Australian Government

Australian Security Intelligence Organisation

ASIO Annual Report 2016–17

ISSN0815–4562 (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.

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

Website: www.asio.gov.au
Location of this annual report: www.asio.gov.au/asio-report-parliament-2016-17

Each year since 2014, ASIO has held a photography competition inviting staff to submit images for inclusion in the annual report. This year's winning image appears as the opening to Part 2—Overview of ASIO.

ASIO ANNUAL REPORT 2016–17

Australian Government

Australian Security Intelligence Organisation

Director-General of Security

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

3 October 2017
Ref: A14075869

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 the Australian Security Intelligence Organisation's (ASIO) annual report for 2016–17.

This report contains information required by the PGPA Rule 2014 and section 94 of the *Australian Security Intelligence Organisation Act 1979*. The full report contains sensitive, national security classified information regarding the intelligence activities of ASIO during this reporting period. In accordance with the determinations made by you and the Minister for Finance under section 105D of the PGPA Act, this classified information has been removed from the annual report tabled in the Parliament in order to avoid prejudice to ASIO's activities. The full report will be separately provided to you and copies distributed to the Minister for Finance, other national security ministers, senior national security officials and the Inspector-General of Intelligence and Security. The full report will be accessible to the Australian National Audit Office.

As required by subsection 17AG(2) of the PGPA Rule, I certify that fraud risk assessments and control plans have been prepared for ASIO, that we have appropriate mechanisms in place for preventing, investigating, detecting and reporting incidents of fraud, and that all reasonable measures have been taken to deal appropriately with fraud.

Yours sincerely,

Duncan Lewis.

Duncan Lewis

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

Contents

1

DIRECTOR-GENERAL'S REVIEW

Director-General's review

The world in which we live continues to be uncertain and often unpredictable. It has become more complex, with the scale and pace of threats continuing to accelerate. In this environment, ASIO works to protect Australia, its people and its interests by collecting and assessing security intelligence, and providing advice to the Australian Government. This advice extends to government agencies and to industry to assist them manage security risks and disrupt harmful activities by individuals, groups and nation states.

During this reporting period, ASIO made a significant contribution to combating terrorism, espionage, foreign interference, cyber and malicious insider–related activities that threatened Australia's national security.

A major survey of 64 of our federal, state and territory government and industry stakeholders—conducted at the end of this reporting period by an external, independent person with extensive national security experience—concluded that, without exception, ASIO is regarded as an effective, capable and reliable partner offering high-quality and largely unique services.

As the Director-General of Security, I am proud of the efforts of ASIO staff and the staff of federal, state and territory national security partