, assessments and travel intelligence helped inform decision-making at our border. We also identified a small number of foreign individuals whose presence or continued presence in Australia posed a potential risk to national security—predominantly for reasons relating to terrorism.

Of ongoing concern for ASIO and partners is the potential for violent protest or conflict between protesters and counter-protesters at rallies organised by Australian extreme right-wing groups. Online engagement between those with extremist agendas is extensive and vitriolic, maintaining tensions and increasing the potential for spontaneous violent activities. Recent rallies have occurred without serious incidents but have involved widespread hostility and verbal clashes. Unfortunately, we expect these clashes will continue.

In the past year, ASIO has continued to expand its reach. Domestically, I addressed numerous open forums, including as the keynote speaker in the *'Security in Government'* conference. In closed settings, I briefed the Prime Minister and other ministers, the Leader of the Opposition and state government representatives on sensitive intelligence matters. I addressed a wide range of partners, including police, business and industry, and state government agencies on broader security intelligence issues. As part of my international engagement and outreach activity, I visited a number of regions to secure Australia's participation in, and contribution to, forums that require collaborative efforts to countering threats. I also hosted a wide range of international visitors, each occasion fostering an ongoing commitment to work in close partnership.

Consistent with a modern security intelligence agency we have an outward focus on partnerships and an information-sharing culture. Our joint work with other intelligence agencies continues to be a high priority, as does growing partnerships with other Commonwealth agencies. With offices in each state and territory, ASIO continues to deepen ongoing relationships and form new partnerships with state government, industry and communities. The effectiveness of ASIO's liaison relationships were highlighted in our annual stakeholder survey. Positively, the results of the survey again showed ASIO is well-regarded and considered a key partner. Our overseas reach also continued to expand, particularly in light of the enduring number and impact of global terrorist attacks. The survey showed opportunity for us to further improve access to information for those with a need-to-know. This will be an area of focus next year.

It is an unfortunate reality that the changes to the security environment have resulted in an increased threat to the personal safety of ASIO staff. Recent low-capability, lone actor terrorist attacks around the world—including attacks against police here in Australia—demonstrate the real danger to staff. My officers are operating in an environment that puts their personal safety at risk from spontaneous or opportunistic attack using readily acquired weapons and relatively simple tactics. Reporting of suspicious

activities and behaviours in and around ASIO premises has risen. To address the threat, our protective security measures have increased commensurate with the level of risk—including through armed Australian Federal Police (AFP) closely patrolling ASIO's headquarters. We are also investing heavily in training our staff in advanced self-defence techniques. We now operate with an elevated security awareness level as we go about our business. We continually reassess our response to the changing environment. Given the nature of the threat, there are no protective security measures that can entirely mitigate the threat to personnel and premises. However, as I have reiterated to my officers, the safety of staff remains the paramount priority for ASIO.

Over the past year, there has been no relief from espionage and foreign interference against Australia and Australian interests. These efforts are occurring on an increasing scale. Given the clandestine nature of espionage and foreign interference, victims are generally unaware that harmful activities have occurred. Although we have some visibility of the activity against the nation, we can be confident that there is more activity than we are seeing. In response, we have:

- identified and provided advice on hostile foreign intelligence activity that is occurring, or will occur, and which is likely to cause serious harm to Australian national interests; and
- at a time when states and territories are focused on privatising significant assets, we have provided assessments on foreign investments as part of the Australian Government consideration of threats arising from proposed foreign investments in critical infrastructure, as well as potential mitigations.

ASIO has a range of functions which also contribute to protecting Australia's defence system from security threats. ASIO, therefore, monitors activities that are intended to, and are likely to, obstruct, hinder or interfere with the performance of the Australian Defence Force in fulfilling its functions. The security risks faced by Australia's defence industry are real, persistent and cover a wide range of technologies and capabilities. Compromise of these projects and their technologies would have a catastrophic impact on the security of our nation.

There is understandably a high government and public expectation of what we, together with our partners, can do to protect Australia. However, the reality is that the scale of the challenge is significant no matter how great our efforts. In today's environment, regardless of resourcing and expertise, we cannot provide complete assurance that all terrorist attacks or high-harm espionage activities affecting Australia and Australians will be identified and prevented. What can be done—and what is incumbent on me as Director-General to do—is to effectively manage the business of ASIO to deliver the best result. That is, to prioritise and focus our efforts and attention against the security risks posing the greatest harm to the nation and its interests.

For ASIO, as it was for the Australian Public Service more generally, the year was not without its challenges from a financial and resourcing perspective. Not surprisingly, our budget is under significant pressure due to the heightened threat environment. The nature and number of our investigations make them very costly. Combined with this, there are escalating business costs associated with managing infrastructure, technologies, staff safety and partner agency relationships. Throughout the year, we

carefully managed and examined our expenditure. Where possible, business practices were streamlined and selected activities delayed to release funds to cover the highest priorities. Despite this, the financial result was an operating loss of $5.4 million (excluding depreciation). As the challenging fiscal environment is expected to continue, I will continue to look for efficiencies, while being mindful of the impact on our ability to address threats now and into the future.

In July 2016, I launched the ASIO2020 program which will identify ways to respond to the major pressures on our business over the coming years. It will ensure that we remain focused on work that provides clear value for the Australian Government and that we have the right culture, people and systems to effectively and efficiently achieve our purpose.

As the leader of ASIO, I must address the fact that our workforce demographic data shows women are currently less likely than men to progress to management positions in ASIO. In response, I have set a forward program to close this gap by committing to achieving gender equity across all levels of ASIO by 2020. This means ensuring that our executive level and senior executive service management teams are representative of the broader organisational gender split. In our recruitment, we will also aim for a 50:50 gender mix on our entry-level development programs. There is a strong staff commitment to this goal, championed by ASIO's leadership team.

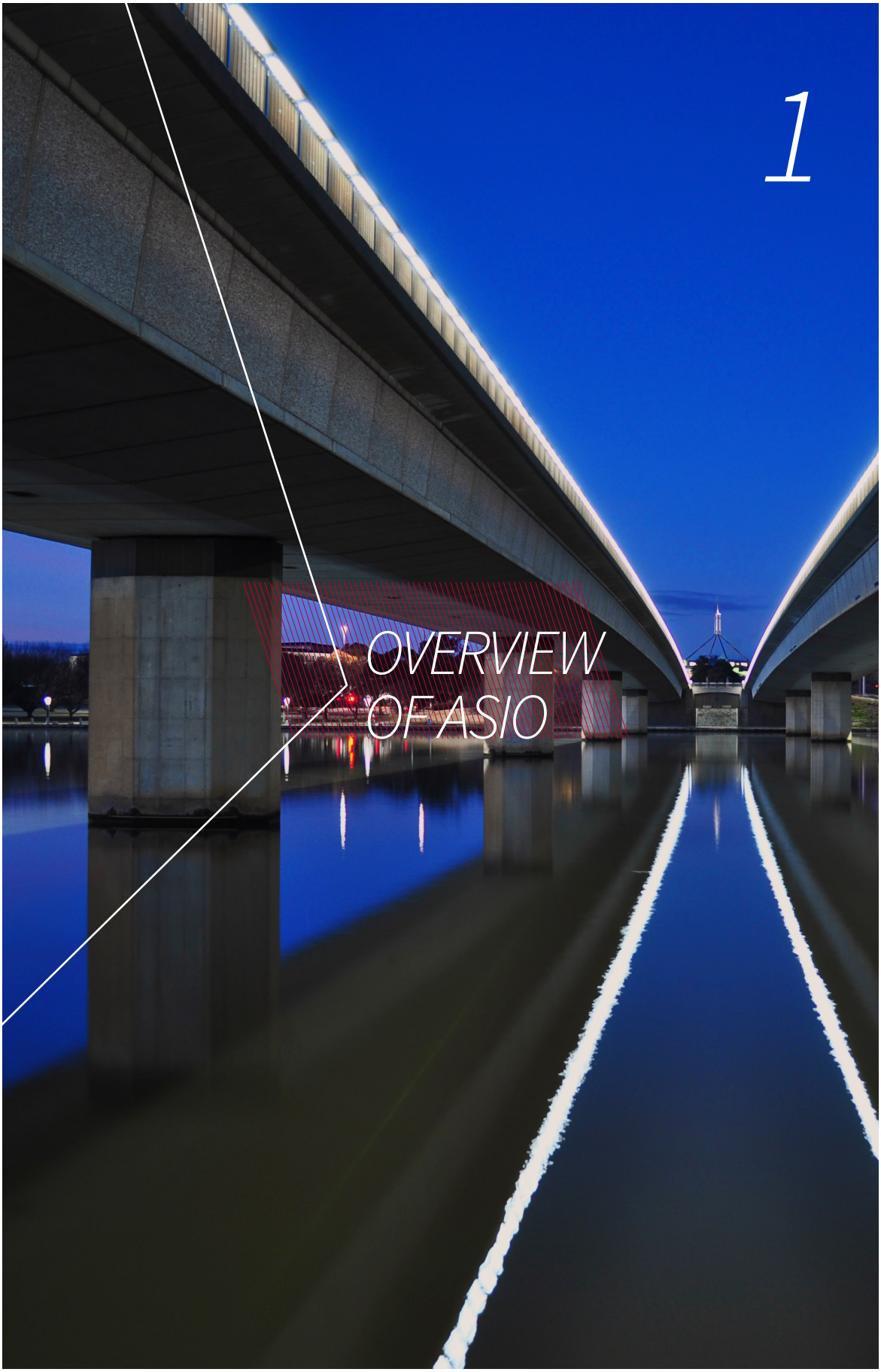
A number of other organisational achievements should be highlighted. Two ASIO staff were awarded Public Service Medals in the Queen's Birthday Honours List. A number of staff received Australia Day Awards for their outstanding contributions to intelligence activities. ASIO's Management and Leadership in Security Intelligence Strategy 2013–2016 won the Australian Human Resources Institute's Rob Goffee Award for Leadership Development. In addition, Volume 1 of the History of ASIO was named a joint winner of the 2015 Prime Minister's Literary Awards Prize for Australian History. Finally our new headquarters—the Ben Chifley Building—received recognition of its unique architecture by winning an Australian Institute of Architecture (ACT Chapter) Award—the W Hayward Award for interior architecture and an award in the commercial architecture category.

Our Canberra based staff are now well settled into the Ben Chifley Building. We hosted a large number of visitors to the building—including His Royal Highness the Prince of Wales and other international dignitaries and senior intelligence community representatives. The Prime Minister toured the building, as did the Governor-General. Functionally, the building was a resource for the wider intelligence and government community, with its conference facilities well utilised for special events, guest speakers and networking functions. We welcomed our family members to the building as part of our Family Day event and children's Christmas party. Later in the year, I was also pleased to invite former ASIO officers for a tour of the building.

Integral to our success is our ability to attract, develop and retain talented and committed people. We also need to ensure that we are maximising the unique and diverse skills of all our people. My vision for ASIO is to be an employer of choice, and an organisation of diversity and innovation. On a wide range of fronts ASIO is doing well. Yet we acknowledge the things that aren't working, and are in the process of change in these areas.

Looking ahead, I have no doubt the security environment will continue to pose many challenges but I am confident that we are best placed to protect Australians and Australian interests. This will involve constant and rigorous examination and re-examination of our priorities in a constrained budgetary environment. I will be working very closely with my senior leadership group to ensure we continue to deliver security intelligence outcomes to government while also achieving sustainable improvement of our business management practices.

Protecting Australian interests both here and abroad, including the safety of my own officers, will be top on my agenda.



1

OVERVIEW OF ASIO

About ASIO

ASIO was established in 1949 as Australia's national security intelligence service in a letter signed by then Prime Minister Ben Chifley. In 1956, the Organisation was provided with a legislative framework which has evolved[3] into the current *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).[4] The ASIO Act defines our roles and responsibilities and is the legislative basis for our purpose, activities, and cooperation with partners.

We have a staff of around 1750 working from the capital cities across Australia and a network of liaison offices overseas. This network supports relationships with more than 300 agencies in more than 120 countries. Our budget estimate is $445.2 million for 2016–17.

Our resources are deployed across hundreds of investigations and thousands of leads. We collect intelligence through human intelligence, warranted activities, surveillance, and requests for protected data. We deliver hundreds of thousands of security assessments and communicate thousands of intelligence products and pieces of advice to enable action to be taken.

ASIO's website has a series of information briefs about ASIO's work, our legislative framework, what security intelligence is, what security assessments are, ASIO's overseas presence, and our role in protective security. You can access these briefs at www.asio.gov.au/information-briefs.html.

[3] Two Royal Commissions by Justice Robert Marsden Hope AC CMC QC have shaped this evolution: the Royal Commission into Intelligence and Security 1974-1977 and the Royal Commission into Australia's Security and Intelligence Agencies 1984.

[4] The ASIO Act is available online from legislation.gov.au. The link to the compilation current at the time of writing is www.legislation.gov.au/Details/C2016C00314

Role and functions

Security and intelligence agencies perform an important function in modern societies. ASIO's purpose is to protect the nation and its interests from threats to security, through intelligence collection, assessment and advice for government, government agencies and business.

ASIO's role as the national security intelligence service is anticipatory and protective in nature: it is expected to identify and act against threats before harm has occurred. This is a key difference between ASIO's work and that of law enforcement partners, whose primary focus is the prosecution of criminal offences. This anticipatory work assists the Australian Government to identify and more effectively manage key national security risks.

ASIO's role and functions are determined by law. ASIO must act lawfully, in line with the provisions of the ASIO Act and other relevant legislation and guidance. The Organisation cannot—and does not—operate 'outside the law'. ASIO must also act with propriety: our activities must be conducted effectively, efficiently, ethically and without bias. ASIO is accountable to the Attorney-General and subject to parliamentary and independent scrutiny. All of this is by design to provide assurance that ASIO acts independently, lawfully and properly discharges its functions.

In line with the functions and areas of security focus mandated in the ASIO Act, ASIO's key priorities today are:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders;
- countering serious threats to Australia's border integrity;
- providing protective security advice; and
- collecting foreign intelligence in Australia.

In pursuing these activities, the Organisation works closely with Australian and international intelligence, law enforcement, border and security agencies, as well as with business and industry, and relies on the support of people from all communities.

ASIO activities are necessarily secret. Inherent in ASIO's responsibilities is the need to investigate Australian citizens, many of whom may subsequently be shown to have no association with the line of inquiry. ASIO thus has a responsibility to protect the reputations of innocent Australian citizens; it does this through information security or secrecy provisions. Over and above the issue of 'protecting the innocent', there is a need to protect sources, tactics, techniques, technologies and procedures. ASIO is also required to protect the identity of its officers.

Organisational structure

There are three groups in the organisational structure:

- strategy;
- counter-espionage and interference, and capabilities; and
- counter-terrorism.

This functional arrangement reflects the resources and governance required for our dominant and high-risk activities:

- countering terrorism and the promotion of communal violence; and
- countering espionage, foreign interference and malicious insiders.

The structure is shown on pages 12–13.

Organisational structure

as at 30 June 2016.

Duncan Lewis

DIRECTOR-GENERAL OF SECURITY

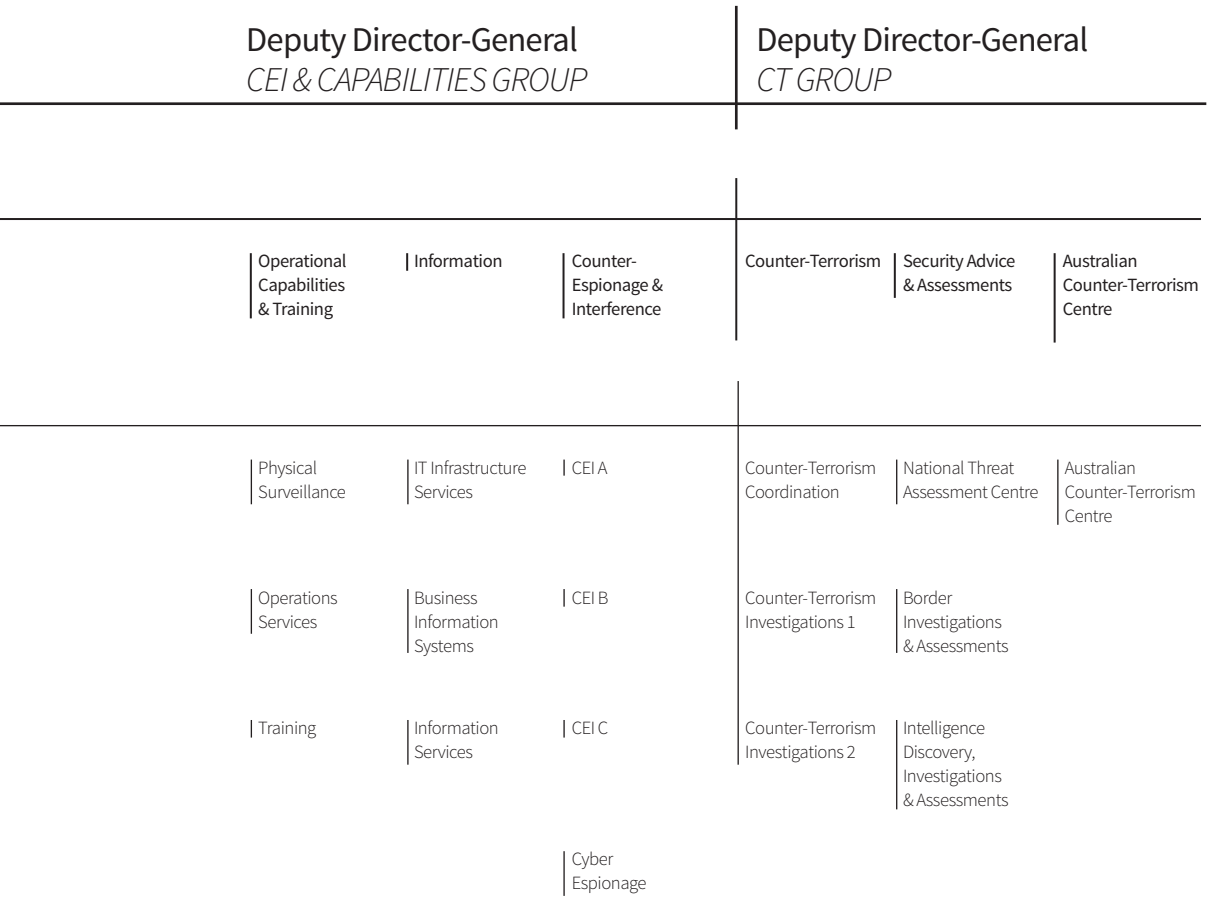
Deputy Director-General
STRATEGY GROUP

First Assistant Director-General

- State Manager NSW North
- Executive
- State Manager VIC South
- Corporate & Security
- Office of Legal Counsel
- Technical Capabilities

Assistant Director-General

- Office of the Senior Executive
- Strategic Partnerships & Production
- ASIO2020
- State Manager QLD
- State Manager SA
- State Manager WA
- State Manager TAS
- Territory Manager NT
- Territory Manager ACT
- Internal Security
- Financial Management
- Human Resources
- Property
- Security Assessments, Employment & Commercial Law
- Legislation, Warrants & Technical Capabilities
- Litigation
- Operations & Capability Protection
- Data & Technical Analysis
- Telecommunication Operations
- Computer Operations
- Close Access Operations
- Strategy & Performance


Deputy Director-General
CEI & CAPABILITIES GROUP
Deputy Director-General
CT GROUP
Operational Capabilities & Training
Information
Counter-Espionage & Interference
Counter-Terrorism
Security Advice & Assessments
Australian Counter-Terrorism Centre
Physical Surveillance
IT Infrastructure Services
CEI A
Counter-Terrorism Coordination
National Threat Assessment Centre
Australian Counter-Terrorism Centre
Operations Services
Business Information Systems
CEI B
Counter-Terrorism Investigations 1
Border Investigations & Assessments
Training
Information Services
CEI C
Counter-Terrorism Investigations 2
Intelligence Discovery, Investigations & Assessments
Cyber Espionage

Performance contracts with government

For the 2015–16 reporting period, the Portfolio Budget Statement (PBS) details appropriations for ASIO to deliver a security intelligence program to achieve a single outcome for government: to protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government. The single outcome is consistent with the purpose expressed in ASIO's 2015–16 corporate plan.

The three key activities ASIO identified in its corporate plan to achieve its purpose were: countering terrorism and the promotion of communal violence; countering espionage, foreign interference and malicious insiders; and countering serious threats to Australia's border integrity.[5] ASIO's PBS contains two additional deliverables: protective security advice for government and business, and foreign intelligence collection in Australia. These five areas are the benchmark against which ASIO has evaluated its performance for 2015–16 in this annual report.

You can read ASIO's current corporate plan, covering the periods 2016–17 to 2019–20, online at www.asio.gov.au and our chapter in the Attorney-General's Portfolio 2016–17 Portfolio Budget Statements online at www.ag.gov.au/Publications/Budgets.

1

Public outreach

ASIO actively engages with the government and business sectors, the media and the Australian public. The Director-General and Deputy Directors-General are the only publicly identified ASIO officers and lead on ASIO's public outreach through media responses, public speeches and appearances at parliamentary or senate hearings. The Director-General and Deputy Directors-General on occasion speak at public seminars or conferences. ASIO's website has more details on recent speeches and statements made: www.asio.gov.au/media/speeches-and-statements.html

ASIO routinely responds to media inquiries but does not comment on operations, investigations, individuals or operational capabilities. ASIO's media effort includes assisting the media in reporting of national security matters through clarifying information. Media inquiries can be directed to the media team on (02) 6249 8381 or via email media@asio.gov.au.

[5] ASIO considers these activities cover two of the four deliverables in the Portfolio Budget Statement relating to security intelligence analysis and advice, and security intelligence investigation and capabilities.

2

THE SECURITY ENVIRONMENT AND OUTLOOK

Terrorism—the Australian security environment

Australia's National Terrorism Threat Level is PROBABLE—credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to conduct terrorist attacks in Australia.[6]

The National Terrorism Threat Level was raised in September 2014. This was not a response to any one development but rather reflected a range of factors—driven by local and overseas events—that saw unprecedented fluidity in the domestic security environment. While these factors have evolved (and some have deteriorated), their cumulative impact remains significant, and so the National Terrorism Threat Level remains elevated.

During the year, one terrorist attack was conducted in Australia and three terrorist plots were disrupted (see 'Onshore terrorist attacks and disruptions').

The principal terrorist threat in Australia emanates from the small number of Australia-based individuals who remain committed to anti-Western violent Sunni Islamist extremist ideology. This group presents a direct threat as well as a secondary threat due to their ability to influence others.

- Some have turned their attention to onshore attack planning after the cancellation of their Australian passports—preventing them from travelling to join terrorist groups in the conflict zone in Syria and Iraq—while some are returnees from that conflict.
- There are around 40 returnees from the conflict in Syria and Iraq. ASIO assesses the vast majority of these are not of security concern, because their activities in Syria were not related to terrorist organisations and they returned before the declaration of the caliphate. However, in the longer term, the small number ASIO is concerned about will be joined by others returning from the conflict who have trained and fought with Islamic State of Iraq and the Levant (ISIL), and other groups of concern in the region. They will have been deeply indoctrinated into ISIL's ideology and inured to the use of extreme violence. It is possible they will undertake terrorist attacks themselves or enable others to do so. ASIO also hold concerns about their connections to networks of extremists who could be a source of information and guidance.
- Recruitment and radicalisation by Australia-based extremists is a key risk. Terrorist groups, particularly ISIL, are adept at broadly promoting their violent extremist message online by producing a plethora of high production quality, high-impact propaganda; this material resonates with some people in Australia.

The changing nature of terrorism provides challenges to the early identification and detection of threats. While large-scale attacks, including coordinated attacks by multiple individuals, are still occurring around the world, there has been a trend towards simpler attacks that require minimal preparation perpetrated by lone actors.

[6] Information on the security environment is also available from www.asio.gov.au/threat-environment.html.

Onshore terrorist attacks and disruptions

The National Terrorism Threat Level is PROBABLE

Common factors

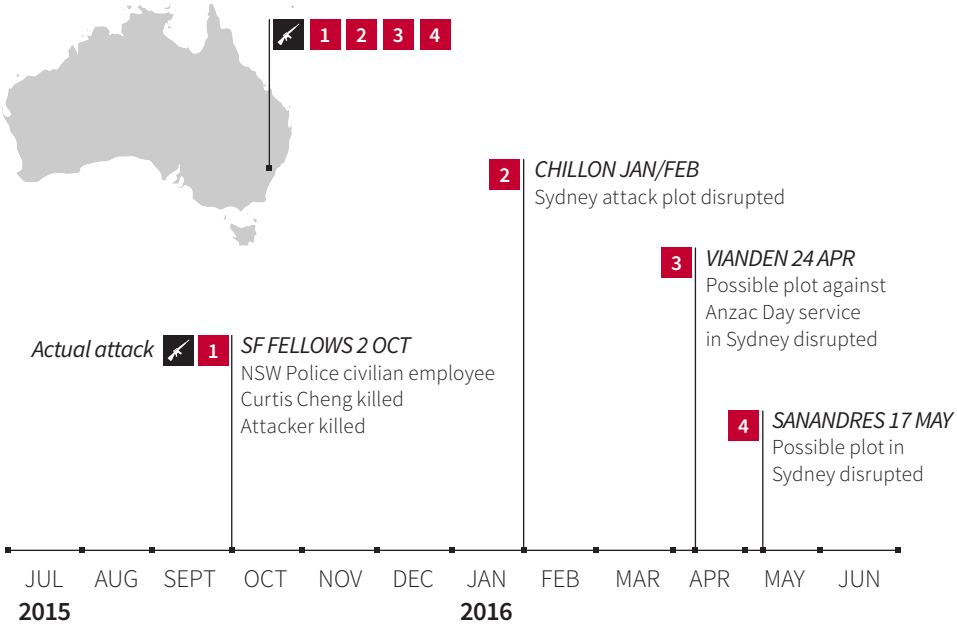
Offshore influences

- Direct communication with offshore extremists
- Graphic and slick publications
- targeted radicalisation

Onshore influences

- Prevention of travel
- Pressure from onshore extremists

- Providing justification, instruction, encouragement and direction for onshore attack
- ISIL affiliation
- Rapid targeting
- Spontaneous and rudimentary attack methodology
- Targeting Australian Government and public



A lone actor is an individual (or small group of like-minded individuals) who conducts, or plans to conduct, a disruptive and typically violent activity for political or religious motives. At the time the action is performed they act independently of real-world accomplices. A range of Islamist extremist groups, most notably and recently ISIL, actively encourage terrorist attacks against 'far enemies'. This type of threat can develop quickly, typically requires little preparation or planning, and can come from individuals who are on the periphery of investigations or who are unknown to authorities.

Many of the recent terrorist attacks and disrupted plots in Australia involved individuals or small groups who were radicalised, often through isolated online activity, to the point where they were willing to act out their grievances through the use of violence.

The four onshore attacks since 2014 were all conducted by single individuals using relatively simple weapons (two with knives and two with firearms). While symbols of government and authority—including military, police and security agencies—remain attractive targets, indiscriminate attacks against the public align with the objectives of terrorists. ISIL, and to a lesser degree al-Qa'ida, continues to endorse and celebrate indiscriminate attacks against innocent citizens so as to reinforce their message and incite fear.

- One aspect of this threat is ISIL's effective campaign of identifying individuals who are susceptible to peer-to-peer radicalisation, enabled by secure communications. Individuals who are vulnerable are typically young disenfranchised and marginalised males who are ill equipped to consider the consequences of their actions.
- Recent onshore terrorist plots have centred on would-be attackers who were groomed and assisted by overseas extremists. While the number of individuals who fall into this category is small, in attacks such as those in Nice, France, and Orlando, United States, we have witnessed the devastating impact a single attacker can have.

A further concern is the increased communal violence between opposing groups in Australia. We have already seen violence between anti-Islam and left-wing groups and protests and rallies, especially in Victoria.

Terrorism—the international security environment

The international security environment is deteriorating due mainly to the influence of resurgent Islamist terrorist groups. The predominant threat emanates from two highly capable and well-financed terrorist groups: ISIL and al-Qa'ida. Both have an international following and global reach, and both leverage this to promote an anti-Western, violent Sunni Islamist extremist ideology. They conduct attacks against Western interests, religious minorities and secular interests, and also exhort adherents to take unilateral action (see 'Global terrorist attacks'). Regional threats come from a range of entities affiliated with, and inspired by, these two groups. These include the South-East Asia–based Abu Sayyaf Group (ASG), Africa-based Boko Haram, al-Shabaab and al-Qa'ida in the Islamic Mahgreb (al-Qa'ida-IM), and the Asia-based Taliban.

The conflict in Syria and Iraq is central to the global resurgence of Islamist extremist terrorism. The conflict presents overlapping security issues:

- the increase in ungoverned spaces and spaces controlled by extremists (such as northern Syria, northern Iraq, Yemen and Libya) that allows extremists to more easily recruit globally, train locally, and plot external attacks in Europe, South-East Asia, Africa, other Middle Eastern countries and elsewhere throughout the globe;
- the threat from returning foreign fighters. Many are battle hardened, inured to the use of violence and have been further radicalised with a strengthened commitment to Islamist extremism. These individuals have credibility and influence which can be used to radicalise others; and
- the threat from those who have not travelled, or have been prevented from travelling, and remain in their home countries. With the opportunity to travel removed, some may turn their attention to onshore attacks, including low-capability attacks that require little skill to conduct effectively. Recent attacks and disruptions in Australia, Europe, the United States, Malaysia, Indonesia and Bangladesh underscore this threat.

In South Asia, ISIL is increasing its influence. This is concerning in light of the broad ISIL message encouraging attacks against Westerners as well as secular and religious minorities. The al-Qa'ida threat in South Asia has not diminished either; the al-Qa'ida affiliate al-Qa'ida in the Indian Subcontinent (al-Qa'ida IS), has increased its presence and undertaken attacks in Pakistan and Bangladesh. Additionally, al-Qa'ida–aligned groups such as Lashkar-e-Tayyiba continue to plot and conduct attacks. The security environment in Afghanistan will continue to deteriorate as the Taliban, al-Qa'ida and the Islamic State Khorasan Province continue to challenge the capability of Afghan security forces.

In Africa, ISIL and al-Qa'ida–aligned groups continue to flourish, evidenced by the number of newly declared ISIL provinces: ISIL-Sinai, ISIL-Libya, ISIL-Algeria and ISIL-West Africa (Boko Haram). This expansion threatens regions previously regarded as safe and poses an increasing threat to foreign interests.

In South-East Asia, the influence of ISIL is growing in a number of countries. In 2016, Indonesia and Malaysia suffered their first terrorist attacks conducted by ISIL-aligned extremists linked to South-East Asian foreign fighters based in Syria and Iraq. Hundreds of individuals from South-East Asia have travelled to Syria and Iraq to fight in the conflicts, including with ISIL. Some of these foreign fighters direct, advocate or encourage attacks, including against Australian interests, and this will motivate some individuals to act. Returnees from the conflict in Syria and Iraq may also increase the likelihood of a terrorist attack. A further troubling development is the declared allegiance of some Philippines groups to ISIL. ASIO is concerned that areas in the southern Philippines could develop into safe havens for regional extremists and returning foreign fighters, who could plan attacks against Western interests throughout the region. The terrorist threat against Australians and Australian interests in the region is unlikely to abate in the near future.

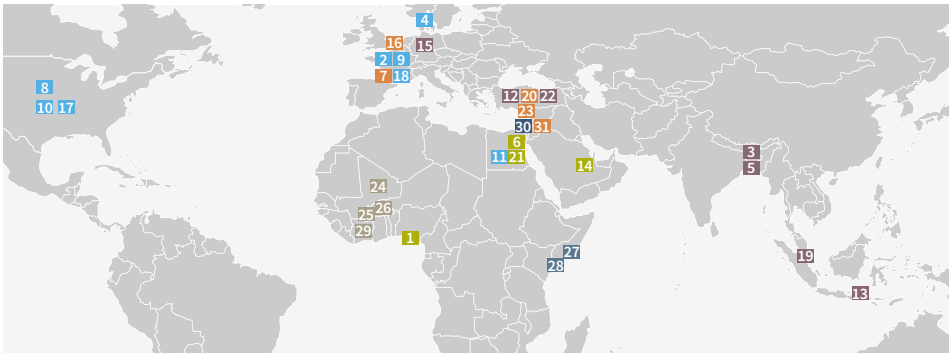
In Europe, the security environment worsened, as demonstrated by attacks in Paris in November 2015, in Brussels in April 2016, and more recently in Nice and Rouen in July 2016. Significant improvement in the foreseeable future is unlikely. Heightened security and counter-terrorism operations in the wake of devastating attacks in many countries likely delayed further terrorist attack plans, but the heightened effort is increasingly unsustainable and may only lead to temporary mitigation.

In Turkey, domestic tensions and proximity to the Syrian conflict negatively impacted on the security environment. There are now at least four active terrorist groups with the intent and capability to conduct large-scale attacks, and some have a stated or proven willingness to target tourists.

Global terrorist attacks

Some regions see attacks daily or weekly, such as the Middle East or West Africa, other regions less frequently. Globally, some attacks have proven highly lethal. Others have resulted in no fatalities, but this does not diminish the seriousness of the threat in these environments.

Through 2015–16 ISIL exerted global reach and influence, inspiring, encouraging and directing multiple attacks, with various methods and tactics employed in the conduct of those terrorist attacks. Al-Qa'ida also remains a threat, with its branches continuing to successfully conduct attacks on the African continent during 2015–16, while its senior leadership and core elements also retain the intent to conduct attacks in the West.



2 Attack provenance

- ISIL Province
- ISIL Directed
- ISIL Encouraged
- ISIL Inspired
- al-Qa'ida Islamic Maghreb
- Al-Shabaab
- Palestinian extremist

Key

✘ Dead ╲ Wounded

Weapons

- Basic weapon (edged)
- Basic weapon (vehicle)
- Explosive
- Firearm

Tactics

- Armed attacker
- Stabbing
- Explosion
- Hostage
- Suicide bombing
- Aviation bombing

Targets

- Public
- Government (military)
- Government (police)
- Australian aid workers
- $ Commercial

Nigeria 16.7.15 1

Gombe market bombing, Damaturu prayer ground bombing.

✕65 \0

France 21.8.15 2

Terrorist attack on Paris-bound train — three injured.

✕0 \3

Bangladesh 28.9.15 3

Multiple attackers shot and killed an Italian citizen.

✕1 \0

Denmark 29.9.15 4

A rejected Palestinian refugee stabbed a police officer at an asylum centre.

✕0 \1

Bangladesh 3.10.15 5

Multiple attackers shot and killed a Japanese citizen near Rangpur.

✕1 \0

Sinai, Egypt 31.10.15 6

Explosion on board Russian Metrojet Flight 9268 killing 224 people.

✕224 \0

France 13.11.15 7

Series of coordinated attacks in Paris, killing 130.

✕130 \368

United States 2.12.15 8

Shooting attack in San Bernardino, United States.

✕14 \22

France 7.1.16 9

Lone actor attack on a Paris police station.

✕0 \0

United States 7.1.16 10

Shooting attack on Philadelphia police officer.

✕0 \1

Egypt 8.1.16 11

Stabbing attack against European tourists — three people injured.

$

✕0 \3

Turkey 12.1.16 12

Likely ISIL suicide bomber kills 10 people, all foreigners, injuring 15.

✕10 \15

Indonesia 14.1.16 13

Attack in central Jakarta targeting a Starbucks café and a police post.

✕4 \23

Saudi Arabia 29.1.16 14

Twin suicide attack on the Imam Rida mosque.

✕4 \18

Germany 26.2.16 15

A teenager stabbed a police officer at Hannover's main train station.

✕0 \1

Belgium 22.3.16 16

Coordinated bombings in Brussels.

✕32 \340

United States 12.6.16 17

Mass shooting in Orlando, Florida by a lone gunman.

✕49 \53

France 13.6.16 18

Attack on two police officers.

✕2 \0

Malaysia 28.6.16 19

Grenade attack on a bar in Puchong.

✕0 \8

Turkey 28.6.16 20

Armed attack at Istanbul's Ataturk Airport.

✕44 \236

Egypt 22.7.15 21

ISIL beheaded a Croatian citizen.

$

✕1 \0

Turkey 10.10.15 22

Twin suicide bombings in Ankara.

✕102 \508

Lebanon 12.11.15 23

Two ISIL suicide bombers attack Shia neighbourhood of Beirut.

✕46 \240

Mali 20.11.15 24

Radisson Blu hotel attack.

✕22 \0

Burkina Faso 14.01.16 25

Two Australians kidnapped.

✕0 \2

Burkina Faso 15.01.16 26

Hotel Cappuccino attack.

✕30 \0

Somalia 2.2.16 27

Daallo Airlines bombing.

✕0 \0

Somalia 7.2.16 28

Beledweyne Airport attack.

✕6 \0

Cote d'Ivoire 13.3.16 29

Grand Bassam attack.

✕18 \33

Israel 18.4.16 30

Improvised explosive device attack on a bus in Jerusalem.

✕0 \23

Jordan 21.6.16 31

Vehicle borne improvised explosive device attack against Jordanian Armed Forces at the Syrian border.

✕7 \13

Communal violence and violent protest

While Sunni Islamist extremism is the pre-eminent terrorist threat facing Australia, other groups continue to engage in politically motivated violence and the promotion of communal violence. Members of these groups are diverse and have differing agendas, including extreme right-wing and extreme left-wing ideologies. A few small subsets of these groups are willing to use violence to further their own interests. While their activities are concerning, they remain a small part of their broader movements and their activities are presently unlikely to lead to wide-scale violence or pose a threat to social cohesion.

Violence at protests in Australia is rare, and the vast majority of protest attendees are peaceful and support our democratic ideals. Social discourse around anti-Islam and anti-migration issues has increased, and public protests for and against have become more frequent; these provide an opportunity for ideological adversaries to converge and sporadic violence can result. Over the past 12 months, violence at protests has mostly comprised small-scale clashes between right-wing and left-wing opponents at anti-Islam protests or protesters targeting police maintaining public order.

Other groups with overseas separatist agendas are represented in Australia, but their membership is small and their influence is limited. Activities in support of overseas issues are mostly confined to fundraising and ideological support.

Espionage, foreign interference and malicious insiders

The harm caused by hostile intelligence activity can undermine Australia's national security and sovereignty. It can damage our international reputation and degrade our diplomatic and trade relations. Both espionage and foreign interference can inflict economic damage, degrade or compromise nationally vital assets and critical infrastructure, and threaten the safety of Australian nationals. Espionage and foreign interference targeting Australian interests remains pervasive and enduring.

One of the most insidious features of both espionage and foreign interference is that the consequences of even a small level of activity can be severe, but can take years to be realised. ASIO has observed increased targeting of Australian interests in Australia and abroad through a variety of methods against an array of sectors.

Australia is a target of hostile foreign intelligence services as a result of:

- our alliance with the United States and the defence relationship we share;
- a desire to gain insights into our positions on international diplomatic, economic and military issues;
- our energy and mineral resources;
- our innovations in science and technology;
- a desire to shape the actions of decision-makers and public opinion; and
- the reach of online technologies enabling hostile cyber activities.

A range of countries continue to conduct espionage against Australia's vital national interests, including our defence capabilities and economic intent. Economic espionage is driven by Australia's role as a global commodity supplier, potential joint venture partner, market competitor, and our advances in scientific research.

Inappropriate and untoward foreign interference in Australia aims to shape the actions of decision-makers and public opinion in order to achieve an outcome favourable to foreign interests.

Cyber espionage can have a significant impact on Australia's national security, economic prosperity, sovereignty and international reputation. Foreign state-sponsored adversaries are targeting the networks of the Australian Government, industry and individuals to achieve intelligence requirements relating to economic advantage, foreign policy, defence and security information, science and technology.

The range, scale and sophistication of state actors engaged in hostile cyber espionage activity against Australian Government and private sector systems continues to increase, as does the threat from malicious insiders. An increasing number of countries are pursuing a cyber espionage program as this offers returns for relatively low cost and plausible deniability. The continued evolution of technology increases the sophistication and complexity of attacks, while rendering the capability increasingly accessible.

Understanding and degrading the espionage and foreign interference activities of our adversaries is among the most challenging types of intelligence work. Undetected espionage activity can have long-term implications, undermining our society and way of life. ASIO works with all government agencies and the private sector to increase awareness of the threat and to implement effective mitigation strategies.

ASIO actively works across government to prevent 'malicious insiders'. These are potential, current or former government employees who have privileged access to information, techniques, technology, assets or premises who deliberately compromise their privileged position breach their duty to maintain the appropriate security conferred upon them by the nature of this access. This potential harm has been aggravated by technologies allowing the aggregation and transfer of large amounts of information.

Malicious insiders can undertake a range of damaging activities, including:

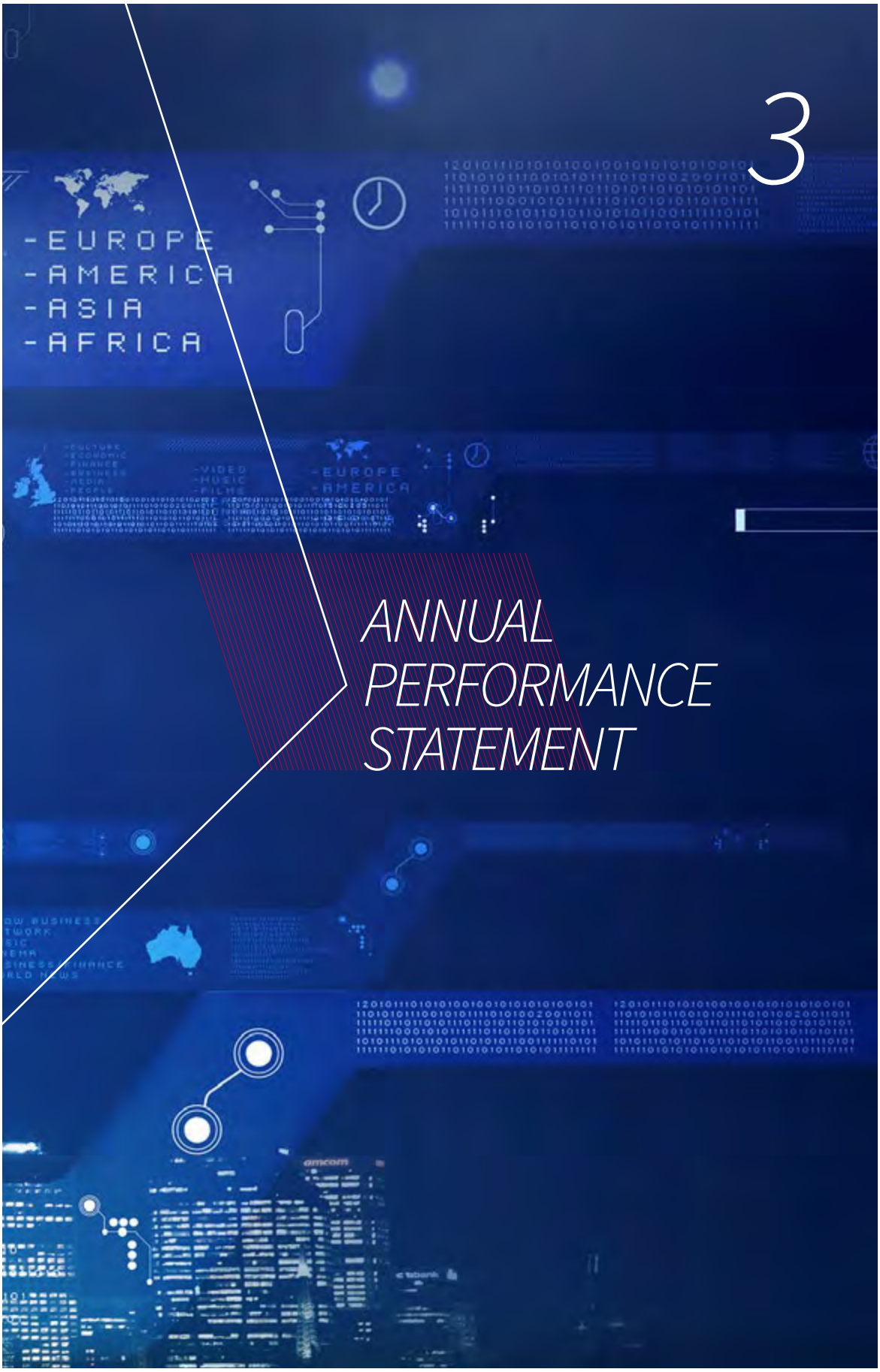
- influencing decision-making processes;
- sabotaging computer systems or equipment;
- using inside information to facilitate an attack;
- mounting a physical attack from the inside; or
- releasing information with the intent to harm Australia's national security and stability.

Malicious insiders are divided into two broad categories based on their intent and motivation:

- self-motivated malicious insiders—individuals whose actions are undertaken of their own volition and not initiated as the result of any connection to, or direction by, a third party; and
- recruited malicious insiders—individuals co-opted by third parties, such as a foreign intelligence service, to exploit their potential, current or former privileged access.

Border integrity

The people-smuggling environment remained similar to that of the past two reporting periods, with significant reduction in planned and actual illegal maritime ventures to Australia. However, people smugglers motivated by financial gain sustained their attempts to actively recruit potential illegal immigrants by marketing misinformation about Australia's border policy, political situation and other events as indicators that Australia's border policy would be relaxed. ASIO continued to work with other Australian Government agencies to counter people-smuggling through participation in Operation Sovereign Borders (OSB).


3
-EUROPE
-AMERICA
-ASIA
-AFRICA
ANNUAL
PERFORMANCE
STATEMENT

Introductory statement

I, as Director-General of Security and the accountable authority of ASIO, present the 2015–16 annual performance statements of ASIO, as required under paragraph 39(1)(a) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). In my opinion, these annual performance statements accurately present the performance of ASIO in achieving its purpose and comply with subsection 39(2) of the PGPA Act.

Some detail has been removed from the performance statements included in the annual report tabled in parliament so as to avoid prejudicing ASIO's activities (in accordance with determinations made by the Attorney-General and the Minister for Finance under the PGPA Act). The complete performance statement is retained in the classified annual report to the Attorney-General, which is also received by the Minister for Finance, other national security ministers, senior officials, the Inspector-General of Intelligence and Security, and is accessible to the Australian National Audit Office.

Duncan Lewis

Our purpose

ASIO's purpose is to protect the nation and its interests from threats to security through intelligence collection, assessment, and advice for government, government agencies, and business.[7]

Our approach to performance

ASIO's overall approach to performance measurement in our corporate plan is to consider the risk management effects generated for our stakeholders as a result of our security advice, reporting, and services.

ASIO pursues its purpose of protecting the nation from threats to security through five activities:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders;
- countering serious threats to Australia's border integrity;
- providing protective security advice to government and business; and
- collecting foreign intelligence in Australia.

The annual performance statements reflect our performance against each of these activities. One source of performance feedback comes from our annual stakeholder survey. The survey seeks feedback from ASIO's partners on their engagement and experience with ASIO and their use of our advice, reporting, and services.

ASIO is also subject to a range of external evaluations of our intelligence role, including:

- the Department of the Prime Minister and Cabinet's evaluation of national intelligence outcomes;
- the evaluation processes established as part of the Australian Government's strengthened counter-terrorism governance arrangements in 2014; and
- the National Intelligence Collection Management Committee's ongoing evaluation of national intelligence collection efforts.

[7] This is the expression of the organisation's purpose from ASIO's 2016–17 corporate plan. It is an evolution of the purpose described in ASIO's 2015–16 corporate plan: 'ASIO provides advice, in accordance with the ASIO Act, to ministers and appropriate agencies and authorities, to protect Australia and its people from threats to national security.' The updated purpose is clearer about the contribution ASIO makes for its key stakeholders.

Financial performance

ASIO's financial position continued to be under pressure throughout the year due to the nature and number of investigations, the heightened security environment, and escalating business costs—including those associated with infrastructure, technologies, staff safety and partner agency relationships.

ASIO actively managed its expenditure; where possible, business practices were streamlined and selected activities re-priorisited to release funds for emerging priorities. Despite this, our financial result was an operating loss of $5.4 million, excluding depreciation. The Minister for Finance approved a $2.8 million operating loss due to the accounting treatment required by Australian Accounting Standards Board Standard 'Employee benefits' (AASB119). External factors impacting on employee leave provisions also moved disproportionately in the latter part of the year, resulting in a variance of $4.4 million (as approved to $2.8 million).

As the challenging fiscal environment is expected to continue, ASIO will continue to strive to identify and implement efficiencies to operate within future budget allocations.

The 2015–16 financial year was the second year of the '*National security—additional counter-terrorism funding*' measure announced in August 2014, with funding received through the 2014–15 additional estimates process in February 2015. ASIO received $31.2 million in operating funding and an equity injection of $13.8 million for capital activities during the year. ASIO anticipates receiving $97.3 million in operating funding and $27.6 million in capital funding for this measure over the next two financial years.

ASIO received $0.8 million under the '*Syrian and Iraqi humanitarian crisis*' measure through the 2015–16 portfolio additional estimates process, and will receive a further $0.6 million for this measure in 2016–17. ASIO also contributed to government initiatives, including $3 million for the National Security Hotline Campaign, and savings measures that will impact on the Departmental Capital Budget and the operating budget across and beyond the forward estimates.

The operating loss for 2014–15 was $12.7 million; a $13 million loss was approved by the Minister for Finance, due to one-off expenditure incurred during the relocation to the Ben Chifley Building. Supplier costs were lower in 2015–16, as anticipated; however, employee-related expenditure increased.

ASIO's Departmental Capital Budget was $32.1m in 2015–16. Asset replacement funding was re-phased in previous financial years to align with our updated replacement schedule. Capital acquisitions during the year reflected this program.

Results against performance measures

ASIO has evaluated the achievement of its purpose through five activities and related measures established in the corporate plan and PBS. The three key activities ASIO identified in the corporate plan to achieve our purpose were:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders; and
- countering serious threats to Australia's border integrity.[8]

ASIO's PBS contains two additional deliverables: protective security advice, and foreign intelligence collection in Australia.

This section presents ASIO's performance against each of the five activities and deliverables described in ASIO's corporate plan and PBS, as well as for all activities in terms of the legality, propriety and security of ASIO's activities. The measures used are taken from ASIO's corporate plan and PBS, with duplication of measures avoided to ensure conciseness of reporting.[9] ASIO's corporate plan and PBS were refined and aligned in 2016–17 to ensure clarity across these strategic documents between activities and deliverables, and between performance measures and key performance indicators.

[8] ASIO considers these three activities cover two of the four deliverables in the PBS, relating to security intelligence analysis and advice, and security intelligence investigation and capabilities.

[9] ASIO considers the corporate plan performance measure 'Effective advice, reporting and services that assist the Australian Government manage security risks and disrupt activities that threaten Australia's security' addresses performance against the key performance indicator in the PBS of 'The contribution of ASIO's action and advice to the management and reduction of risk to people and property, government business and national infrastructure, and special events of national and international significance'.

Overall performance analysis

The security environment remained challenging for Australia through the period.

- The tempo of counter-terrorism investigations and operations remained elevated across the reporting period. ASIO's intelligence contributed to the disruption of multiple terrorist plots in Australia during the year.
- Clandestine foreign actors continued to cause harm to Australia through espionage, interference and cyber activity. ASIO continued to partner with others to detect, defend against and degrade these activities.
- The deteriorating international security environment highlighted the importance of intelligence advice on the cross-border movements of persons of security concern. While most travellers to and from Australia were not of security concern, ASIO identified a small number who posed a potential risk to national security, predominantly on the grounds of politically motivated violence.
- Other ongoing challenges include the pervasiveness of online activities and encryption technologies, the diminishing intelligence value from increasingly encrypted content and datasets, demographic changes in the nature of the terrorism threat, the increased pace of radicalisation and the ongoing risk of lone actors.

The demand from clients for security advice continued to be high—driven by the terrorism, espionage and cyber challenges of the security environment—requiring ASIO to adapt its offerings, tailor its outreach, and work with stakeholders to manage expectations.

ASIO surveys key stakeholders in the Australian Government and states and territories through an annual stakeholder survey. The survey seeks to capture feedback on the quality of our advice, the effectiveness of our capabilities and people, and the value added through cooperation and collaboration. Stakeholders surveyed indicated that ASIO:

- is highly or well regarded by agencies, with the organisation and its staff seen as professional and responsive;
- is considered a key partner by many stakeholders across all Australian governments;
- assistance to build or enhance their own capabilities would be/is appreciated;
- assessed product and analytical capability is respected, across both the counter-terrorism and countering espionage and interference activities, and many stakeholders expressed an appetite for more anticipatory assessments; and
- remained responsive and agile in providing counter-terrorism intelligence and support to partners, and law enforcement partners expressed an appetite for increased availability of unclassified information to enhance our cooperation and enable their activities.

Countering terrorism and the promotion of communal violence

Intended results

- Identify terrorism-related activities and the promotion of communal violence affecting Australia, its people and its interests.
- Provide advice and undertake or enable activities that disrupt terrorism-related activities and the promotion of communal violence affecting Australia, its people and its interests.
- Advice improves the effectiveness of the Australian Government's protective security responses to terrorism.
- Advice supports the development of Australian Government policy responses to terrorism and the promotion of communal violence.

Measure

Effective identification of threats to Australia's security

3

Where did the measure come from?

2015–16 Corporate Plan

- Streamlining of internal resources and processes increased ASIO's intelligence discovery function and the agility with which ASIO responded to security incidents.
  - This included new capabilities dedicated to intelligence discovery, including online, and the generation of actionable intelligence in support of investigations.
  - Resources focused on enabling partners to identify 'indicators' of radicalisation were increased.
- ASIO investigations and cooperation with partner agencies resulted in the disruption of three terrorist plots in Australia over the past 12 months. Beyond these major disruptions, close cooperation between intelligence and law enforcement agencies has also led to a series of targeted disruptions and other activities to contain threats.
  - During the period, there was also one terrorist attack on the New South Wales (NSW) Police office in Parramatta, which involved the fatal shooting of NSW Police employee Curtis Cheng. ASIO intelligence assisted the post-incident investigation.

Measure

Effective advice, reporting and services that assist the Australian Government manage security risks and disrupt activities that threaten Australia's security

Where did the measure come from?

2015–16 Corporate Plan

- Enhancements were made to ASIO products and delivery mechanisms for security intelligence advice, including through implementation of the new National Terrorism Threat Advisory System and the development of new lines of threat reporting to enhance timeliness and relevance for all stakeholders.
- ASIO continued to produce timely and relevant security intelligence advice, informing the security posture of government, industry and business which underpinned their risk management and mitigation activities.
- ASIO worked closely and collaboratively with Australian and international partners to share information and assessments about threats to Australia's security, ensuring the Australian Government was fully informed on developments with the potential to impact on Australia.
- ASIO expanded its outreach to Australian agencies to inform more Australian policy-makers and to shape future collection/reporting requirements.
  - Work is ongoing with a range of policy and service delivery agencies both for disruptions and for supporting vulnerable individuals and sections of the community.

Countering espionage, foreign interference and malicious insiders

Intended results

- Discover espionage, foreign interference and the activities of 'malicious insiders' and degrade their impacts.
- Advice improves the effectiveness of Australian Government defences against clandestine espionage, foreign interference and malicious insiders.

Measure

Effective identification of threats to Australia's security

Where did the measure come from?

2015–16 Corporate Plan

- ASIO continued to identify significant collection activities being undertaken by foreign intelligence services, which were detrimental to Australia's security.
  - Significant espionage and foreign interference activity was detected and degraded, though more undetected activity is likely to be occurring as the scale exceeds our capacity to respond.
  - This included cyber targeting and exploitation activities.
  - ASIO, in conjunction with partner collection agencies, reported on a range of targeting priorities of hostile foreign intelligence services.
- ASIO investigations, operations and liaison with foreign partners identified continued targeted efforts to access sensitive and/or classified Australian Government information.
- ASIO continued to undertake investigations into apparent breaches by persons in trusted positions with access to sensitive information.
- ASIO's Contact Reporting Scheme continued to act as an important means of detecting possible espionage and foreign interference activities.

Measure

Effective advice, reporting and services that assist the Australian Government manage security risks and disrupt activities that threaten Australia's security

Where did the measure come from?

2015–16 Corporate Plan

- ASIO continued to develop outreach to industry, government and academic institutions likely to be of interest to foreign intelligence services, and continued to receive requests for defensive briefings—confirming our advice and assessment is in demand, valued and trusted by senior officials, Australian Government agencies and industry.
- ASIO's proactive threat briefings to the Australian Government and state governments in advance of high-profile events, overseas travel and official engagement have led to an increased knowledge of the threat posed by hostile intelligence services. This advice continued to be proactively sought by relevant departments and ministerial offices.
- The ASIO annual stakeholder survey reflected a recognition of the need to pay additional attention to espionage and cyber in particular. The survey results reflected the value of ASIO's work and a strong desire for increased ASIO input into security awareness programs and stakeholders' responses to threats.
- ASIO reporting during the period identified emerging areas of vulnerability and relevant advice was shared across the Australian Government. ASIO worked with other relevant departments to pursue legislative amendments and strategic reforms to respond to Australia's changing threat environment and enhance ASIO and partner capabilities.

Countering serious threats to Australia's border integrity

Intended results

- Identify activities that represent a serious threat to Australia's border integrity.
- Advice is used to assist Australia's agencies effectively manage and/or disrupt activities that represent a serious threat to Australia's border integrity.

Measure

Effective identification of threats to Australia's security

Where did the measure come from?

2015–16 Corporate Plan

- ASIO provided assessments which identified persons of security concern who intended to travel to, or remain in, Australia. This informed decision-making by the Department of Immigration and Border Protection (DIBP) and reduced the threat to Australian interests posed by these individuals.
- ASIO provided intelligence in support of national watchlisting systems which contributed to the identification of persons of security concern, or potential security concern, who intended to travel to or from, or remain in, Australia. This enabled border agencies to take appropriate action in visa issue. Management of travel alert intelligence enabled border agencies to act to mitigate threats to national security.
- ASIO provided intelligence reporting which contributed to border agencies' understanding of the security environment and helped inform their decision-making on threats at the border.
- In conjunction with partner agencies, ASIO undertook activities which led to the identification of individuals involved in maritime people-smuggling networks, and contributed to whole-of-government efforts to disrupt and deter people-smuggling.

Measure

Effective advice, reporting and services that assist the Australian Government manage security risks and disrupt activities that threaten Australia's security

Where did the measure come from?

2015–16 Corporate Plan

- In 2015–16, ASIO completed 11 962 visa security assessments. This helped inform DIBP decision-making on whether to grant, refuse or cancel visas.
- ASIO's finalisation of visa security assessments assisted with the delivery of DIBP's migration program. ASIO worked closely with DIBP to align resources with DIBP's annual and program priorities.
  - ASIO met DIBP's annual targets for permanent visa and refugee/humanitarian caseloads.
  - ASIO met the service-level agreement on the temporary visa caseload.
- ASIO provided 141 820 border-related security access security assessments in 2015–16. Most of these related to Aviation Security Identification Cards (ASIC) and Maritime Security Identification Cards (MSIC). These assessments informed decisions by regulating agencies about whether to grant access to security-controlled areas at airports and ports.
- ASIO contributed to the development of policy and procedure on border security issues, particularly through its engagement with DIBP and the Australian Border Force (ABF) on information-sharing, watchlisting and counter-terrorism disruption arrangements. This helped ensure national security considerations were factored into decision-making on border security.
- ASIO provided analytical and intelligence input to the whole-of-government efforts against people-smuggling as a member of Operation Sovereign Borders (OSB). This helped inform Australian Government policy on people-smuggling issues.
- In 2015–16, ASIO continued its internal review of adverse assessments and issued new assessments on eligible Illegal maritime arrivals previously issued with adverse assessments. The reviews of these assessments were based on new information or changes in the security environment. This directly contributed to DIBP decision-making on the immigration status of these individuals.

Providing protective security advice to government and business

Intended results

- Government, business and industry adopt security by design to protect Australia's people, assets and other national interests.
- There is increased protective security awareness and capacity across Australian Government agencies, business, and industry.

Measure

Effective protective security advice, reporting and services that inform security by design by government, business, and industry

Where did the measure come from?

This measure is in ASIO's 2016–17 Corporate Plan and is an evolution of the measure in the 2015–16 PBS which focuses on management and reduction of risk

- ASIO's T4 Protective Security Directorate seeks to ensure a consistent application of protective security standards across the Australian Government, to assist in protecting information, people and assets. This continued to be achieved by providing high-quality physical security certification program, technical surveillance countermeasures inspections, and resources for security managers to meet policy requirements.
- ASIO continued to provide quality personnel security assessments to enable agencies to issue security clearances to their staff. During the period, ASIO embarked on a continuous program of review and reform in this area and contributed to the development of strategic reforms in personnel security policy.
- ASIO enhanced its strategic analysis capability in relation to national security implications arising from foreign investment, and examined 285 Foreign Investment Review Board (FIRB) referrals from Treasury, which was an increase on the previous year.
  - This has strengthened wider government understanding and decision-making about the threats to Australia's national security from foreign investment, especially in the critical infrastructure sectors.

- ASIO's Business Liaison Unit (BLU) increased its engagement with critical infrastructure sectors, focusing on sectors more likely to be targeted by foreign intelligence services.
- ASIO worked closely with the Department of Veterans' Affairs to provide security advice for the World War One Centenary Commemorations in Turkey, France and Belgium. This advice was tailored and regularly updated in light of the changing security environments in those locations.

Collecting foreign intelligence in Australia

Intended results

- Provide niche foreign intelligence collection services to partners, in accordance with National Intelligence Priorities.

Measure

We provide intelligence that is useful to progress Australia's national security, foreign relations, or economic wellbeing

Where did the measure come from?

This measure is in ASIO's 2016–17 Corporate Plan and is an evolution of the focus in the 2015–16 PBS on client satisfaction and feedback

3

- ASIO continued to collect foreign intelligence, generating advice of unique intelligence value that enhanced Australia's national security.
- ASIO's responsibility to collect foreign intelligence is complemented and supported by other agencies.

Measures across all activities

Measure

Legality and propriety of ASIO activities and effectiveness of the organisation's engagement with oversight and accountability bodies

Where did the measure come from?

2015–16 Corporate Plan

- ASIO engaged closely with the Inspector-General of Intelligence and Security (IGIS) and her office, addressing all requests for information.
  - There were no formal inquiries concerning ASIO.
  - All issues raised by routine IGIS inspections have been resolved, with no impropriety identified.
- ASIO continued to provide briefings and information to the Independent Reviewer of Adverse Security Assessments to facilitate the review of eligible adverse assessments.
- ASIO continued to provide submissions and appear before the Independent National Security Legislation Monitor.
- Compliance and performance audits found ASIO to be compliant with all requirements under relevant legislation, policies and external agreements.

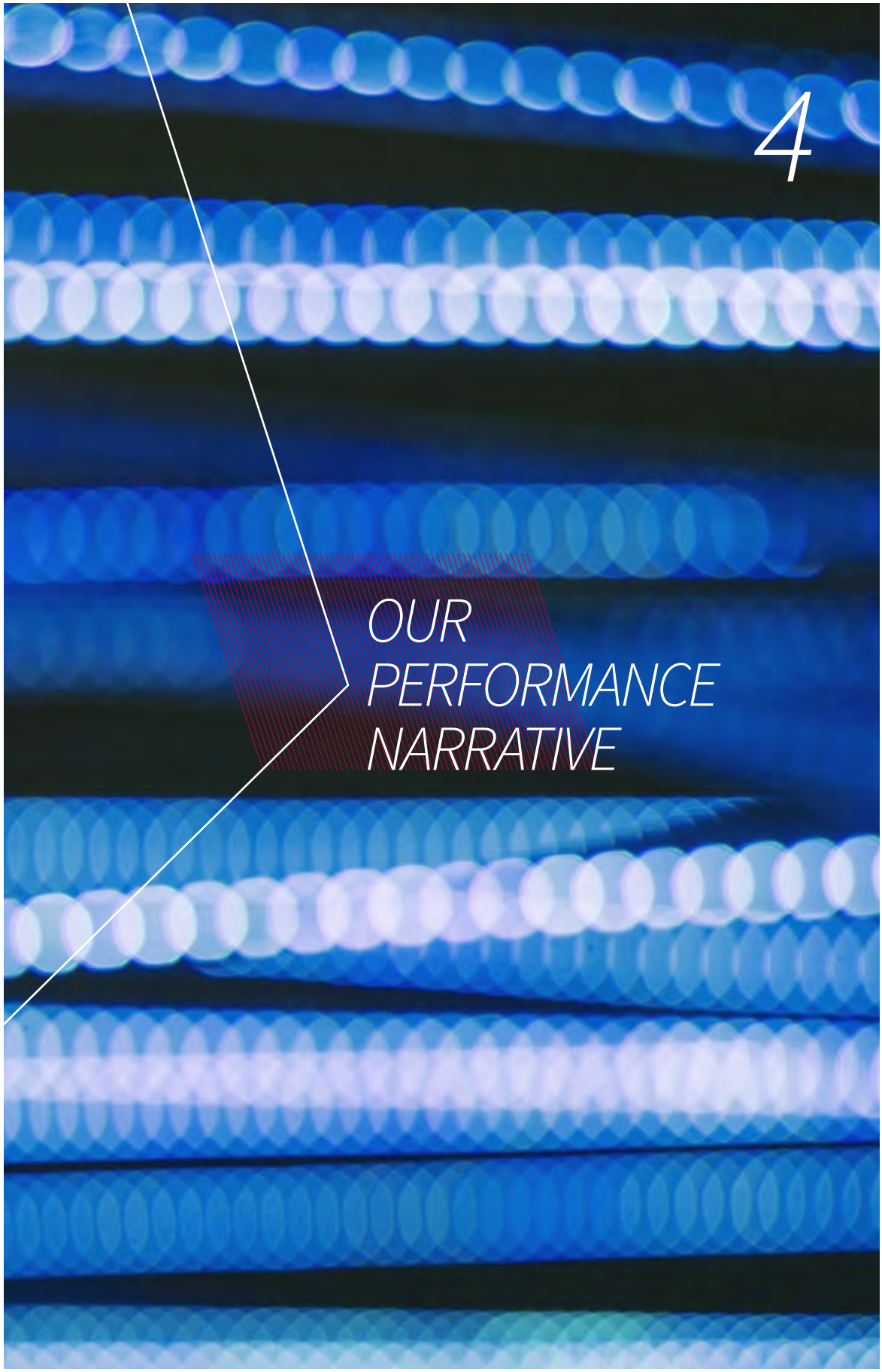
Measure

The security of ASIO's activities

Where did the measure come from?

2015–16 Portfolio Budget Statement

- ASIO continued to enhance its security culture through a range of measures, including mandatory security and safety training.
- ASIO continued to protect information, information technology and resources in line with relevant government policy including the Protective Security Policy Framework.
- ASIO continued to ensure that its policies and procedures were updated to meet the requirements of the security environment in which it operates.



4

OUR PERFORMANCE NARRATIVE

Countering terrorism and the promotion of communal violence

Intended results

- Identify terrorism-related activities and the promotion of communal violence affecting Australia, its people and its interests.
- Provide advice and undertake or enable activities that disrupt terrorism-related activities and the promotion of communal violence affecting Australia, its people and its interests.
- Advice improves the effectiveness of the Australian Government's protective security responses to terrorism.
- Advice supports the development of Australian Government policy responses to terrorism and the promotion of communal violence.

Effective identification of threats to Australia's security

Intelligence discovery

Over the last two years, ASIO has seen a 250 per cent increase in the number of counter-terrorism–related lead referrals. These leads come from a range of sources including from members of the public, other Australian Government agencies and international partners. To meet the demands of an increasingly volatile and unpredictable security environment, ASIO established a branch focused specifically on intelligence discovery and the generation of unique actionable intelligence in support of counter-terrorism–related investigations.

This branch also hosts the multi-agency Jihadist Network Mapping and Targeting Unit (JNMTU), which is now well established as a central point within the national security community for understanding and targeting Australian and South-East Asian foreign fighter networks. Key outcomes have included the generation of a growing number of high-value investigative and operational leads and the identification of several previously unknown foreign fighters.

During the year, ASIO also delivered updated resources to support police identify signs an individual or group may be intending to undertake a terrorist attack. This work made accessible a suite of 'indicators' drawing on our knowledge of radicalisation, extremist behaviour and terrorist methodologies. A program to disseminate this advice, deliver briefings and provide reference materials to departments and agencies was rolled out to over 1000 staff at Australian Government and state/territory levels.

Investigative and operational caseload

Both the number of ongoing investigations being managed by ASIO and the tempo of investigations have remained at a historically elevated level. This is largely, but not entirely, driven by the conflict in Syria and Iraq.
The number of Australians in Syria and Iraq has remained consistent over the reporting period. ASIO continues to investigate the activities of Australians there, to determine what security issues may arise on their return to Australia or their travel to third countries, as well as to identify whether they are involved in efforts to radicalise or inspire others to extremism.

Significant disruptions during the year

During the reporting period, there were three major disruption operations in relation to imminent attack planning in Australia, achieved through close work with law enforcement partners (see Table 1).

The factors that contribute to the elevated terrorist threat in Australia persist, and ASIO continues to identify and investigate individuals in Australia who are engaged in, or support, terrorism. Beyond the three major disruptions noted above, close cooperation between intelligence and law enforcement agencies also led to a series of targeted disruptions and other activities to contain threats.

ASIO provided support to law enforcement agencies in relation to a range of criminal charges that have resulted from joint operations against individuals who are the subject of ASIO counter-terrorism investigations.

January–February 2016	Operation CHILLON (NSW Joint Counter Terrorism Team (JCTT) operation name)	Sydney attack plot targeting members of the public disrupted
April 2016	Operation VIANDEN (NSW JCTT operation name)	Possible plot against Anzac Day service in Sydney disrupted
May 2016	Operation SANANDRES (NSW JCTT operation name)	Imminent Islamist lone actor attack disrupted

Table 1: Counter-terrorism disruptions during 2015–16

Effective advice, reporting and services that assist the Australian Government manage security risks and disrupt activities that threaten Australia's security

Enhancements to ASIO reporting

The National Terrorism Threat Advisory System (NTTAS) was implemented on 26 November 2015 with ASIO integral to the design and development of the system. It is a five-tier, colour-coded system that provides a greater degree of flexibility and nuance at the higher end of the threat scale. A public narrative, provided by the National Threat Assessment Centre (NTAC), is available on the Australian National Security website—www.nationalsecurity.gov.au—informing the public about the nature of the terrorist threat and the likelihood of an act of terrorism occurring in Australia

ASIO enhanced its intelligence reporting during the year. This included the creation of additional lines of reporting to provide assessment and commentary on current investigations, intelligence and threat issues, and to highlight significant or topical lines of reporting produced by the NTAC. Enhanced timeliness and a broader range of recipients have meant partner agencies having increased visibility of potential threats to Australia's security. ASIO has also improved the way in which it conveys key messages, including through the use of information graphics to communicate complex messages and data.

Provision of timely security advice with impact

ASIO's annual stakeholder survey recognised the need for ASIO to remain responsive and agile in the provision of counter-terrorism intelligence and support to partners, and that the rapid pace of operational developments and the constantly evolving security environment made this an ongoing challenge for us.

- Strong positive feedback from partners indicated that NTAC product is particularly valued and respected. Law enforcement agencies were particularly complimentary of ASIO's analytical capabilities with one stakeholder commenting ASIO has no peer in the law enforcement community in this area and it is a capability the law enforcement community has come to rely upon.
- Law enforcement partners also acknowledged ASIO's continued work to improve its appreciation and awareness of evidentiary requirements and were keen for this to continue to grow and for greater accessibility to ASIO intelligence and advice in an unclassified format to assist in the preparation of documentation to enable law enforcement activity.

ASIO's published products contributed to our audiences' understanding of local and international terrorist threats and potential implications for Australian interests globally. ASIO's security intelligence advice also aided government and industry risk managers in protective security decision-making. Our published product included over 40 changes to terrorism threat levels for overseas countries; the advice underpinned decisions by the Department of Foreign Affairs and Trade (DFAT) on travel advice for the Australian public.

In addition to the significant volume of classified reporting produced, where possible, ASIO also published versions of reports at lower classification to broaden the reach of our product and advice. This included the dissemination of 'For Official Use Only' reports to relevant stakeholders from the private sector to inform their security posture.

ASIO's Business Liaison Unit 's (BLU) subscriber-only website published 55 terrorism-related reports to its 3612 subscribers. The BLU also hosted five briefing days, providing classified advice to the aviation, banking and finance, and defence industries sectors, and to those responsible for the security of places of mass gathering and mass passenger transport.

In addition, the BLU briefed a number of industry forums including aviation, energy and resources, and banking and finance groups. The detailed sector-specific information provided to the private sector helps ensure owners and operators of critical infrastructure have relevant information regardless of their security clearance. Broadening the private sector's understanding of threats helps build resilience and raises awareness of potential threats from a range of vectors.

Withholding passports is an important means of preventing Australians from travelling overseas to engage in activities prejudicial to security including training for, or participating in, terrorist activities and concurrently gaining capability which could be used in a future attack. Since December 2014, ASIO has also had the capability to request that the Minister for Foreign Affairs suspend an Australian passport for up to 14 days where ASIO has security concerns about the holder's travel which require further time to resolve.

ASIO can recommend to DFAT 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. For people already in conflict zones, cancellation of their Australian passport helps reduce the risk they pose and may prevent these individuals of concern from using their Australian passports to travel to other countries to do harm. In such cases, temporary documentation can be issued to facilitate the return of Australian citizens to Australia.

In 2015–16, ASIO issued adverse security assessments for 62 passports (see Table 2). While still the second-highest annual number recorded in the past decade, this is a decrease from the previous reporting period—largely due to fewer Australians seeking to travel to the conflicts in Syria and Iraq.

Year	Passports subject to adverse security assessments	Australian passports subject to temporary suspension
2015–16	62	23
2014–15	93	9
2013–14	45	N/A
2012–13	18	N/A
2011–12	7	N/A
2010–11	7	N/A
2009–10	8	N/A

Table 2: Number of passports subject to adverse security assessments or suspension provisions

Notes: The data on passports subject to adverse security assessments includes Australian and foreign passports. The ability to temporarily suspend passports on security grounds came into effect in December 2014.

Cooperation with Australian and international partner agencies

ASIO worked closely with a range of international intelligence and law enforcement partners to manage global security issues relating to international terrorist groups and linked individuals. This included those involved in the conflict in Syria and Iraq and others involved in other international trouble spots.

ASIO representatives participated in multiagency forums, interdepartmental taskforces and working groups on significant issues throughout 2015–16, including:

- major sporting events (focused on the Rio 2016 Olympic Games and the Gold Coast 2018 Commonwealth Games);
- World War One Centenary commemoration events;
- the DFAT-led responses to the three kidnappings of Australians overseas during the reporting period; and
- multi-jurisdictional counter-terrorism exercises.

ASIO participates in the work of the Australia-New Zealand Counter-Terrorism Committee (ANZCTC). The ANZCTC works to the Council of Australian Governments and brings together state and territory police, state and territory Premier's departments, and relevant Australian Government agencies. The ANZCTC's role is to build an effective nationwide counter-terrorism capability. ASIO provides assessments to inform ANZCTC decision-making, participates in the sub-committees and other entities supporting the ANZCTC, and participates in ANZCTC exercises designed to test Australia's counter-terrorism response arrangements. More information on the ANZCTC is available online from www.nationalsecurity.gov.au.

The Australian Government's countering violent extremism (CVE) efforts are led and coordinated by the Attorney-General's Department (AGD) through the CVE Centre. ASIO, and in particular the NTAC, continued its commitment to the AGD-led CVE effort by providing security intelligence advice and other measures to help build and support CVE programs and capabilities. This included tailored assessments written to share CVE-specific information with Australian Government departments and agencies.

Countering espionage, foreign interference and malicious insiders

Intended results

- Discover espionage, foreign interference and the activities of 'malicious insiders' and degrade their impacts.
- Our advice improves the effectiveness of Australian Government defences against clandestine espionage, foreign interference and malicious insiders.

Effective identification of threats to Australia's security

ASIO continued to conduct investigations and provide advice on the threat from hostile foreign intelligence services. But it is difficult to quantify the harm from espionage and foreign interference activity because of the disparate nature of the activities and their latencies. Indeed, victims are generally unaware such activities have occurred because of their clandestine nature. Although there is some visibility of the activity against Australian interests, we are confident there is more activity than is evident. ASIO, as part of the Australian Cyber Security Centre (ACSC), is aware of daily cyber espionage activity targeting Australian Government networks.

ASIO continued to investigate apparent breaches by trusted insiders with access to sensitive information. Malicious insiders are individuals who deliberately and wilfully breach their duty to maintain the security of their privileged access to information, techniques, technology, assets or premises. They have always been a potential source of harm to Australia's national interests. ASIO continued to work closely with other government agencies to ensure that all agencies maintain a collective, best practice approach to the threat of malicious insiders.

The Contact Reporting Scheme is a whole-of-government counter-espionage strategy managed by ASIO as part of the Protective Security Policy Framework (PSPF). Information obtained through the scheme can:

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

Trends from the scheme inform ASIO's protective security response to foreign nationals in contact with Australian government officials. For this reason, ASIO actively works to promote the scheme and encourages compliance and participation in line with the PSPF.

Effective advice, reporting and services that assist the Australian Government manage security risks and disrupt activities that threaten Australia's security

ASIO provides advice on the threat that hostile intelligence services pose to our officials abroad and recommends protective security measures. ASIO is investing significant effort in addressing government's growing need for more quantifiable information on the harm and estimated financial costs of espionage to Australia.

ASIO continued to engage closely with Australian government and private sectors to better develop understanding of the actual and potential targeting of Australian officials and interests overseas.

ASIO further provided advice on the risk of overseas travel to certain locations to government and industry sectors that could attract targeting by foreign intelligence services and to high-level senior stakeholders.

ASIO engaged with the broader Australian Government and relevant industry, at executive levels and with security advisers, to raise awareness of the threat of malicious insiders and foreign intelligence services. ASIO's annual stakeholder survey underscored the value stakeholders place in these outreach efforts with briefings viewed as professional, timely, and tailored to the needs of the particular audience. Stakeholders also expressed a growing appetite for increased ASIO input into their security awareness programs and responses to insider and cyber threats.

Countering serious threats to Australia's border integrity

Intended results

- Identify activities that represent a serious threat to Australia's border integrity.
- Advice is used to assist Australia's agencies effectively manage and/or disrupt activities that represent a serious threat to Australia's border integrity.

Effective identification of threats to Australia's security

Information sharing and watchlisting

National information-sharing and watchlisting arrangements continued to serve as an important pillar of national security arrangements. ASIO contributed extensively to watchlists managed by DIBP and the ABF, which helped identify persons of security concern, or potential security concern, who sought to travel to, or remain in, Australia.

ASIO also worked closely with border agencies to provide actionable intelligence on border security issues. This included providing intelligence reporting which informed agencies about the broader security environment, as well as advice on maritime and aviation security matters. Tailored reporting, assessments and travel intelligence helped inform decision-making at the border.

Adverse and qualified visa security assessments

ASIO undertakes visa security assessments using an intelligence-led, risk-managed approach. Visa security assessments are in response to DIBP requests or where ASIO identifies national security indicators. ASIO's advice informs DIBP decision-making about whether to grant, refuse, or cancel a visa. We will furnish an adverse assessment to DIBP where an individual is assessed to be a direct or indirect threat to security. Qualified assessments are given in cases where we cannot make a prejudicial recommendation but need to communicate information to DIBP that is relevant to security. Most adverse and qualified visa security assessments completed during 2015–16 were furnished on the basis of concerns about politically motivated violence, mainly terrorism. A smaller number were furnished on the basis of espionage and foreign interference concerns.

Countering people smuggling

ASIO undertook onshore collection and disruption activities in conjunction with OSB partner agencies, which led to the identification of individuals involved in maritime people-smuggling networks. Additionally, ASIO conducted security assessments for visa applicants with possible links to people-smuggling activities.

Effective advice, reporting and services that assist the Australian Government to manage security risks and disrupt activities that threaten Australia's security

Management of serious security risks—people-smuggling

ASIO is an active partner in OSB and continued to contribute to whole-of-government people-smuggling disruption and deterrence activities. ASIO also provided advice to the Australian Government on the people-smuggling threat and its impact on border integrity.

Supporting delivery of the migration program

ASIO provided visa security assessments to DIBP in line with national security considerations and DIBP's migration program priorities. ASIO met targets agreed with DIBP to achieve their annual and program priorities. These included visa security assessments of the priority Iraqi/Syrian refugee caseload, in conjunction with the legacy caseload of illegal maritime arrivals.

Security screening travellers

ASIO furnished 11 962 visa security assessments (see Table 3). A major revision of ASIO's visa security assessment model carried out in 2014–15 contributed to a reduction in visa referrals in 2015–16, and enabled us to focus resources on more complex and higher risk cases.

Type of entry	Number of assessments completed 2015–16[10]
Temporary visas	3515
Permanent residence and citizenship	985
Onshore protection (air)	75
Offshore refugee / humanitarian	1772
Illegal Maritime Arrivals	864
Other referred visa caseloads	4751
TOTAL	**11 962**

Table 3: ASIO visa security assessments by type

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

Security assessments for access to security-controlled places and substances

ASIO completed 9115 security assessments for access to security-controlled places or substances, excluding border-related security access assessments. These comprised security assessments for:

- access to security-sensitive ammonium nitrates (SSANs), which are used as an explosive and as a fertiliser. States and territories have their own licensing arrangements for access to SSANs, consistent with principles agreed by the Council of Australian Governments in 2005;
- access to security-sensitive biological agents (SSBAs) provided to the Department of Health as part of the SSBA Regulatory Scheme under the *National Health Security Act 2007*;
- access to the Australian Nuclear Science and Technology Organisation nuclear facility at Lucas Heights; and
- special events, such as designated sporting events or international forums.

Security access assessments

ASIO undertakes security assessments on access to security-controlled places, including assessing whether an individual requiring access to security-controlled areas at airports and ports presents a threat to security. AusCheck (within AGD) coordinates other checking and determines overall suitability for granting an Aviation Security Identification Card (ASIC) or Maritime Security Identification Card (MSIC). ASIO completed 141 820 border-related security assessments with almost all of these related to granting an ASIC or MSIC.

ASIO reduced the number of complex security access cases awaiting finalisation during 2015–16 through a functional restructure to better match resourcing to the caseload and refined intelligence-led prioritisation. ASIO also engaged with the Office of Transport Security to develop procedures for handling qualified security assessments.

Security advice informing whole-of-government policy, disruption and prosecutions

ASIO engages closely with DIBP, ABF and law enforcement agencies on border security and national security issues that may arise at the border. This cooperation extends from intelligence support to agencies to help them carry out their functions at the border, through to engagement on the development of policy and strategic assessments on border security matters. In 2015–16, ASIO contributed to inter-agency cooperation on policy issues, particularly on information-sharing and watchlisting. ASIO provided intelligence to inform counter-terrorism disruption activities at the border. ASIO also continued to provide training and briefings to border agency staff on national security issues to inform visa security assessment arrangements and to enhance effective cooperation on national security issues.

Providing protective security advice to government and business

Intended results

- Government, business, and industry adopt security by design to protect Australia's people, assets, and other national interests.
- There is increased protective security awareness and capacity across Australian Government agencies, business, and industry.

Effective protective security advice, reporting and services that inform security by design by government, business, and industry

T4 protective security advice and services

ASIO provides protective security advice for government and industry to enhance physical, technical, procedural, personnel and information security. The advice, provided by ASIO's T4 protective security directorate (T4), includes security risk reviews and vulnerability assessments, physical security certifications, technical surveillance countermeasures, equipment testing, and evaluation, and training/advisory services. More information and email contact details for T4 are available online at www.asio.gov.au/asio-t4-protective-security-asio-t4.html.

Zone 5 certification

One of T4's primary work programs is the physical security certification of facilities to Zone 5 standards. Zone 5 facilities are those where the compromise, loss of integrity or unavailability of information would have a catastrophic impact on business. These facilities require certification every five years and range in complexity. This work program is supplemented by other T4 functions, such as equipment approvals and technical surveillance countermeasures inspections. T4 met all Zone 5 certification responsibilities during 2015–16.

Security reviews

T4 conducted a number of security reviews for the Australian Government, state government agencies and corporations (see Figure 1). The reviews provided advice and recommendations on how to mitigate threats from terrorism, foreign intelligence services and malicious insiders.

Figure 1: Imagery taken in support of a protective security risk review for Airservices Australia

Security working groups

T4 provided subject matter expertise to a number of security working groups in Australian Government and state government agencies that are undertaking significant security infrastructure projects.

Security product evaluation program

The Security Construction and Equipment Committee (SCEC) is a standing inter-departmental committee responsile for the evaluation of security equipment for use by Australian Government departments and agencies. Further information on SCEC is available online from www.scec.gov.au. T4 manages the security product evaluation program on behalf of SCEC to evaluate the effectiveness of physical security products. Over the period, T4 engaged more proactively with commercial providers of security products to achieve more effective outcomes for government. Through greater engagement and openness with industry, T4 has increased the quality of security products and made the evaluation process easier for providers.

Case study: Educating security personnel

Due to the ever-increasing demand for T4 services, this year it initiated a communications program to provide pre-emptive support to Agency Security Advisors (ASAs) across government. In the heightened threat environment, the program seeks to identify and take advantage of opportunities to increase, broaden and consolidate the understanding of protective security issues. It also aims to reduce the high demand for individual, nuanced requests from security practitioners by enhancing awareness and self-reliance. Highlights from this program include the following:

- a new 'Security Zones' course for personnel responsible for constructing and managing property in accordance with the PSPF. The course increased the confidence and awareness of government security practitioners in the practical application of the PSPF.
- T4 also produced comprehensive guides and circulars on contemporary security issues, including selecting security systems and hardware, developing and reviewing security plans, and detecting and responding to hostile reconnaissance and rehearsals. The guides were released on Govdex, the Australian Government's online security collaboration tool, to ASAs and on the BLU website for a wider readership across government. They have ranked amongst the most popular BLU documents during the reporting year.

T4 seeks to build upon these successes in the next reporting period with a focus on providing government and industry with resources for operating in an increasingly complex security environment.

T4 protective security outcomes in summary

During the year, T4 provided protective security advice and services to its clients through the outputs shown in Table 4.

Advice/Service	2015–16	
Protective security reports	4 protective security reports	24 Zone 5 site certifications
Physical security certification program	50 site inspections 3 destruction service approvals	8 lead agency gateway facility certifications
Technical surveillance countermeasures	ASIO does not comment publicly on the details of this work program	
Security services and equipment evaluation	105 security equipment evaluations	6 courier evaluations, including 3 endorsements
Communication program	2 protective security training courses	1 technical note
	2 SCEC-approved locksmith briefings	5 protective security circulars
	2 safe maintainer courses	3 protective security guides for industry and government
	1 security equipment guide	

Table 4: T4 protective security advice and services for 2015–16

Personnel security assessments

ASIO is responsible for providing security assessments for Australian government personnel seeking security clearances for new or ongoing access to nationally classified, sensitive and privileged government information and areas. This is a critical frontline defence against the malicious insider threat and potential compromise by foreign intelligence services, and helps protect the integrity of government business.

ASIO continuously reviews and reforms security assessment processes to identify refinements and efficiency gains wherever possible. Partner agencies processes are also reviewed as part of this program. In doing so, ASIO seeks to enhance the quality of security outcomes to government in a heightened foreign intelligence services threat environment. A focus continued to be on ensuring the requirements of the PSPF were closely adhered to, that resources were focused on areas of greatest risk and potential harm, and that best practice was employed for checking security clearance applicants.

Type of Access	2014–15	2015–16
Positive vetting	428	1 329
Negative vetting level 2	6 619	8 943
Negative vetting level 1	16 020	20 759
Other	6	35
Total	**23 073**	**31 066**

Table 5: Number and type of national security clearance assessments completed

AGD is leading the Personnel Security Strategic Reform Taskforce to mitigate the malicious insider threat to the Australian Government's business through effective, efficient, and risk-based security vetting. ASIO is contributing to the Taskforce through bringing its experience, and that of international partners, in conducting investigations and personnel security assessments to inform the strategic reforms being pursued.

National security implications of foreign investment

ASIO advises Treasury on the national security implications of foreign investment proposals on a case-by-case basis and assesses the potential threat of espionage, foreign investment and sabotage from the investment. Consultation with Treasury ensures mitigations are in place, where possible, to address the threat from foreign intelligence services through investment.

- ASIO provided security intelligence advice on 285 foreign investment proposals to the FIRB, referred from Treasury. This was a marked increase on the previous year.
- In a number of cases over the reporting period, we advised on the use of management and operational controls to be applied to the structure of various foreign investment proposals to mitigate or reduce the national security risk.
- This has strengthened wider government understanding and decision-making about the threats to Australia's national security from foreign investment, especially in the critical infrastructure sectors.

ASIO works closely with a range of Australian Government agencies on foreign investment issues, in particular with the Department of Defence and AGD in ensuring a consistent approach to assessments relating to national security.

Continued development of our strategic analytical capability of national security implications arising from foreign investment across particular industries and sectors was a key focus during the reporting period.

Business and government liaison

ASIO's Business Liaison Unit (BLU) provides an interface between the Australian Intelligence Community (AIC) and the private sector. The BLU hosts a secure website which has 3612 subscribers and where intelligence-backed, declassified reports are published. In the reporting period, 64 ASIO reports, 75 foreign government agency reports, and three Australian government agency reports were published on the website. The BLU website was upgraded to improve user experience and search functionality in June 2016.

The BLU hosted five classified briefing days for high-threat sectors (such as aviation, communication and places of mass gathering), provided hundreds of tailored briefings to corporate security managers, and facilitated dozens of executive-level briefings. The detailed, sector-specific information provided by the BLU to the private sector ensures owners and operators of critical infrastructure, and other high threat sectors, have the necessary security information regardless of their clearance level.

ASIO's cyber outreach activities were coordinated through its membership of the multi-agency ACSC. The ACSC comprises elements of Australian Signals Directorate (ASD), Defence Intelligence Organisation (DIO), Computer Emergency Response Team Australia (CERT Australia), the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC) and ASIO. The ACSC is a hub for collaboration and information sharing with the private sector, state and territory governments, academia and international partners to combat the full range of cyber threats. More information on the ACSC is available at www.acsc.gov.au.

ASIO continued to provide advice to Australia's telecommunications industry on the national security threats to the sector and worked closely with key partners to mitigate risks of unauthorised access or interference to their networks and data holdings. Services provided by the telecommunications industry are critical to Australia's national security, growth and prosperity. Our advice helped the industry consider and mitigate risks to the availability, integrity and security of these services. This advice complemented, and was enriched by, the best-practice information assurance principles and policies developed within the ACSC for broader industry and government engagement on cyber security issues.

Increased government outreach continued during the reporting period. Some 1684 Australian government subscribers accessed ASIO reporting through the BLU website. Expanded liaison supported major international events, including regular briefings to inter-departmental committees, security working groups and organising committees of major international events.

ASIO provided protective security advice in the lead-up to, and during, major international events to support the Australian Government's broader security responses leveraging our international partnerships and threat assessment capability. ASIO's activities helped build resilience and raise awareness by broadening the understanding of threats faced by the Australian community. Events we supported included World War One Centenary commemoration services in Turkey, France and Belgium, the Olympic Games, the Asia-Pacific Economic Cooperation forum, the Commonwealth Heads of Government Meeting, and the Group of Twenty (G20) forum.

Collecting foreign intelligence in Australia

Intended results

- Provide niche foreign intelligence collection services to partners, in accordance with National Intelligence Priorities.

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.

Foreign intelligence is intelligence relating to the capabilities, intentions and/or activities of people or organisations outside Australia. It can encompass political, economic and diplomatic matters, as well as matters relevant to security. Our responsibility to collect foreign intelligence is complemented and supported by other agencies.

ASIO continued to provide a valuable contribution to the ongoing foreign intelligence effort by generating advice of unique intelligence value that enhanced Australia's national security.

Measures across all activities

The security of ASIO's activities

The direct threat to ASIO and law enforcement agencies has increased since the beginning of 2015. ASIO has also been the subject of terrorist intent. Accordingly, we have diverted resources to further build layered security and safety measures. These include:

- developing and operating new staff-tracking and duress alert technologies to support employees working operationally;
- introducing a suite of enhanced personal safety and security training to equip employees to operate in a more hostile environment; and
- introducing a range of enhanced security measures for ASIO premises, including overt physical security measures and the patrolling of our headquarters by armed AFP officers.

Personal safety and security training courses were delivered frequently through the year and across Australia. In addition, elements of these courses were extended to close partner agencies that operate in a similar environment and have similar staff development requirements. Elements have also been adopted by close partner agencies to enhance their own internal programs and the safety and security of their staff.

5

CORPORATE MANAGEMENT

Corporate strategy and governance

Strategic planning

ASIO released its first corporate plan under the PGPA Act in July 2015. The plan relates our purpose to our activities, delivery strategy, intended results, and new performance measures. We continued to refine our corporate planning approach during the reporting period. Our current corporate plan is available from www.asio.gov.au.

ASIO has strategic plans for its activities in countering terrorism, espionage, foreign interference and malicious insiders.

During the reporting period, work commenced on the ASIO2020 program which will address the most serious challenges to our future success. This work continued into the next reporting period and will feature in the 2016–17 annual report.

Governance committees

The Director-General of Security is the accountable authority for ASIO under the PGPA Act. Our corporate governance committees support the Director-General in fulfilling his PGPA Act responsibilities.

ASIO Executive Board

The Executive Board is the peak advisory committee to the Director-General. The Executive Board comprises the Director-General, the Deputy Directors-General and an external member.

The Executive Board meets monthly. The board sets overall strategic direction, oversees resource management and is the principal forum for managing strategic corporate priorities and resource matters.

Over the reporting period, the board received regular reporting from ASIO's committees on corporate outcomes and issues including, key security developments, budget, capability development, risk management and importantly our progress toward our diversity goals.

Intelligence Coordination Committee

The Intelligence Coordination Committee plays a key role in fulfilling ASIO's responsibilities in accordance with the PGPA Act, through the management of ASIO's security intelligence program. The committee provides strategic direction, manages risk, coordinates effort and evaluates performance. During the period, the committee was chaired by Deputy Director-General Counter-Terrorism.

The committee's work program comprised three of the activities ASIO pursues to achieve its purpose and a fourth element focused on ASIO's specialised intelligence capability requirements:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders;
- countering serious threats to Australia's border integrity; and
- enhancing security intelligence capabilities.

Over the reporting period, the committee increased its guidance and oversight of ASIO's Investment Program to better align the organisation's development of new and enhanced intelligence capabilities with acute and enduring strategic and operational risks. The committee also established a new security intelligence capabilities sub-program to ensure the organisation's operating paradigm and ICT systems keep pace with the evolving threat and technological environment.

Workforce Capability Committee

The Workforce Capability Committee considers issues concerning ASIO's workforce to ensure it is sufficiently sized, skilled, equipped and accommodated to meet the current and future capability needs of the organisation. During the period, the committee was chaired by Deputy Director-General Strategy. The Work Health and Safety Committee is a subcommittee responsible for ensuring better health and safety policies and practices across ASIO. (See also 'Work health and safety').

Over the reporting period, the committee oversaw the initiation of the 10th Workplace Agreement, the ASIO Gender Equity Strategy, the progress of recruitment to build ASIO's counter-terrorism capacity and a range of broader workforce issues.

Security Committee

The Security Committee reports directly to the Executive Board providing assurance of sound and secure practices in ASIO. It considers the evolving security environment, and reviews and addresses key issues relevant to the security of 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. During the period, the committee was chaired by Deputy Director-General Strategy.

Finance Committee

The Finance Committee provides advice and makes recommendations to the Executive Board on resource allocation and financial management and strategy. Resources include human capital, accommodation and assets. During the period, the committee was chaired by Deputy Director-General Counter-Espionage and Interference and Capabilities.

Audit and Risk Committee

The role of the ASIO Audit and Risk Committee is to provide independent assurance and advice to the Director-General and the Executive Board on the design, operation and performance of ASIO's internal governance, risk and control framework and compliance with its internal and external accountabilities and responsibilities. The committee is responsible for reviewing and advising on:

- risk management;
- internal audit and assurance;
- external audit and review;
- internal control;
- financial statements;
- legislative and policy compliance; and
- performance reporting.

Committee members, including the chair, are appointed for an initial period of no more than three years. Over the reporting period, three ASIO officers and five external members served as committee members. The committee currently comprises three ASIO officers and three external members. The committee is chaired by Mr Geoff Knuckey, an external member.

Over the reporting period, the committee met its responsibilities under its charter and assessed ASIO's 2014–15 financial performance as sound. Key activities included: overseeing the implementation of the Integrated Assurance Model; establishing an Assurance Group, bringing together several internal assurance, performance and accountability capabilities; and commissioning a refreshed Fraud Risk Assessment, whose findings informed the development of the ASIO Fraud Control Framework 2016–18.

ASIO Consultative Council

The ASIO Consultative Council, Chaired by ASIO's First Assistant Director-General Corporate and Security, enables ASIO management and employees to meet in a regular and structured way to discuss and resolve issues. Two representatives from ASIO's Staff Association and two representatives from ASIO's management group constitute a quorum for the monthly meeting.

This year the council focused on:

- progress of the 10th Workplace Agreement negotiation process, and the consequent amendments to ASIO's Consolidated Determination, human resource delegations, and policies;
- clarifying the terms and conditions of the Surveillance job family; and
- contributing to a review of ASIO's performance management framework.

Into the next period, the Council will continue to consider the proposed introduction of pre-employment and general employment medical standards and the concept of an ASIO career hub.

People

Workforce management and reporting

At the end of 2015–16, ASIO employed 1753.4 full-time equivalent (FTE) staff, an increase of just over 2 per cent from 2014–15. ASIO's separation rate at 30 June 2016 was 4.44 per cent.

ASIO's priority was to increase staffing levels in accordance with the '*National Security—additional counter-terrorism*' funding measure announced in August 2014, with funding received through the 2014–15 additional estimates process in February 2015. The growth in FTE has been, and will continue to be, in our intelligence, technical, information and communication technology areas. There was also some emphasis on building corporate capabilities, such as vetting and recruitment.

The Organisational Capability Program is a mechanism for deploying ASIO staff across the organisation to distribute resourcing to critical positions. As this program continues to grow, it will provide staff with access to opportunities that align with their own development and also provide ASIO with the ability to deploy staff as priorities dictate.

Since 1994, non-corporate Commonwealth entities have reported on their performance as policy adviser, purchaser, employer, regulator and provider under the Commonwealth Disability Strategy. In 2007–08, reporting on the employer role was transferred to the Australian Public Service Commission's State of the Service reports and the *APS Statistical Bulletin*. These reports are available at www.apsc.gov.au. From 2010–11, entities have no longer been required to report on these functions.

The Commonwealth Disability Strategy has been overtaken by the National Disability Strategy 2010–2020, which sets out a 10-year national policy framework to improve the lives of people with disability, promote participation and create a more inclusive society. A high-level, two-yearly report will track progress against each of the six outcome areas of the strategy and present a picture of how people with disability are faring. The first of these progress reports was published in 2014, and can be found at www.dss.gov.au.

Recruitment

Recruitment efforts focused on the difficult-to-fill roles of surveillance officers, intelligence officers, technical officers and information and communications technology (ICT) positions.

Two significant recruitment changes were made during the reporting period:

- the continuous acceptance of applications for intelligence officers (rather than only twice a year); and
- the introduction of an intelligence analyst development program stream.

The recruitment campaign for surveillance officers included a targeted media campaign to attract candidates with a trade background. This popular campaign attracted several thousand applications.

ASIO continued to use the recruitment agency panel established in 2014–15 to broaden our capability and capacity. This included providing administrative support for large recruitment campaigns, such as the surveillance campaign outlined above.

University graduates are one of the target audiences for intelligence officer, junior technical and ICT roles with ASIO. Market research provided insight into graduate employment preferences and feedback on our recruitment marketing material. Recruitment brochures, relevant documentation and website content were reviewed and updated in line with the research findings. The research will inform our recruitment activity in 2016–17. ASIO also attended nine career fairs and held targeted information sessions for particular disciplines at a number of universities to promote employment opportunities and the organisation, and to allow students to ask detailed questions.

Our expenditure on recruitment advertising for difficult-to-fill roles and career fair attendance decreased from $871 902 in 2014–15 to $791 016 in 2015–16. This reduction was achieved by refining our recruitment advertising and prioritising our attendance at career fairs.

Over 6500 applications were submitted to ASIO's online employment register during the year. The register allows those interested in ongoing opportunities to lodge their interest. Candidates were sourced from the register for a variety of vacancies. In particular it has been a valuable means to identifying people interested in technical and ICT roles. The register was refined to attract more candidates with the skill sets in highest demand and it will be reviewed further in 2016–17. The register can be accessed from www.asio.gov.au/careers.html.

Diversity agenda

ASIO continued its commitment to gender equity, diversity and inclusion in 2015–16. A Gender Equity Strategy was developed and implemented, with release on 8 March 2016 to mark International Women's Day. Our Gender Equity Reference Group, established in 2015, was critical to informing an action plan and ensuring staff engagement. A dedicated senior officer was appointed to lead the implementation of the strategy and to scope a broader diversity and inclusion program.

ASIO staff also heard from leaders on the topic of gender equity. In March 2016, Ms Lucy Turnbull AO addressed staff. In April 2016, ASIO staff attended an Australian Intelligence Community diversity event and heard Dr Martin Parkinson PSM, Secretary of the Department of the Prime Minister and Cabinet, and Ms Elizabeth Broderick AO, former Sex Discrimination Commissioner, speak about their experiences in addressing gender inequality.

Women comprise 45% of ASIO's workforce. ASIO has made progress in improving the statistics of women in the senior executive, particularly at the SES Band 1 level where there is now around a 45 per cent representation. However there is still more work to do, particularly at the executive levels. In the next period, and through to 2020, the diversity agenda will focus on a series of goals to achieve gender equity across all levels.

Human resource programs

ASIO completed a review of all aspects of its Performance Management Framework. This review was designed to ensure ASIO continued to support and drive a high-performing culture, with a focus on further developing employee and organisational capability and gaining efficiencies in people management. Where possible, principles of the Australian Public Service Commissioner Directions 2013, Chapter 4 'Performance Management' were adopted, placing a greater level of accountability on employees, line managers and senior management to support and drive a performance-based culture. The outcomes of the review resulted in the:

- introduction of a standard annual salary advancement date for all employees, with stronger links to performance outcomes;
- development of further training for line managers in managing unsatisfactory performance or behaviour; and
- development of a broad suite of policy and process documents to support all areas of the performance management cycle.

Workplace agreement

ASIO concluded the negotiation processes and voting for its 10th Workplace Agreement. ASIO is required by the ASIO Act to adopt the employment principles of the Australian Public Service (APS) to the extent they are consistent with the effective performance of the organisation. All negotiation processes aligned with, where possible, the broader Australian Government Employment Bargaining Framework.

ASIO was bound by similar budgetary and time constraints as those of APS agencies and was required to demonstrate increased productivity and performance outcomes to offset any employee salary increases.

The proposed agreement was voted on by 71 per cent of ASIO employees, and 82 per cent of voters accepted the proposed agreement. The agreement took effect from 10 March 2016 for three years.

Changes to terms and conditions under the workplace agreement related to certain leave types, part-time employment arrangements and redundancy provisions. These changes allowed ASIO to:

- streamline the administration of these provisions;
- apply further consistency to their application across ASIO; and
- create greater alignment and consistency with APS provisions and National Employment Standards.

ASIO Ombudsman

The ASIO Ombudsman is an external service provider who acts to resolve staff issues or concerns impartially and informally, through advice, consultation and mediation. The Ombudsman continued to meet regularly with ASIO senior management and with representatives of the Staff Association to discuss the health of the workplace.

The Ombudsman continued to provide valuable support and advice to employees and line managers during the reporting period. During the year, the Ombudsman:

- provided advice and guidance in response to 20 informal contacts from staff;

- provided formal advice based on investigations into eight matters. Four investigations were relevant to the Code of Conduct, two were related to organisational restructures and conditions, and two were independent reviews of management actions;
- provided assistance to an inquiry from the IGIS related to a previous employee; and
- undertook formal consideration of conditions-of-service matters and provided advice to staff and management.

The Ombudsman also actively promoted the role of the Ombudsman and the importance of the ASIO Values and Code of Conduct in establishing a proper and respectful workplace culture, in a wide range of presentations, branch meetings, induction programs and management training sessions.The Ombudsman was also directly involved with the Harassment and Discrimination Network.

In 2015–16, the ASIO Ombudsman did not participate in any work related to public interest disclosures.

Work health and safety

ASIO's Health and Safety Representative network continues to engage with and to inform work teams on the importance of maintaining a safe workplace. In response to injury or incident, our first aid officers also provide an integral service to the workforce.

Our health and wellbeing program 'HealthINT' was refocused during the reporting period. A new primary provider for the program was engaged to ensure initiatives are targeted and build awareness of the benefits of maintaining a healthy lifestyle. The program will continue throughout the year and will seek to deliver initiatives that are innovative and cost effective. In March 2016, the annual influenza vaccination program was offered to all employees who could either attend an in-house appointment or be reimbursed for vaccination cost.

The Work Health and Safety Committee meets quarterly to discuss current issues and to endorse work health and safety policy and procedures. Attended by employee representatives, management representatives and Health and Safety Representatives, the committee has an important role in ensuring a safe working environment.

Safety risk awareness drives our involvement in a number of training programs and ensures the safety and wellbeing of employees remains a key requirement in all ASIO functions. These programs and initiatives continue to highlight work health and safety risk as an important strategic issue for the organisation. Individuals are encouraged to build an awareness of, and to improve, their personal health and wellbeing. An ongoing priority will be to focus on safety risk management processes and engage across the organisation to further support our strategic safety agenda. The safety, engagement and overall resilience of ASIO's workforce is improved by these initiatives.

Awareness of the importance of reporting work health and safety incidents will continue to be raised with work teams and managers. Systems and reporting thresholds may need to be clarified to ensure data is accurate and effective.

The total number of injuries, incidents and near misses reported in 2015–16 did not notably change.

- Four incidents were reported to Comcare in line with legislated notification obligations. One serious injury and three dangerous incidents were reported; however, Comcare recorded only three of these as notifiable incidents.
- Comcare did not initiate any investigations into the notifiable incidents, nor were any notices issued to ASIO under the *Work Health and Safety Act 2011*.

ASIO continued its active early intervention and preventative approach in compensation and rehabilitation—for both compensable and non-compensable staffing matters. This approach is reflected in the reduction of the compensation premium paid and the outcomes of rehabilitation audits.
The rehabilitation audit examined ASIO's Rehabilitation Management System, processes and outcomes and validated ASIO's compliance with the *Safety Rehabilitation and Compensation Act 1988* and *Guidelines for Rehabilitation Authorities 2012*. No areas of non-compliance were identified. ASIO continues to enhance processes and maintains an active and positive relationship with the regulator Comcare in both work health and safety, and rehabilitation.

ASIO's Work Health and Safety Policy is available online from www.asio.gov.au/work-health-and-safety-policy.html.

Public Interest Disclosure Act

ASIO is committed to the highest standards of ethical and accountable conduct and support for staff members who make a public interest disclosure in accordance with the *Public Interest Disclosure Act 2013* (PID Act). For intelligence agencies, the PID Act works in conjunction with other legislation to protect intelligence information, and provides specific avenues for individuals to make a public interest disclosure involving intelligence information. The ASIO Act, the *Inspector-General of Intelligence and Security Act 1986*, the *Intelligence Services Act 2001* and the *Crimes Act 1914* are examples of pieces of legislation which complement the PID Act.

ASIO meets its responsibilities under the PID Act. ASIO has trained authorised PID officers, a PID briefing is provided to all new starters and all staff are required to complete a mandatory PID eLearning package. Some further information is available on our website at www.asio.gov.au/p-i-d-act.html.

ASIO provides annual reporting to the Office of the IGIS relating to any public interest disclosures received, in accordance with the legislative requirements. This, in turn, is included in the IGIS annual report and mandatory reporting to the Commonwealth Ombudsman from the IGIS, on behalf of the AIC.

Social club and support for the community

ASIO's social club is run by a group of volunteers who arrange social and community events for ASIO staff. These include trivia nights, charity fundraisers and special events. The charities supported by the social club include the Cancer Council ACT through participating in Australia's Biggest Morning Tea and Daffodil Day. The social club has supported Daffodil Day since 2005 and held a Biggest Morning Tea each year since 2006. The support of ASIO's staff for the Cancer Council has grown over time, and, following the Biggest Morning Tea in May 2016, ASIO was recognised as one of the top five fundraisers in the Australian Capital Territory (ACT). The funds raised for the Cancer Council go towards cancer research, prevention, and support services.

Training

ASIO continued to drive forward training and capability development in line with the principles of a learning organisation and the 70:20:10 principle. The principles of a learning organisation include creating, acquiring and transferring knowledge, and synthesising new knowledge and insights. The 70:20:10 principle advocates that, of all employee learning:

- 70 per cent should be acquired by on-the-job experience;
- 20 per cent should be acquired by informal learning; and
- 10 per cent should be acquired by formal learning.

This approach aligns with the outcomes of the ASIO training review commissioned by the Director-General in 2014–15.

ASIO's continued investment in this area has seen new programs developed in line with the changes in our operating, security and technical environments. Training delivery models were broadened and diversified so that staff can access training opportunities via different mediums. This ensures staff can continue to develop their skills and capabilities despite the high operational tempo.

During the reporting period, ASIO continued our focus on enhancing relationships with close national and international partners to deliver mutual training benefits and ensure best practice through benchmarking. These partnerships have enabled the sharing of training opportunities, facilities, instructors and standards.

Intelligence training

ASIO continued to expand its graduate development programs, through which it recruits, develops and produces 'job ready' officers with the necessary intelligence discipline skills. The programs are the:

- Intelligence Officer Development Program (IODP);
- Technical Graduate Program (TGP); and
- Intelligence Analyst Development Program (IADP).

These programs reflect the focus on attracting and developing a high-quality and skilled workforce for the future.

The IODP trains and develops new intelligence officers in analytical and operational tradecraft. The program incorporates classroom-based learning and practical exercises, integrated mentoring and short-term placements in the workplace to solidify learning outcomes. Two IODPs were completed in the reporting period.

The new TGP is being run on an annual basis since the success of the first iteration in 2014–15. The TGP includes specialist training, integrated mentoring, and placements in a range of technical areas within ASIO's Technical Capabilities Division, including in software development, technical development, telecommunications, computer forensics and technical operations.

In recognition of the importance of our analytical and assessment function, a new IADP commenced in June 2016. The IADP includes classroom-based learning and practical exercises, new specialist analytical training, integrated mentoring, and a range of short-term placements across ASIO's analytical and assessment areas.

ASIO continued to focus on developing advanced and specialised intelligence training courses during this reporting period. This included investing in refresher training for perishable skills and developing and delivering new programs to further develop or refine advanced skill sets. New programs included tailored leadership training for each intelligence discipline, which complement broader management and leadership programs (see 'Management and leadership').

Core capability development

ASIO continued to deliver a wide range of high-quality core-capability development opportunities to meet the diverse business needs of our workforce. Programs were delivered both in-house and by external training providers.

Each program is regularly reviewed, evaluated and where necessary updated to ensure best practice in adult learning. Most recently, our remodelled new starter induction program was shared with close partners due to its innovative delivery format and comprehensive course content.

Rob Goffee Award for Leadership Development—Australian Human Resources Institute

The annual Australian Human Resources Institute (AHRI) awards celebrate the best ideas, programs and individual achievements in the human resources profession across Australia.

AHRI awarded the Rob Goffee Award for Leadership Development to ASIO in December 2015. This award recognises outstanding leadership development initiatives, programs and strategies, implemented to develop and encourage current and future leaders.

Our submission for the award was premised on the success of our Management and Leadership in Security Intelligence Strategy (2013–16) and our delivery of associated training and development programs across the ASIO workforce. Overwhelmingly positive participant feedback from these programs provided the statistical basis for our submission.

In particular, the award recognised that 'In a strong field, the ASIO initiative is distinguished by its ambitious scope, and deep connection with the cultural and strategic context. Its innovative, integrated and long term approach show how skilful leadership development can really make a difference'.

Factors critical to the success of the strategy were:

- a commitment by, and engagement of, senior leaders at all stages via inclusive design and delivery approaches;
- a targeted and integrated approach to engender cultural change via strategically aligned individual development;
- the placing of learners' experiences and real ASIO issues at the core of innovative learning processes; and
- a focus on ongoing workplace application for cultural evolution, with sustained individual learning and performance over time.

An area of significant focus over the reporting period was building on existing online training, known as the eLearning Academy, to design and deliver training courses for the our workforce. To ensure alignment with workforce requirements, the new program was developed with input from a working group representing relevant ASIO divisions. All staff members now have access to a diversity of training opportunities, including more advanced or specialised modules based on specific role requirements.

The eLearning Academy continued to deliver mandatory competency-based training on a range of subject areas, such as work health and safety, workplace behaviour, ethics and accountability, environmental management and the public interest disclosure scheme. New modules were developed and added to the existing catalogue, including some in support of our safety and security training program. Of note, two additional information technology modules related to core systems training were added to further support the accreditation of staff.

We recorded 2498 mandatory and 1760 non-mandatory eLearning Academy course completions. This figure is in addition to 4728 instances of face-to-face training, attended by 1643 employees across 120 training courses.

Management and leadership

ASIO continued to deliver management and leadership development opportunities in line with our overarching Management and Leadership in Security Intelligence Strategy (2013–16). Notably, this strategy, and our associated development programs, was awarded the 2015 Rob Goffee Award for Leadership Development by the Australian Human Resources Institute (see previous page).

In addition to our well-developed pathway programs—the Management Skills in ASIO program, the Introduction to Management Program and the Mastering Management Program—our management and leadership program now includes a range of alumni and leadership networking events. These opportunities build on the investment made in our formal management and leadership programs over recent years and serve to enhance our relationships and strategic alignment with close partners.

Investment in the development of our Senior Executive Service (SES) also continued, including through:

- external mentoring partnerships;
- internal leadership-themed events, including a leadership speakers program—launched by the Governor-General, His Excellency General the Honourable Peter Cosgrove AK MC (Retd), and with speakers including Dr Martin Parkinson PSM, Secretary of the Department of the Prime Minister and Cabinet; and
- targeted individual development opportunities, including secondments and/or formal development programs delivered internally or by academic institutions.

This investment, in which every ASIO SES officer has been involved, represents our commitment to develop and maintain a diverse pool of leadership talent capable of leading the organisation to meet future challenges.

A new Management and Leadership in Security Intelligence Strategy will be developed for the 2017–20 period, to align with key strategic objectives including the ASIO 2020 program and our gender diversity goals.

Study support and language development programs

Over 10 per cent of ASIO staff received support to undertake study or language development during 2015–16.

- A total of 117 officers participated in ASIO-supported study programs, at a cost of $301 635. These programs included 79 courses across a range of disciplines, including security and policy, conflict and strategic studies, business management, project management and information technology.
- Our Language Skills Development Program aims to build language capability, with employees encouraged to maintain language proficiency and to apply for opportunities where relevant to their role. ASIO spent $370 281 on language training for 69 employees across 21 languages.

A new internal language development program was also developed. This has been well received and has helped staff build language skills during their business day.

Property

Ben Chifley Building

Figure 2: The corporate foyer of the Ben Chifley Building

The BCB has been fully occupied since July 2015, housing staff from ASIO, the ACSC and the Australian Counter-Terrorism Centre. The building which previously housed ASIO's headquarters, located in the Russell Defence precinct, was returned to the Department of Finance in October 2015.

The corporate suites in BCB were designed to enhance and build our capability by providing a venue for training, engagement and partnership. This area includes the auditorium, which is the largest accredited facility of its type in Australia. Suites were used frequently by ASIO, the ACSC and AIC partners to host approximately 130 functions per month, ranging from small training groups to large industry forums and senior-level addresses.

In June 2016, the BCB won awards for Commercial Architecture and Interior Architecture at the ACT Chapter of the Australian Institute of Architecture Awards (Figure 2 shows one of the images used for that competition).

Environmental performance

ASIO continued its commitment to reduce its carbon footprint in 2015–16. Achievements and initiatives included:

- A reduction of 231 597 kilowatt hours in ASIO's total energy consumption through the use of solar panels, saving approximately $28 000 and 212 tonnes of carbon emissions.

- The production of 45 000 kilowatt hours of electricity produced by a gas-fired co-generator plant, reducing grid electricity cost by a further $5 440 and saving 41 tonnes in carbon emissions.
- Use of 18 646 kilolitres of captured stormwater for irrigation and toilet flushing, reducing reliance on bore water and saving approximately $97 100 of potable water.
- The recycling of 73 591 kg of waste, including paper products, printer toner cartridges, batteries, scrap metal and fluorescent light tubes.
- Increased efficiencies in the data centre through temperature adjustment and installation of blanking panels to reduce energy consumption and decrease maintenance requirements.
- Participation in the ninth consecutive Earth Hour event held on 26 March 2016.

Information and technology services

5

Contemporary communications networks and associated services are critical in promoting innovation and collaboration and to enable the achievement of business efficiencies. We continued our focus on delivering modern communications technologies to support our activities and purpose and the activities of other Australian national security agencies. We worked with partners to improve access to secure and ubiquitous voice, video and data services. ASIO has also implemented new services to streamline telephony and email services and is replacing legacy point-to-point systems with enterprise-ready approaches.

Financial services

Procurement and purchasing

Throughout 2015–16, ASIO adhered to the Commonwealth Procurement Rules and associated policy and guidelines. This involved exercising contemporary procurement advice and methodology to ensure that ASIO managed procurement effectively and delivered value for money. Compliance is monitored through our Audit and Risk and Finance Committees. No significant issues were identified and overall compliance was acceptable.

ASIO supports small business participation in the Commonwealth Government procurement market. Small- and medium-sized enterprise participation statistics are available on the Department of Finance's website at www.finance.gov.au/procurement/statistics-on-commonwealth-purchasing-contracts/.

Procurement practices to support small– and medium-sized enterprises include:

- standardising contract and approach-to-market templates which use clear and simple language;
- ensuring information is easily accessible through electronic advertisement of business opportunities and electronic submission for responses; and
- using electronic systems to facilitate the Department of Finance's 'Procurement On-Time Payment Policy for Small Businesses', including payment cards.

We recognise the importance of ensuring that small businesses are paid on time. The results of the survey of Australian government payment to small business are available on The Treasury's website www.treasury.gov.au.

Consultants

We entered into 22 new consultancy contracts involving total actual expenditure of $1.67 million (GST-inclusive). In addition, five ongoing consultancy contracts were active during the period, involving total actual expenditure of $0.20 million (GST-inclusive).

ASIO applies the Commonwealth Procurement Rules and the guidance and advice documentation provided by the Department of Finance when selecting and engaging consultants. We also follow an internal policy and associated procedures which provide guidance on identifying and determining the nature of a contract. This ensures appropriate methods for engagement and contracting are executed. We engage consultants when there is a need for professional, independent and expert advice or services which are not available from within the organisation.

Annual reports contain information about actual expenditure on contracts for consultancies. A list of consultancy contracts let to the value of $10 000 or more, 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. This is subject to authorised exemptions for the protection of national security. This list may also be made available to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), which has oversight of ASIO's administration and expenditure, on request. For national security reasons, ASIO is not required to publish information on the AusTender website.

Contracts

During the reporting period, ASIO did not enter into any contracts valued at $100 000 or more that did not provide for the Auditor-General to have access to the contractor's premises.

The Director-General has applied measures necessary to protect national security which exempt ASIO from publicly publishing details of contract arrangements, including standing offers, in accordance with clause 2.6 of the Commonwealth Procurement Rules.

Details of ASIO's agreements, contracts and standing offers are available on request to members of the PJCIS.

Advertising and market research spends

ASIO spent $792 031 on advertising in 2015–16, predominantly on recruitment campaigns. ASIO does not fall within the definition of agencies covered by the reporting requirements of s311A of the *Commonwealth Electoral Act 1918*.

Internal assurance

ASIO is committed to enhancing its fraud control and management arrangements so that they reflect best practice. In the reporting period, the fraud risk assessment was updated which informed a revised fraud control plan and guidelines. The ASIO Fraud Control Plan 2016–18 is available online from www.asio.gov.au. During this period, ASIO received no allegations of fraud.

Fraud awareness training for all new employees and contractors has been a feature of ASIO induction training for several years. The organisation also provides a mandatory training module on ethics and accountability, including fraud awareness, as part of its eLearning Academy.

The internal audit team completed compliance audits in line with legislated requirements and those imposed by Memorandums of Understanding. These audits found ASIO to be compliant with all requirements and indentified only administrative issues that were promptly addressed. Performance audits were completed on asset management and external database search processes. These audits found ASIO to be compliant and made recommendations to improve the efficiency and effectiveness of processes.

As part of ASIO's Integrated Assurance Model, a Baseline Assurance Map was compiled capturing all internal controls and assurance activities across ASIO's functions. This document has been used to set the assurance work program for 2016–17, which is closely aligned with, and supports, the ASIO2020 program.

During the year, we made considerable progress in reviewing and updating our suite of operational policies and procedures. The resulting product—the Intelligence Practice Manual—increases the accessibility of guidance to staff, aligns with the contemporary operating environment, as well as legal and compliance frameworks, and makes future updates of operational guidance easier.

External scrutiny

Ministerial accountability

ASIO's ministerial accountability is to the Attorney-General, Senator the Hon. George Brandis QC. We conduct our security intelligence activities in accordance with the Attorney-General's Guidelines, which are available online at www.asio.gov.au/attorney-generals-guidelines.html. The guidelines stipulate that ASIO's activities must be conducted in a lawful, timely and efficient manner, applying the principle 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 are currently being reviewed by AGD following a recommendation by the PJCIS.

The Attorney-General issues all warrants for ASIO to employ its special powers, 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 presents a warrant request to the Attorney-General. Each warrant request is independently reviewed by AGD before progressing to the Attorney-General. The Attorney-General considers the request and, if in agreement, issues the warrant. For every warrant issued, ASIO must report to the Attorney-General on the extent to which the warrant assisted ASIO in carrying out its functions.

ASIO 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 321 formal submissions. The Director-General also briefs other ministers on security issues and matters relevant to their portfolios, when required.

Engagement with parliament

Leader of the Opposition

The Director-General of Security is a statutory position, with a responsibility to provide impartial advice. The ASIO Act requires the Director-General to regularly brief the Leader of the Opposition on matters relating to security and to provide him or her with a copy of ASIO's classified annual report. From time to time, with the Attorney-General's knowledge, classified briefings on specific security cases have been provided for other shadow ministers. During 2015–16, the Director-General briefed the Leader of the Opposition on significant security matters when required.

Parliamentary Joint Committee on Intelligence and Security

ASIO is subject to scrutiny by the PJCIS on matters relating to administration and expenditure, and other matters that may be referred to it by the government or the parliament such as the review of ASIO's questioning and detention powers. The PJCIS also has a role in reviewing Australian Government proscription of terrorist organisations. In addition, the PJCIS examines amendments to national security legislation.

During 2015–16, ASIO made one submission to the committee as part of its Review of Administration and Expenditure No 14 (2014–15) Australian Intelligence Agencies. Representatives from ASIO attended a private hearing in February 2016.

In September 2015, ASIO representatives attended the public hearings on the review of the re-listing of Al-Shabaab, Hamas' Izz al-Din al-Qassam Brigades, Kurdistan Workers' Party (PKK), Lashkar-e-Tayyiba and Palestinian Islamic Jihad as terrorist organisations.

In August 2015, ASIO representatives attended the public hearings on the PJCIS *Advisory report on the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015*.

ASIO's evidence to the committee can be found on the relevant inquiry page on the committee's website http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security.

Senate Legal and Constitutional Affairs Committee

ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the senate estimates process on 9 February 2016 and 5 May 2016 (ASIO was released from appearing at the hearing on 15 October 2015). ASIO's evidence to the committee can be found in the estimates Hansard for the relevant days (go to www.aph.gov.au/Parliametary_Business/Senate_Estimates and navigate to the relevant hearing).

Inspector-General of Intelligence and Security

The Hon. Margaret Stone was appointed as Inspector-General of Intelligence and Security (IGIS) in August 2015. The role of the IGIS is to review the activities of the AIC and provide assurance that agencies operate with propriety, according to law, consistent with ministerial guidelines and directives, and with due regard for human rights. The IGIS has powers akin to a standing royal commission.

During 2015–16, the IGIS undertook a regular inspection program of activities across ASIO operational functions and investigated complaints received by her office. There were no formal inquiries or release of any reports of inquiries making findings in relation to ASIO. Details of the ongoing inspection work of the IGIS can be found in her annual report, available online from www.igis.gov.au.

Independent Reviewer of Adverse Security Assessments

The role of the Independent Reviewer is to conduct an independent advisory review of ASIO adverse security assessments furnished to the DIBP for persons who remain in immigration detention, having been found by the department to be owed protection obligations under international law and to be ineligible for a permanent protection visa, or who have had their permanent protection visa cancelled because they are the subject of an adverse security assessment.

The Reviewer conducts an initial primary review of each adverse security assessment and subsequent periodic reviews every 12 months for the duration of the adverse assessment.

ASIO also undertakes internal reviews of adverse security assessments of its own volition and, over time, those internal reviews have resulted in a number of adverse assessments being replaced with a qualified or non-prejudicial assessment. As a result, those cases no longer come within the Reviewer's terms of reference.

In performing their task, the Reviewer has access to all materials relied on by ASIO to make its assessment and any information obtained by ASIO since the adverse security assessment was completed or provided to the Reviewer by the applicant or his or her legal representatives. Particularly for periodic reviews, the Reviewer closely considers the overall security environment, which is informed by ASIO's contemporary assessment of security threats, and any changes to the applicant's circumstances or ideology during his or her time in detention.

The Reviewer's terms of reference are available at www.ag.gov.au/asareview. The Reviewer's annual report in accordance with the terms of reference is at Appendix E.

Independent National Security Legislation Monitor

The Hon. Roger Gyles AO QC was appointed as the Independent National Security Legislation Monitor on 7 December 2014. The Monitor's role is to review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation, and report to the Prime Minister and the parliament, on an ongoing basis.

During 2015–16, ASIO made submissions to the Monitor on the following inquiries:

- section 35 P of the ASIO Act concerning offences for the disclosure of information relating to a 'special intelligence operation'; and
- certain questioning and questioning and detention powers in relation to terrorism.

ASIO representatives also attended the public and private hearings on these matters.

ASIO's submissions to the Monitor and evidence given at public hearings can be found on the relevant inquiry page on the Monitor's website: www.inslm.gov.au.

Significant legal matters impacting on ASIO's business

ASIO's involvement in civil litigation (in particular, merits reviews and judicial reviews of its security assessments) and criminal prosecutions and control order hearings (especially in relation to counter-terrorism matters) continued this year.

We worked to provide the Administrative Appeals Tribunal (AAT), courts and applicants with relevant material in security assessment reviews, and to contribute sensitive information as evidence in criminal and civil proceedings. A particular concern was to balance the necessary protection of sensitive information (including intelligence capabilities and methods, officer and source identities, and liaison relationships) with our obligation to meet discovery requirements, assist the Crown to meet disclosure obligations and provide the fullest possible responses to subpoenas and statutory requests.

Coronial inquests are one area in which there has been a considerable increase in the involvement of national security agencies, including ASIO. ASIO gave evidence in two coronial inquests during the reporting period: those held into the deaths arising from the Lindt Café siege in Martin Place and the death of Ahmed Numan Haider.

Judicial reviews—security assessments

Two security assessment reviews were also commenced in the Federal Court of Australia during the reporting period.

- *BSX15 v Minister for Immigration and Border Protection and Director-General of Security* (VID473/2015) was commenced in August 2015 and heard by Justice Markovic on 19 April 2016 (decision reserved).
- *Mustapha El Ossman v Minister for Immigration and Border Protection and Director-General of Security* (NSD885/2016) was commenced in June 2016 (and yet to be heard at the time of reporting).

Both matters were still before the courts and both applicants were in immigration detention at the time of this reporting.

Tribunal reviews—security assessments

ASIO managed nine security assessment reviews by the AAT and an additional 13 reviews were commenced during the reporting period. Of these 22 security assessment reviews:

- nine were withdrawn at various stages of ASIO preparation;
- two were heard by the AAT—one was affirmed and reported as *TNFD and Director-General of Security; Minister for Foreign Affairs* [2015] AATA 752 (25 September 2015), and the other is yet to be decided; and
- 11 were being managed at the end of the reporting period.

Release of ASIO records

ASIO is subject to the release of its records under the *Archives Act 1983*, which allows for public access to all Australian Government records in the open access period. The open access period currently covers access to records created in or before 1991.

Requests to access ASIO records are made to the National Archives of Australia (NAA). The NAA passes the application to ASIO where relevant records are located and assessed. ASIO determines whether any information should be exempt from public release on national security grounds, balancing the request for public access with the need to protect sensitive information.

Applicants dissatisfied with ASIO exemptions can request a reconsideration of the decision. In 2015–16, there were four internal considerations. The NAA upheld the ASIO exemptions in all cases.

Applicants may also appeal the exemptions to the AAT if their request is not completed within 90 days. There was one new AAT appeal in the reporting period, which remains ongoing. One application from 2012–13 for 'deemed refusal' of multiple requests was finalised in February 2016 after ASIO provided the applicant with 11 032 pages of records.

In 2015–16, the number of applications made for access to records decreased (see Table 6). A total of 650 requests were completed in 2015–16. Although the number of requests completed declined, the number of pages examined increased.

	2014–15	2015–16
Applications for record access	790	473
Requests completed	811	650

Table 6: Processing of applications for access to ASIO records

1956 Melbourne Olympic Games

ASIO released 26 records about the 1956 Melbourne Olympic Games.

The Games were held at a time when there was considerable international tension arising from Britain, France and Israel seizing the Suez Canal and then withdrawing due to international pressure, and Soviet troops entering Hungary to suppress a popular revolution.

ASIO focused on three areas of concern for the Games. The first was that members of the Soviet bloc countries might take the opportunity to conduct intelligence operations using the Games and its athletes as cover. The second was that the Soviet Union might attempt to contact or assassinate the Petrovs who had defected to Australia in 1954; to mitigate this risk ASIO sent the Petrovs on holiday to Queensland during the games. The third was that members of Soviet bloc teams could attempt to seek political asylum in Australia.

ASIO and several other government departments developed policies and procedures to handle possible defections, and Cabinet approved these on 16 October 1956.

The Soviet bloc sent 1116 representatives to the Games. Many travelled by air but 124 arrived on a Russian ship, *The Gruzia* (see Figures 3 and 4). The Communist Party of Australia (CPA) formed an Olympic Games Committee to arrange entertainment for the Soviet visitors, and some members of the CPA were entertained aboard *The Gruzia*.

As expected, a number of visitors from the communist delegations applied for political asylum; this included representatives from Hungary, Russia, Romania, Yugoslavia and Poland.

These records are available for viewing at the NAA. Information on accessing NAA records can be found at www.naa.gov.au.

Figure 3: Members of the 1956 Russian Olympics team arriving at Essendon Airport

Figure 4: *The Gruzia* docked in Melbourne

History of ASIO project

The *Protest Years: the Official History of ASIO 1963–1975*, Volume II of the history, was launched by the Attorney-General on 16 October 2015. This volume was written by Dr John Blaxland of the Australian National University's (ANU) Strategic and Defence Studies Centre. Overall responsibility and direction for the project at the ANU remains with Professor David Horner AM. The third and final volume, *The Secret Cold War: the Official History of ASIO 1975–1989*, authored by Dr Blaxland and Dr Rhys Crawley, is scheduled for release in October 2016. Since their release, Volume I, *The Spy Catchers: the Official History of ASIO 1949–1963*, has sold over 8500 copies and was named a joint winner of the 2015 Prime Minister's Literary Awards Prize for Australian History. Volume II has sold over 5000 copies. ASIO's website has more information about the project at www.asio.gov.au/history.html.


F
FINANCIAL
STATEMENTS

Contents

Due to rounding, figures presented throughout these financial statements may not add precisely to the totals provided.

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2016 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

23 August 2016

Australian National Audit Office

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 2016, which comprise:

- Statement by the Director-General of Security;
- Statement of Comprehensive Income;
- Statement of Financial Position;
- Statement of Changes in Equity;
- Statement of Cash Flows; and
- Notes to and forming part of the Financial Statements and other explanatory information.

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 2016 and its financial performance and cash flows for the year then ended.

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 and is also responsible for such internal control as the Director-General of Security determines 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.

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

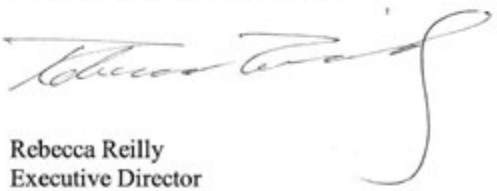
An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgement, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the 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 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.

Australian National Audit Office



Rebecca Reilly
Executive Director

Delegate of the Auditor-General

Canberra
23 August 2016

F

Due to rounding, figures presented throughout these financial statements may not add precisely to the totals provided.

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2016

	Notes	2016 $'000	Original Budget 2016 $'000	2015 $'000
EXPENSES				
Employee benefits	1.1.A	235,287	232,422	221,554
Suppliers	1.1.B	168,862	168,122	179,933
Depreciation and amortisation	2.2.B	76,111	62,997	63,800
Other	1.1.C	1,155	-	759
TOTAL EXPENSES		**481,415**	**463,541**	**466,046**
OWN-SOURCE INCOME				
Revenue				
Sale of goods and services	1.2.A	14,094	16,571	16,539
Other revenue	1.2.B	4,022	3,361	3,778
Gains	1.2.C	754	130	810
TOTAL OWN-SOURCE INCOME		**18,870**	**20,062**	**21,127**
NET COST OF SERVICES		**462,545**	**443,479**	**444,919**
REVENUE FROM GOVERNMENT	1.2.D	**381,081**	**380,482**	**368,423**
DEFICIT ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT		**(81,463)**	**(62,997)**	**(76,496)**
OTHER COMPREHENSIVE INCOME				
Changes in asset revaluation surplus		15,117	-	-
TOTAL COMPREHENSIVE DEFICIT		**(66,346)**	**(62,997)**	**(76,496)**

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

F

STATEMENT OF FINANCIAL POSITION as at 30 June 2016

	Notes	2016 $'000	Original Budget 2016 $'000	2015 $'000
ASSETS				
Financial assets				
Cash and cash equivalents	2.1.A	22,433	12,956	22,023
Trade and other receivables	2.1.B	93,868	92,766	93,975
Accrued revenue	2.1.C	711	6,687	4,998
Total financial assets		***117,013***	***112,409***	***120,996***
Non-financial assets				
Prepayments	2.2.A	20,870	13,136	25,354
Land and buildings	2.2.B	174,878	237,457	175,571
Property, plant and equipment	2.2.B	134,463	113,263	159,787
Computer software	2.2.B	44,441	51,147	36,868
Total non-financial assets		***374,652***	***415,003***	***397,580***
TOTAL ASSETS		**491,664**	**527,412**	**518,576**
LIABILITIES				
Payables				
Suppliers	2.3.A	6,083	25,013	16,622
Other payables	2.3.B	24,590	11,340	30,622
Total payables		***30,673***	***36,353***	***47,244***
Provisions				
Employee provisions	2.4.A	71,448	58,353	62,608
Restoration obligations	2.4.B	7,374	5,552	6,281
Total provisions		***78,822***	***63,905***	***68,889***
TOTAL LIABILITIES		**109,495**	**100,258**	**116,133**
NET ASSETS		**382,170**	**427,154**	**402,443**
EQUITY				
Parent equity interest				
Contributed equity		626,449	662,191	580,376
Reserves		33,047	17,931	17,930
Retained deficit		(277,326)	(252,968)	(195,863)
TOTAL EQUITY		**382,170**	**427,154**	**402,443**

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

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2016

	2016	Original Budget 2016	2015
	$'000	$'000	$'000
RETAINED EARNINGS			
Opening balance	(195,863)	(189,971)	(119,367)
Comprehensive income			
Deficit for the period	(81,463)	(62,997)	(76,496)
CLOSING BALANCE	**(277,326)**	**(252,968)**	**(195,863)**
ASSET REVALUATION SURPLUS			
Opening balance	17,930	17,931	17,930
Other comprehensive income			
Changes in asset revaluation surplus	15,117	-	-
CLOSING BALANCE	**33,047**	**17,931**	**17,930**
CONTRIBUTED EQUITY			
Opening balance	580,376	613,253	614,046
Transactions with owners			
Distributions to owners			
Returns of capital – reduction of appropriation	(3,000)	-	(82,877)
Contributions by owners			
Equity injection – appropriation	13,973	13,838	16,028
Departmental capital budget	35,100	35,100	33,179
CLOSING BALANCE	**626,449**	**662,191**	**580,376**
CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT	**382,170**	**427,154**	**402,443**

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

Accounting policy

Equity injections

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

STATEMENT OF CASH FLOWS
for the period ended 30 June 2016

	Notes	2016 $'000	Original Budget 2016 $'000	2015 $'000
OPERATING ACTIVITIES				
Cash received				
Appropriations		415,985	410,284	410,284
Sales of goods and services		18,715	16,394	16,973
Net GST received		16,080	15,415	17,004
Other		4,022	5,034	-
Total cash received		***454,802***	***447,127***	***444,261***
Cash used				
Employees		233,661	240,961	212,749
Suppliers		177,837	169,581	192,272
Section 74 receipts		26,338	19,932	22,055
Total cash used		***437,836***	***430,474***	***427,076***
NET CASH FROM OPERATING ACTIVITIES	3.2	**16,966**	**16,653**	**17,185**
INVESTING ACTIVITIES				
Cash received				
Proceeds from sales of property, plant and equipment		3,174	-	623
Total cash received		***3,174***	***-***	***623***
Cash used				
Purchase of property, plant and equipment		25,945	66,222	39,861
Purchase of intangibles		26,919	-	18,797
Total cash used		***52,864***	***66,222***	***58,658***
NET CASH USED BY INVESTING ACTIVITIES		**(49,690)**	**(66,222)**	**(58,035)**
FINANCING ACTIVITIES				
Cash received				
Contributed equity		33,135	48,938	45,772
Total cash received		***33,135***	***48,938***	***45,772***
NET CASH FROM FINANCING ACTIVITIES		**33,135**	**48,938**	**45,772**
Net increase in cash held		410	(631)	4,922
Cash and cash equivalents at the beginning of the reporting period	2.1.A	22,023	13,587	17,101
CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD		**22,433**	**12,956**	**22,023**

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

Notes to and forming part of the Financial Statements

OVERVIEW

Objective of ASIO

ASIO is an Australian Government-controlled not-for-profit entity. As authorised by the *Australian Security Intelligence Organisation Act 1979*, ASIO's purpose is to protect the nation and its interests from threats to security through intelligence collection, assessment, and advice for Government, government agencies, and business.

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 engages in five broad activities to achieve its purpose and meet its outcome: countering terrorism and the promotion of communal violence; countering espionage, foreign interference and malicious insiders; countering serious threats to Australia's border integrity; providing protective security advice to government and business; and collecting foreign intelligence in Australia. 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 Parliament.

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* (PGPA Act).

The financial statements have been prepared in accordance with:

Public Governance, Performance and Accountability (Financial Reporting) Rule 2015 (FRR) for reporting periods ending on or after 1 July 2015; 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.

New accounting standards

Adoption of New Australian Accounting Standard Requirements

Except for AASB 2015–7 (refer note 4.3 Fair value measurement) 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 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

ASIO expects to apply AASB 16 Leases from 2019–20. This standard will require the net present value of payments under most operating leases to be recognised as assets and liabilities. ASIO currently has $572.197m in operating lease commitments.

Taxation

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

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.

F

1. Financial Performance

	2016	2015
	$'000	$'000
1.1 EXPENSES		
1.1.A Employee benefits		
Wages and salaries	178,953	169,592
Superannuation		
Defined contribution plans	15,675	14,156
Defined benefit plans	17,072	17,084
Leave and other entitlements	23,466	20,300
Separation and redundancies	121	422
Total employee benefits	***235,287***	***221,554***
1.1.B Suppliers		
Goods supplied	5,490	10,928
Services supplied	123,217	124,718
Operating lease payments	37,837	41,708
Workers' compensation premiums	2,317	2,579
Total supplier expenses	***168,862***	***179,933***

Leasing Commitments

As lessee, ASIO has a number of operating lease commitments. These 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. Commitments are GST inclusive where relevant.

Commitments for minimum lease payments are payable:		
Within 1 year	51,552	51,213
Between 1 to 5 years	176,663	213,123
More than 5 years	343,982	342,585
Total operating lease commitments	***572,197***	***606,921***

Accounting policy

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

1.1.C Other expenses		
Finance costs: unwinding of discount – restoration obligations	204	193
Write-down and impairment of assets from:		
Impairment of receivables	-	4
Write-down of property, plant and equipment	951	376
Losses from asset sales	-	186
Other expenses	1	-
Total other expenses	***1,155***	***759***

	2016 $'000	2015 $'000
1.2 OWN-SOURCE REVENUE AND GAINS		
1.2.A Sale of goods and services		
Sale of goods	10	37
Sale of services	14,084	16,502
Total sale of goods and services	***14,094***	***16,539***

Accounting policy

Revenue from the sale of goods is recognised when the risks and rewards have been transferred to the buyer and ASIO retains no managerial involvement or effective control over the goods.

Revenue from the sale of services is recognised by reference to the stage of completion of contracts at reporting date. This is determined by the proportion that costs incurred to date bear to the estimated total costs of the transaction.

1.2.B Other revenue		
Rental income – operating lease	3,063	3,283
Royalties	19	19
Other	940	476
Total other revenue	***4,022***	***3,778***

Sublease rental income commitments

As lessor, operating lease income commitments are for office accommodation.

Commitments for rental income are receivable:		
Within 1 year	2,031	1,753
Between 1 to 5 years	8,752	9,589
More than 5 years	7,545	6,710
Total rental income commitments	***18,328***	***18,052***

	2016 $'000	2015 $'000
1.2.C Gains		
Resources received free of charge:		
Remuneration of auditors	140	130
Other	-	632
Gains from asset sales	555	-
Other gains	59	48
Total gains	***754***	***810***

Accounting policy

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.

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

1.2.D Revenue from government – Departmental appropriations	***381,081***	***368,423***

Accounting policy

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.

F

2. Financial Position

	2016 $'000	2015 $'000
2.1 FINANCIAL ASSETS		
2.1.A Cash and cash equivalents	***22,433***	***22,023***

Accounting policy

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

cash on hand; and

demand deposits in bank accounts with an original maturity of 3 months or less that are readily convertible to known amounts of cash and subject to insignificant risk of changes in value.

2.1.B Trade and other receivables		
Goods and services receivables	3,423	4,799
Appropriation receivable	85,962	84,441
GST receivable	4,483	4,735
Total trade and other receivables (net)	***93,868***	***93,975***
Age of receivables		
Not overdue	93,114	93,807
Overdue by:		
less than 30 days	276	17
31 to 60 days	87	55
61 to 90 days	196	3
more than 90 days	195	94
Total receivables (net)	***93,868***	***93,975***

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

Credit terms for goods and services were within 30 days (2015: 30 days).

Financial assets were assessed for impairment at 30 June 2016. No indicators of impairment have been identified.

Accounting policy

Trade receivables are classified as 'loans and receivables' and recorded at the nominal amounts 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.

Collectability of debts is reviewed at the end of the reporting period. Allowances are made when collectibility of the debt is no longer probable.

2.1.C Accrued revenue	***711***	***4,998***
Accrued revenue is expected to be recovered in:		
No more than 12 months	*711*	4,998

	2016	2015
	$'000	$'000
2.2 NON-FINANCIAL ASSETS		
2.2.A Prepayments	***20,870***	**25,354**
Prepayments are expected to be recovered in:		
No more than 12 months	*17,323*	19,936
More than 12 months	*3,547*	5,418
Total prepayments	**20,870**	***25,354***

F

2.2.B Reconciliation of Property, Plant, Equipment and Computer software

	Land	Buildings	Buildings - leasehold improvement	Property, plant & equipment	Computer software	Total
	$'000	$'000	$'000	$'000	$'000	$'000
2016						
As at 1 July 2015						
Gross book value	**1,565**	**6,688**	**199,694**	**222,517**	**79,283**	**509,747**
Accumulated depreciation, amortisation and impairment	**-**	**(1,858)**	**(30,519)**	**(62,730)**	**(42,415)**	**(137,521)**
Net book value 1 July 2015	***1,565***	***4,830***	***169,176***	***159,787***	***36,868***	***372,226***
Additions by purchase	**-**	**-**	**2,834**	**19,554**	**21,842**	**44,231**
Depreciation and amortisation expense	**-**	**(392)**	**(17,551)**	**(43,930)**	**(14,238)**	**(76,111)**
Disposals – other	**(1,565)**	**(258)**	**-**	**(1,714)**	**(32)**	**(3,569)**
Revaluations	**-**	**401**	**15,838**	**767**	**-**	**17,005**
Net book value 30 June 2016	***-***	***4,581***	***170,297***	***134,463***	***44,441***	***353,782***
Gross book value	**-**	**4,581**	**170,297**	**134,705**	**100,194**	**409,777**
Accumulated depreciation, amortisation and impairment	**-**	**-**	**-**	**(242)**	**(55,753)**	**(55,995)**
Net book value 30 June 2016	***-***	***4,581***	***170,297***	***134,463***	***44,441***	***353,782***

	Land	Buildings	Buildings - leasehold improvement	Property, plant & equipment	Computer software	Total
	$'000	$'000	$'000	$'000	$'000	$'000
2015						
As at 1 July 2014						
Gross book value	1,565	5,635	283,095	113,127	61,621	465,043
Accumulated depreciation, amortisation and impairment	-	(543)	(20,703)	(28,863)	(35,510)	(85,620)
Net book value 1 July 2014	***1,565***	***5,092***	***262,392***	***84,264***	***26,110***	***379,424***
Additions by purchase	-	1,053	10,424	27,505	18,827	57,809
Depreciation and amortisation expense	-	(1,314)	(16,301)	(38,147)	(8,039)	(63,802)
Disposals – other	-	-	(1)	(1,174)	(31)	(1,206)
Reclassification	-	-	(87,338)	87,338	-	-
Net book value 30 June 2015	***1,565***	***4,830***	***169,176***	***159,787***	***36,868***	***372,226***
Gross book value	1,565	6,688	199,694	222,518	79,283	509,748
Accumulated depreciation, amortisation and impairment	-	(1,858)	(30,518)	(62,731)	(42,414)	(137,521)
Net book value 30 June 2015	***1,565***	***4,830***	***169,176***	***159,787***	***36,868***	***372,226***

Computer software

The carrying value of computer software included $19.620m (2015 $11.622m) purchased software and $24.821m (2015 $25.246m) internally generated software.

Impairment

No indicators of impairment were found for property, plant, equipment and computer software.

Sale or disposal

Property, plant and equipment of an immaterial value only is expected to be sold or disposed of within the next 12 months. No land, buildings or computer software are expected to be sold or disposed of within the next 12 months.

Contractual commitments for the acquisition of property, plant, equipment and computer software

Within 1 year	-	-	3,040	689	3,226	6,954
Between 1 to 5 years	-	-	-	755	-	755
Total capital commitments	***-***	***-***	***3,040***	***1,443***	***3,226***	***7,709***

Accounting policy

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 $4,000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

Property, Plant and Equipment

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.

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:

	2016	2015
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

All assets were assessed for impairment at 30 June 2016. 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.

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

Computer software

ASIO's software comprises 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 (2014–15: 1–10 years).

	2016 $'000	2015 $'000
2.3 PAYABLES		
2.3.A Suppliers		
Trade creditors and accruals	6,083	16,622
Total suppliers	***6,083***	***16,622***
Settlement is usually made within 30 days.		
2.3.B Other payables		
Salaries	692	6,503
Superannuation	127	1,061
Unearned income	9,817	11,441
Amortisation of rent expense	11,111	7,876
Lease incentives	742	1,171
Fringe benefits tax	2,101	2,570
Total other payables	***24,590***	***30,622***
Other payables are expected to be settled in:		
No more than 12 months	2,088	13,310
More than 12 months	22,502	17,312
Total other payables	***24,590***	***30,622***
2.4 PROVISIONS		
2.4.A Employee provisions		
Leave	71,186	62,347
Superannuation	261	261
Total employee provisions	***71,448***	***62,608***
Employee provisions are expected to be settled in:		
No more than 12 months	18,363	17,271
More than 12 months	53,085	45,337
Total employee provisions	***71,448***	***62,608***

Accounting judgements and estimates

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.

Accounting policy

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.

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.

	2016	2015
	$'000	$'000

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. An assessment of ASIO's staff profile at balance date was performed; the assessment determined that the data profile used by the actuary is still relevant at balance date. The estimate of present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

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

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

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

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

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

F

2.4.B Restoration obligations	***7,374***	***6,281***
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.		
Restoration obligations to be settled in:		
No more than 12 months	4,353	2,401
More than 12 months	3,021	3,880
Total restoration obligations	***7,374***	***6,281***
Carrying amount 1 July 2015	6,281	6,088
Provision utilised	(1,000)	-
Unwinding of discount or change in discount rate	204	193
Revaluation as at 30 June	1,889	-
Closing balance	***7,374***	***6,281***

3. Funding

	Departmental		
	Ordinary annual services	**Capital budget**	**Equity injections**
	$'000	**$'000**	**$'000**
3.1 APPROPRIATIONS			
3.1.A Annual appropriations			
2016			
Appropriation Act			
Annual appropriation	**381,081**	35,100	13,973
PGPA Act			
Section 74 transfers	**26,338**	-	-
Total appropriation	***407,419***	***35,100***	***13,973***
Appropriation applied (current and prior years)	**(415,909)**	**(23,000)**	**(10,135)**
Variance	***(8,490)***	***12,100***	***3,838***

$2.401m (net) was returned to Government due to new government measures after original Budget and in accordance with section 51 PGPA Act.

Variances in 2015-16 are due to prior year appropriations applied in the current year and appropriations unspent due to the timing of asset purchases.

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: $2.852m (2015: $12.116m).

Department of Foreign Affairs and Trade relating to services overseas: $7.490m (2015: $7.249m).

2015			
Appropriation Act			
Annual appropriation	368,423	33,179	16,028
PGPA Act			
Section 74	22,055	-	-
Total appropriation	***390,478***	***33,179***	***16,028***
Appropriation applied (current and prior years)	(417,477)	(24,682)	(21,090)
Variance	***(26,999)***	***8,497***	***(5,062)***

$32.877m 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.

	2016	2015
	$'000	$'000
3.1.B Unspent departmental annual appropriations (recoverable GST exclusive)		
Appropriation Act (No. 1) 2015–16	**99,214**	-
Appropriation Act (No. 2) 2015–16	**3,838**	-
Appropriation Act (No. 1) 2014–15	**5,342**	80,218
Appropriation Act (No. 1) 2013–14	**-**	23,020
Appropriation Act (No. 1) 2012–13	**-**	3,227
Total	***108,394***	***106,465***

3.1.C Deficit excluding depreciation and amortisation

Revenue appropriations do not include an amount for depreciation and amortisation expenses. ASIO receives a separate capital budget provided through equity appropriations when capital expenditure is required.

Total deficit excluding depreciation and amortisation	**(5,352)**	**(12,696)**
Depreciation and amortisation	**(76,111)**	(63,800)
Deficit as per statement of comprehensive income	**(81,463)**	(76,496)

F

	2016	2015
	$'000	$'000

3.2 CASH FLOW RECONCILIATION

Reconciliation of cash and cash equivalents as per Statement of Financial Position to Statement of Cash Flows

Cash and cash equivalents as per:		
Cash Flow Statement	**22,433**	22,023
Statement of Financial Position	**22,433**	22,023
Reconciliation of net cost of services to net cash from operating activities		
Net cost of services	**(462,545)**	(444,919)
Revenue from Government	**381,081**	368,423
Adjustments for non-cash items		
Depreciation/amortisation	**76,111**	63,800
Net write-down of non-financial assets	**951**	376
Net gain (loss) on disposal of assets	**(555)**	186
Changes in assets/liabilities		
Decrease in receivables	**13,044**	27,333
Decrease in accrued revenue	**4,287**	455
(Increase)/decrease in prepayments	**4,484**	(2,713)
Increase/(decrease) in supplier payables	**(3,794)**	1,845
Increase in amortisation of rent expense	**3,235**	3,863
Decrease in lease incentives	**(429)**	(503)
Increase/(decrease) in other payables	**(8,838)**	775
Increase in employee provisions	**8,840**	6,071
Increase in restoration obligations	**1,093**	193
Decrease in other provisions	**-**	(8,000)
Net cash from operating activities	***16,966***	***17,185***

4. Managing uncertainties

	2016	2015
	$'000	$'000

4.1 CONTINGENT ASSETS AND LIABILITIES

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	150	1,125
New contingent liabilities recognised	-	150
Obligations expired	(150)	(1,125)
Total contingent liabilities	***-***	***150***

Unquantifiable contingencies

At 30 June 2016, 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.

Accounting policy

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.

4.2 FINANCIAL INSTRUMENTS

4.2.A Categories of financial instruments

Financial assets

Loans and receivables

Cash	22,433	22,023
Trade receivables	3,423	4,799
Accrued revenue	711	4,998
Total financial assets	***26,567***	***31,820***

Financial liabilities

At amortised cost

Trade creditors and accruals	6,083	16,622
Total financial liabilities	***6,083***	***16,622***

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 2016 (2015: Nil).

4.2.B 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.

4.2.C Liquidity risk

ASIO has sufficient available financial assets to meet all financial liabilities at 30 June 2016.

4.2.D 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'.

Accounting policy

Financial assets

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.

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.

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.

4.3 FAIR VALUE MEASUREMENT

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 2016

	Category	Fair value 2016	Fair value 2015	Valuation technique	Inputs used
		$'000	$'000		
Land	Level 3	**-**	1,565	Market approach	Price per square metre
Buildings on freehold land	Level 3	**1,255**	1,321	Market approach	Price per square metre
Buildings (specialised)	Level 3	**3,326**	3,509	Depreciated replacement cost	Replacement cost new Consumed economic benefit/ obsolescence of asset
Leasehold improvements	Level 3	**170,297**	159,540	Depreciated replacement cost	Replacement cost new Consumed economic benefit/ obsolescence of asset
Plant and equipment	Level 2	**40,403**	36,461	Market approach	Adjusted market transactions
Plant and equipment	Level 3	**7,145**	15,841	Market approach	Adjusted market transactions
Plant and equipment	Level 3	**86,668**	104,046	Depreciated replacement cost	Replacement cost new Consumed economic benefit/ obsolescence of asset
Total		***309,094***	***322,283***		

A reconciliation of movements in property, plant and equipment has been included in Note 2.2.B.

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 2016.

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 full revaluation and confirm the models developed comply with AASB 13 as at 30 June 2016.

There were no changes in valuation technique from the previous reporting period.

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

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 the asset 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.

Accounting policy

ASIO has chosen to early adopt *AASB 2015-7 Amendments to Australian Accounting Standards – Fair Value Disclosures of Not-for-Profit Public Sector Entities* at 30 June 2016. The future economic benefits of ASIO's non-financial assets are not primarily dependent on their ability to generate cash flows. ASIO has not disclosed qualitative information about the significant unobservable inputs or a narrative description of the sensitivities of the fair value measurements to changes in the unobservable inputs.

5. Other information

	2016	2015
	$'000	$'000
5.1 SENIOR MANAGMENT PERSONNEL REMUNERATION		
Short-term employee benefits		
Salary and allowances	11,578	10,648
Motor vehicle and other fringe benefits	1,176	782
Long-term employee benefits		
Annual leave accrued	1,139	1,015
Long-service leave accrued	365	325
Post-employment benefits		
Superannuation	2,409	2,257
Total senior management personnel remuneration	***16,667***	***15,027***

The total number of senior management personnel included above is 62. (2015: 56)

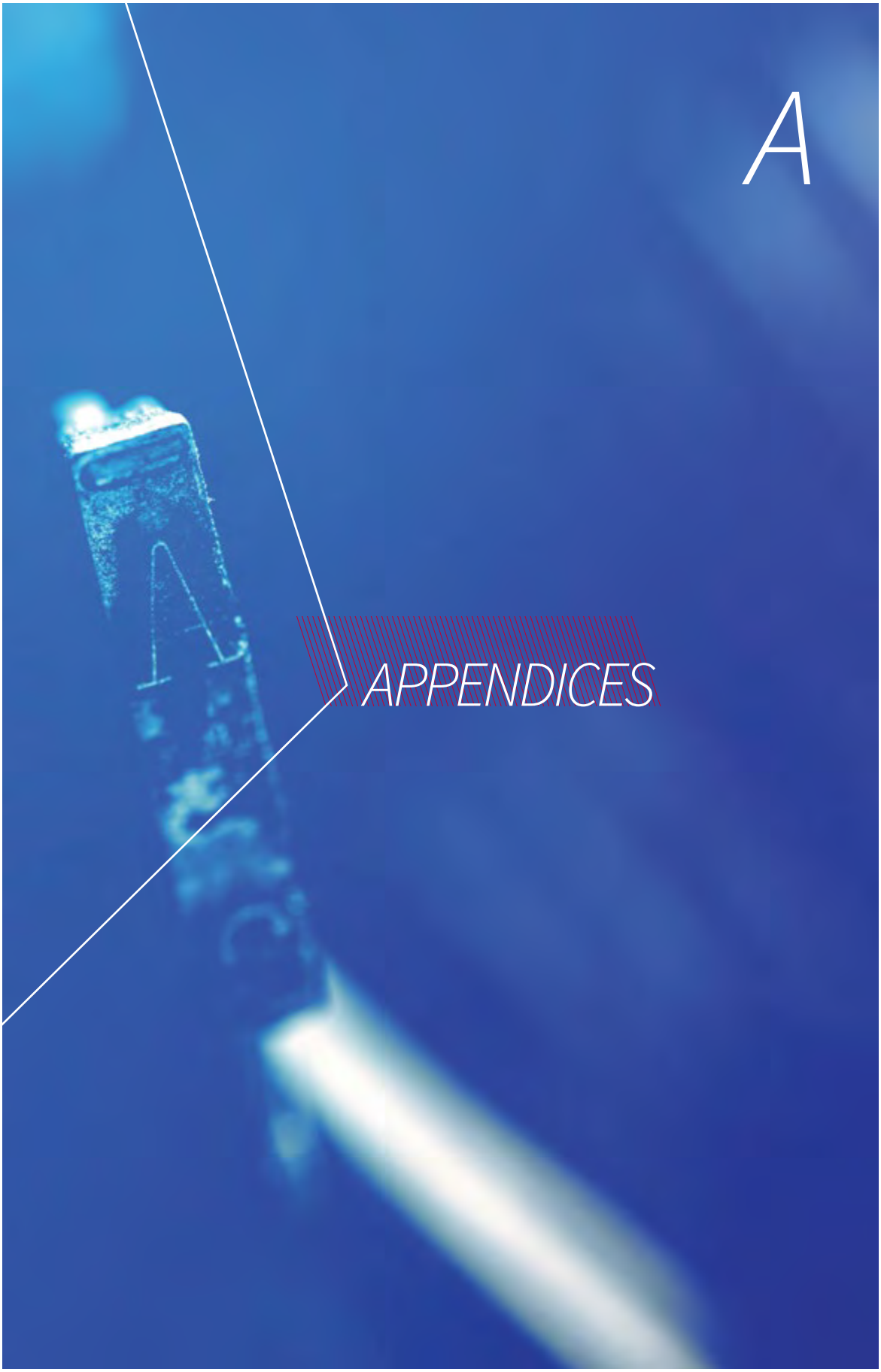
5.2 REPORTING OF OUTCOMES

Departmental		
Expenses	481,415	466,046
Own-source income	(18,870)	(21,127)
Net cost of outcome delivery	***462,545***	***444,919***

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

5.3 MAJOR BUDGET VARIANCES

Explanations of major variances between 2016 actual amounts and original budget amounts	Items affected
Movement in the 10 year bond rate had a financial impact on employee benefits due to accounting standard AASB 119 requirements.	**Statement of Comprehensive Income** Employee benefits **Statement of Financial Position** Employee provisions **Statement of Changes in Equity** Deficit for the period
Subsequent to the approval of the original budget ASIO reclassified a significant number of assets from Land and Buildings to Property, Plant and Equipment. This occurred as part of commissioning Ben Chifley Building assets. Property, Plant and Equipment assets have a shorter useful life thus depreciate at a higher rate.	**Statement of Comprehensive Income** Depreciation and amortisation **Statement of Financial Position** Land and Buildings Property, plant and equipment Computer software **Statement of Changes in Equity** Deficit for the period
Non-financial assets revaluation and resulting increase in the asset revaluation reserve was not included in the budget due to the nature and uncertainty of the activity.	**Statement of Comprehensive Income** Changes in asset revaluation surplus **Statement of Financial Position** Reserves **Statement of Changes in Equity** Changes in asset revaluation surplus
Capital expenditure has been less than anticipated due to resource re-prioritisation. Expenditure has been rescheduled to occur over a longer period of time.	**Statement of Financial Position** Land and Buildings Property, plant and equipment Computer software **Statement of Cash Flows** Cash received – contributed equity Purchase of property, plant and equipment Purchase of computer software
Re-profiling of ASIO's Departmental Capital Budget occurred post budget; appropriations were returned to Government and reallocated in future years to better reflect forecast asset replacement.	**Statement of Financial Position** Contributed equity **Statement of Changes in Equity** Contributed equity opening balance
ASIO contributed $3m to the National Security Campaign which occurred post budget.	**Statement of Cash Flows** Cash received – contributed equity



A

APPENDICES

Appendix A—Agency resource statement

	Actual available appropriation 2015–16 $'000	Payments made 2015–16 $'000	Balance remaining 2015–16 $'000
ORDINARY ANNUAL SERVICES[1]			
Departmental appropriation			
Prior year appropriation[2]	84,441*	79,098	5,342
2015–16 appropriation	381,081*	331,400	49,681
s74 relevant agency receipts[3]	26,338*	26,338	-
2015–16 capital budget	32,100*	5,000	27,100
Cash on hand	22,023	(410)	22,433
TOTAL ORDINARY ANNUAL SERVICES	**545,983**	**441,426**	**104,557**
OTHER SERVICES			
Departmental non-operating[4]			
Prior year equity injections	-*	-	-
Equity injections	13,973*	10,135	3,838
TOTAL OTHER SERVICES	**13,973**	**10,135**	**3,838**
TOTAL NET RESOURCING AND PAYMENTS FOR ASIO	**559,956**	**451,561**	

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

[2] Includes an amount of $18.0m from 2013-14 for the Departmental Capital Budget For accounting purposes this amount has been designated as 'contributions by owners'

[3] $22.085m per Portfolio Budget Statement plus $4.253m underestimate at time of PBS

[4] 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* 2015–16 $'000	Actual Expenses 2015–16 $'000	Variation 2015–16 $'000
Program 1.1: Security Intelligence			
Departmental expenses			
Appropriation[1]	381,081	381,081	(0)
Expenses not requiring appropriation in the Budget year	63,610	63,942	(332)
Total for Program 1.1	**444,691**	**445,023**	**(332)**
Total expenses for Outcome 1	**444,691**	**445,023**	**(332)**

* as per Portfolio Budget Statements including adjustments made at Additional Estimates

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

A

Appendix C—Workforce statistics

	2014–15			2015–16		
	Ongoing	Non-Ongoing	Total	Ongoing	Non-Ongoing	Total
Full-time	1,517	31	1,548	1,565	18	1,583
Part-time	211	17	228	225	15	240
Casual	N/A	53	53	N/A	57	57
Total	**1,728**	**101**	**1,829**	**1,790**	**90**	**1,880**

Table 7: Staff by load and employment status

Notes: Non-ongoing employees include locally engaged staff and secondees.

	2014–15				2015–16			
	Ongoing	Non-Ongoing	Casual	Total	Ongoing	Non-Ongoing	Casual	Total
Female	772	23	14	809	811	16	14	841
Male	956	25	39	1,020	979	17	43	1,039
Total	**1,728**	**48**	**53**	**1,829**	**1,790**	**33**	**57**	**1,880**

Table 8: Staff by gender and employment status

		2014–15				2015–16			
		Ongoing	Non-Ongoing	Casual	Total	Ongoing	Non-Ongoing	Casual	Total
Senior Executive Service	SES Band 3	1	1	0	2	2	1	0	3
	SES Band 2	8	2	0	10	12	1	0	13
	SES Band 1	36	2	0	38	34	2	1	37
Senior officers	AEE2/3	156	7	3	166	156	3	1	160
	AEE1	330	6	3	339	372	3	4	379
Employees	AE1-AE6	1,083	29	46	1,158	1,085	23	50	1,158
IT employees	ITO1/2	105	1	1	107	121	0	1	122
Engineers	Grade 1/2	9	0	0	9	8	0	0	8
Total		**1,728**	**48**	**53**	**1,829**	**1,790**	**33**	**57**	**1,880**

Table 9: Employees by classification and employment status

Notes: The number of employees at each level is not broken down any further in the public version of the annual report to avoid prejudice to ASIO's activities.

A

	2014–15				2015–16			
	Ongoing	Non-Ongoing	Casual	Total	Ongoing	Non-Ongoing	Casual	Total
Canberra-based	1,224	37	39	1,300	1,268	20	46	1,334
Other locations	504	11	14	529	522	13	11	546
Total	**1,728**	**48**	**53**	**1,829**	**1,790**	**33**	**57**	**1,880**

Table 10: Employees by location and employment status

Notes: The location of employees is not broken down any further in the public version of the annual report to avoid prejudice to ASIO's activities.

	2014–15	2015–16
Identify as Indigenous	9	10
People with a disability	20	19
Non-English speaking background	109	106

Table 11: Diversity of ASIO employees

Notes: Employees identifying as Indigenous, with a disability, or from a non-English speaking background calculated using available data.

Appendix D—ASIO's salary classification structure as at 30 June 2016

Senior Executive Service	
SES Band 3	$308 525 minimum point
SES Band 2	$224 555 minimum point
SES Band 1	$183 484 minimum point
Senior employees	
AEE3	$149 189
AEE2	$126 065–149 189
AEE1	$109 994–122 916
Employees	
AE6	$86 538–97 503
AE5	$78 292–84 044
AE4	$71 337–76 551
AE3	$63 092–68 951
AE2	$55 492–61 458
AE1	$47 891–53 202
Intelligence employees	
IE	$86 538–97 503
IE trainees	$78 292–92 181
Information technology employees	
SITEA	$149 189
SITEB	$126 065–149 189
SITEC	$109 994–122 916
ITE2	$86 538–97 503
ITE1	$75 358–82 850
Engineers	
SIE(E)5	$149 189
SIE(E)4	$126 065–149 189
SIE(E)3	$109 994–122 916
SIE(E)2	$86 538–97 503
SIE(E)1	$75 358–82 850

Notes: The salary figures include a 7.5 per cent service allowance. The service allowance is paid to all employees and recognises the imposition of security, professional and personal restrictions applicable to working in ASIO.

Appendix E—Report of the Independent Reviewer of Adverse Security Assessments

The Hon. Margaret Stone concluded her term as Independent Reviewer of Adverse Security Assessments on 21 August 2015 before taking up a new appointment as IGIS. Robert Cornall AO was appointed as Independent Reviewer on 3 September 2015.

During the reporting period to 21 August 2015, the Hon. Margaret Stone completed two periodic reviews:

- In one of those two cases, the Independent Reviewer's draft report recommended ASIO issue a non-prejudicial security assessment. After considering the Reviewer's draft findings and other information derived from its own investigations, ASIO issued a non-prejudicial assessment and the Reviewer finalised her report on the basis that the new non-prejudicial assessment was appropriate.
- In the second case, the Reviewer found that the adverse security assessment was appropriate (but see below).

In another case, the Independent Reviewer deferred the conduct of a periodic review as it was not appropriate to proceed at that time (also see below).

Since the appointment of the new Independent Reviewer on 3 September 2015, nine cases have been finalised.

A number of legal representatives advised the former Independent Reviewer they would await the outcome of ASIO's concurrent internal review before turning their attention to the Reviewer's process. This agreement avoided possible duplication of work if the adverse security assessment was replaced with a qualified or non-prejudicial assessment.

One primary and three periodic reviews were finalised under this arrangement after ASIO's decision to issue a qualified security assessment to each of those four applicants.

In the case referred to above in which Ms Stone found that the adverse security assessment was appropriate, ASIO issued a qualified security assessment for that applicant on 4 September 2015 based on new information.

In four other periodic reviews, the former Independent Reviewer had prepared draft reports before the end of her term. In each of those cases, the newly appointed Independent Reviewer completed the periodic review reports after ASIO's decision during the reporting period to issue each of those four applicants with a qualified security assessment in place of their previous adverse security assessment.

In summary:

- Ten adverse security assessments have been reviewed during the year (one primary and nine periodic reviews).
- There was no difference of opinion between the Independent Reviewer and the Director-General as to the appropriate outcome in any of those cases.
- As indicated above, the outcome of both the Independent Reviewer's processes and ASIO's internal reviews resulted in an opinion or a decision that the adverse security assessment was no longer appropriate based on ASIO's current assessment of the threat environment, any new information and any other relevant factors regarding an individual applicant.

Only four cases remain before the Independent Reviewer: two primary and two periodic reviews. At the end of the reporting period:

- one primary review was close to completion;
- the other primary review was under active consideration and awaiting a submission from the applicant's solicitors;
- a complicated matter due for periodic review was deferred with the agreement of the applicant's solicitors, pending the outcome of ASIO's current internal review of that adverse security assessment; and
- the periodic review referred to above which was deferred by the former Independent Reviewer is still deferred, with the agreement of the applicant's legal advisers, pending the completion of ASIO's separate internal review which was in train at the end of the reporting period.

Appendix F—ASIO's use of questioning warrants and questioning and detention warrants

ASIO is required by section 94 of the ASIO Act to include details on its use of questioning warrants and questioning and detention warrants in its annual report. Table 12 provides the required detail.

Section	Description	2014–15	2015–16
94(1)(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	0
94(1)(b)	The total number of warrants issued during the year under that division	0	0
94(1)(c)	The total number of warrants issued during the year under section 34E	0	0
94(1)(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	0
94(1)(e)	The total number of warrants issued during the year under section 34G	0	0
94(1)(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	0
94(1)(f)(ii)	The number of hours each person spent in detention under such a warrant	0	0
94(1)(f)(iii)	The total of all those hours for all those persons	0	0
94(1)(g)	The number of times each prescribed authority had persons appear for questioning before him or her under warrants issued during the year	0	0

Table 12: ASIO's use of questioning warrants and questioning and detention warrants.

List of requirements

Below is the table set out in Schedule 2 of the PGPA Rule. Section 17AJ(d) requires this table to be included in entities' annual reports as an aid of access.

PGPA Rule Reference	Part of Report	Description	Requirement	Part
17AD(g)	**Letter of transmittal**			
17AI		A copy of the letter of transmittal signed and dated by accountable authority on date final text approved, with statement that the report has been prepared in accordance with section 46 of the Act and any enabling legislation that specifies additional requirements in relation to the annual report.	Mandatory	Preliminaries
17AD(h)	**Aids to access**			
17AJ(a)		Table of contents.	Mandatory	Preliminaries
17AJ(b)		Alphabetical index.	Mandatory	Appendices
17AJ(c)		Glossary of abbreviations and acronyms.	Mandatory	Appendices
17AJ(d)		List of requirements.	Mandatory	Appendices
17AJ(e)		Details of contact officer.	Mandatory	Inside front cover
17AJ(f)		Entity's website address.	Mandatory	Inside front cover
17AJ(g)		Electronic address of report.	Mandatory	Guide to this report
17AD(a)	**Review by accountable authority**			
17AD(a)		A review by the accountable authority of the entity.	Mandatory	1
17AD(b)	**Overview of the entity**			
17AE(1)(a)(i)		A description of the role and functions of the entity.	Mandatory	1
17AE(1)(a)(ii)		A description of the organisational structure of the entity.	Mandatory	1
17AE(1)(a)(iii)		A description of the outcomes and programmes administered by the entity.	Mandatory	1
17AE(1)(a)(iv)		A description of the purposes of the entity as included in corporate plan.	Mandatory	3
17AE(1)(b)		An outline of the structure of the portfolio of the entity.	Portfolio departments - mandatory	N/A

PGPA Rule Reference	Part of Report	Description	Requirement	Part
17AE(2)		Where the outcomes and programs administered by the entity differ from any Portfolio Budget Statement, Portfolio Additional Estimates Statement or other portfolio estimates statement that was prepared for the entity for the period, include details of variation and reasons for change.	If applicable, Mandatory	N/A
17AD(c)	**Report on the Performance of the entity**			
	Annual performance Statements			
17AD(c)(i); 16F		Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule.	Mandatory	3
17AD(c)(ii)	***Report on Financial Performance***			
17AF(1)(a)		A discussion and analysis of the entity's financial performance.	Mandatory	3
17AF(1)(b)		A table summarising the total resources and total payments of the entity.	Mandatory	Appendix A
17AF(2)		If there may be significant changes in the financial results during or after the previous or current reporting period, information on those changes, including: the cause of any operating loss of the entity; how the entity has responded to the loss and the actions that have been taken in relation to the loss; and any matter or circumstances that it can reasonably be anticipated will have a significant impact on the entity's future operation or financial results.	If applicable, Mandatory	3
17AD(d)	**Management and Accountability**			
	Corporate Governance			
17AG(2)(a)		Information on compliance with section 10 (fraud systems).	Mandatory	Letter of Transmittal
17AG(2)(b)(i)		A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	Letter of Transmittal
17AG(2)(b)(ii)		A certification by accountable authority that appropriate mechanisms for preventing, detecting incidents of, investigating or otherwise dealing with, and recording or reporting fraud that meet the specific needs of the entity are in place.	Mandatory	Letter of Transmittal

PGPA Rule Reference	Part of Report	Description	Requirement	Part
17AG(2)(b)(iii)		A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud relating to the entity.	Mandatory	Letter of Transmittal
17AG(2)(c)		An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance.	Mandatory	5
17AG(2)(d) – (e)		A statement of significant issues reported to Minister under paragraph 19(1)(e) of the Act that relates to non-compliance with Finance law and action taken to remedy non-compliance.	If applicable, Mandatory	N/A
	External Scrutiny			
17AG(3)		Information on the most significant developments in external scrutiny and the entity's response to the scrutiny.	Mandatory	5
17AG(3)(a)		Information on judicial decisions and decisions of administrative tribunals and by the Australian Information Commissioner that may have a significant effect on the operations of the entity.	If applicable, Mandatory	N/A
17AG(3)(b)		Information on any reports on operations of the entity by the Auditor-General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman.	If applicable, Mandatory	N/A
17AG(3)(c)		Information on any capability reviews on the entity that were released during the period.	If applicable, Mandatory	N/A
	Management of Human Resources			
17AG(4)(a)		An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	5

PGPA Rule Reference	Part of Report	Description	Requirement	Part
17AG(4)(b)		Statistics on the entity's APS employees on an ongoing and non-ongoing basis; including the following: Statistics on staffing classification level; Statistics on full-time employees; Statistics on part-time employees; Statistics on gender; Statistics on staff location; Statistics on employees who identify as Indigenous.	Mandatory	Appendix C
17AG(4)(c)		Information on any enterprise agreements, individual flexibility arrangements, Australian workplace agreements, common law contracts and determinations under subsection 24(1) of the Public Service Act 1999.	Mandatory	5
17AG(4)(c)(i)		Information on the number of SES and non-SES employees covered by agreements etc identified in paragraph 17AD(4)(c).	Mandatory	Appendix C
17AG(4)(c)(ii)		The salary ranges available for APS employees by classification level.	Mandatory	Appendix D
17AG(4)(c)(iii)		A description of non-salary benefits provided to employees.	Mandatory	N/A
17AG(4)(d)(i)		Information on the number of employees at each classification level who received performance pay.	If applicable, Mandatory	N/A
17AG(4)(d)(ii)		Information on aggregate amounts of performance pay at each classification level.	If applicable, Mandatory	N/A
17AG(4)(d)(iii)		Information on the average amount of performance payment, and range of such payments, at each classification level.	If applicable, Mandatory	N/A
17AG(4)(d)(iv)		Information on aggregate amount of performance payments.	If applicable, Mandatory	N/A
	Assets Management			
17AG(5)		An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities.	If applicable, mandatory	N/A
	Purchasing			
17AG(6)		An assessment of entity performance against the Commonwealth Procurement Rules.	Mandatory	5

PGPA Rule Reference	Part of Report	Description	Requirement	Part
		Consultants		
17AG(7)(a)		A summary statement detailing the number of new contracts engaging consultants entered into during the period; the total actual expenditure on all new consultancy contracts entered into during the period (inclusive of GST); the number of ongoing consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting year on the ongoing consultancy contracts (inclusive of GST).	Mandatory	5
17AG(7)(b)		A statement that "During [reporting period], [specified number] new consultancy contracts were entered into involving total actual expenditure of $[specified million]. In addition, [specified number] ongoing consultancy contracts were active during the period, involving total actual expenditure of $[specified million]".	Mandatory	5
17AG(7)(c)		A summary of the policies and procedures for selecting and engaging consultants and the main categories of purposes for which consultants were selected and engaged.	Mandatory	5
17AG(7)(d)		A statement that "Annual reports contain information about actual expenditure on contracts for consultancies. Information on the value of contracts and consultancies is available on the AusTender website."	Mandatory	5
		Australian National Audit Office Access Clauses		
17AG(8)		If an entity entered into a contract with a value of more than $100 000 (inclusive of GST) and the contract did not provide the Auditor-General with access to the contractor's premises, the report must include the name of the contractor, purpose and value of the contract, and the reason why a clause allowing access was not included in the contract.	If applicable, Mandatory	N/A

PGPA Rule Reference	Part of Report	Description	Requirement	Part
	Exempt contracts			
17AG(9)		If an entity entered into a contract or there is a standing offer with a value greater than $10 000 (inclusive of GST) which has been exempted from being published in AusTender because it would disclose exempt matters under the FOI Act, the annual report must include a statement that the contract or standing offer has been exempted, and the value of the contract or standing offer, to the extent that doing so does not disclose the exempt matters.	If applicable, Mandatory	N/A
	Small business			
17AG(10)(a)		A statement that "[Name of entity] supports small business participation in the Commonwealth Government procurement market. Small and Medium Enterprises (SME) and Small Enterprise participation statistics are available on the Department of Finance's website."	Mandatory	5
17AG(10)(b)		An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	5
17AG(10)(c)		If the entity is considered by the Department administered by the Finance Minister as material in nature—a statement that "[Name of entity] recognises the importance of ensuring that small businesses are paid on time. The results of the Survey of Australian Government Payments to Small Business are available on the Treasury's website."	If applicable, Mandatory	5
	Financial Statements			
17AD(e)		Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	5
17AD(f)	**Other Mandatory Information**			
17AH(1)(a)(ii)		If the entity did not conduct advertising campaigns, a statement to that effect.	If applicable, Mandatory	N/A
17AH(1)(b)		A statement that "Information on grants awarded to [name of entity] during [reporting period] is available at [address of entity's website]."	If applicable, Mandatory	N/A
17AH(1)(c)		Outline of mechanisms of disability reporting, including reference to website for further information.	Mandatory	5

PGPA Rule Reference	Part of Report	Description	Requirement	Part
17AH(1)(d)		Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found.	Mandatory	N/A exempt from FOI
17AH(1)(e)		Correction of material errors in previous annual report	If applicable, mandatory	N/A
17AH(2)		Information required by other legislation	Mandatory	N/A

List of ASIO Act requirements

ASIO is required by section 94 of the ASIO Act to include in its annual report details on its use of: questioning warrants and questioning and detention warrants; special intelligence operations; and authorisations for telecommunications data. The table below shows where this detail can be found in the report.

Requirement	Refer to
Reporting on questioning warrants and questioning and detention warrants	Appendix F
Reporting on special intelligence operations	Appendix G
Reporting on authorisations for telecommunications data	Appendix H

Notes: Appendices G and H are deleted from the public version of the annual report to avoid prejudice to ASIO's activities.

A

Abbreviations and short forms

A

AASB119—Australian Accounting Standards Board Standard 'Employee Benefits'

AAT—Administrative Appeals Tribunal

ABF—Australian Border Force

ACIC—Australian Criminal Intelligence Commission

ACSC—Australian Cyber Security Centre

ACT—Australian Capital Territory

AE—ASIO employee

AEE—ASIO executive employee

AFP—Australian Federal Police

AGD—Attorney-General's Department

AHRI—Australian Human Resources Institute

AIC—Australian Intelligence Community

al-Qa'ida IS—al-Qa'ida in the Indian Subcontinent

al-Qa'ida-IM—al-Qa'ida in the Islamic Mahgreb

ANU—Australian National University

ANZCTC—Australian – New Zealand Counter-Terrorism Committee

APS—Australian Public Service

ASA—Agency Security Adviser

ASD—Australian Signals Directorate

ASG—Abu Sayyaf Group

ASIC—Aviation Security Identification Card

ASIO—Australian Security Intelligence Organisation

ASIO2020—ASIO's strategic program

B

BCB—Ben Chifley Building

BLU—Business Liaison Unit

Boko Haram—ISIL-West Africa

Bold Goals—ASIO's diversity agenda

C

CELO—Counter-Espionage Liaison Officer

CERT—Computer Emergency Response Team Australia

CPA—Communist Party of Australia

CVE—countering violent extremism

D

DFAT—Department of Foreign Affairs and Trade

DIBP—Department of Immigration and Border Protection

DIO—Defence Intelligence Organisation

E

e-Learning—ASIO's intranet-based learning software program

F

FIRB—Foreign Investment Review Board

FTE—full-time equivalent

G

GST—Goods and Services Tax

G20—Group of Twenty

H

HealthINT—ASIO's staff health and wellbeing program

I

IADP—Intelligence Analyst Development Program

ICT—information and communications technology

IE—intelligence employee

IGIS—Inspector-General of Intelligence and Security

IODP—Intelligence Officer Development Program

ISIL—Islamic State of Iraq and the Levant

ISIL-West Africa—Boko Haram

ITE—information technology employee

ITO—information technology officer

J

JCTT—Joint Counter-Terrorism Team

JNMTU—Jihadist Network Mapping and Targeting Unit

M

MSIC—Maritime Security Identification Card

N

NAA—National Archives of Australia

NSW—New South Wales

NTAC—National Threat Assessment Centre

NTTAS—National Terrorism Threat Advisory System

O

OSB—Operation Sovereign Borders

P

PBS—Portfolio Budget Statement

PGPA Act—*Public Governance, Performance and Accountability Act 2013*

PID Act—*Public Interest Disclosure Act 2013*

PJCIS—Parliamentary Joint Committee on Intelligence and Security

PKK—Kurdistan Workers' Party

PSPF—Protective Security Policy Framework

S

SSANs—security-sensitive ammonium nitrates

SSBAs—security-sensitive biological agents

SCEC—Security Construction and Equipment Committee

SES—senior executive service

SITE—senior information technology employee

T

TGP—Technical Graduate Program

TIA Act—*Telecommunications (Interception and Access) Act 1979*

T4—ASIO's Protective Security Directorate

W

WWI—World War One

Glossary

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 a refusal of a visa or cancellation of a passport.

communal violence—is violence between different groups or persons in the Australian community that endangers the peace, order or good government of the Commonwealth.

foreign interference—activities relating to Australia that are carried on by, or on behalf of, are directed or subsidised by, or are undertaken in active collaboration with, a foreign power, being activities that:

A. involve a threat to any person; or

B. are clandestine or deceptive and:

   – are carried on for intelligence purposes;

   – are carried on for the purpose of affecting political or governmental processes; or

   – are otherwise detrimental to the interests of Australia.

espionage—the theft of Australian information or capability by person/s either acting on behalf of a foreign power or with the intent of providing information to a foreign power in order to provide that foreign power with an advantage.

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

foreign power—a foreign government, or an entity that is directed or controlled by a foreign government or governments, or a foreign political organisation.

investigation—the processes involved in collecting, correlating and evaluating information on known harmful activities and emerging security risks. The purpose of ASIO's security investigations is to develop insights that inform government decision-making and enables preventative action, including by partner agencies.

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

lone actors— an individual (or small group of like-minded individuals) who conducts, or plans to conduct, a disruptive and typically violent activity for political or religious motives. At the time the action is performed they act independently of real-world accomplices.

malicious insiders–are trusted employees and contractors who deliberately and willfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.

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.

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.

A

Index

A

A

A

R

S

T

U

V

W

Y

Each year since 2014, ASIO has held a photography competition inviting staff to submit images for inclusion in the annual report. This year's theme was 'Securing Australia's future'. The winning image appears as the opening to Part 1 – Overview of ASIO.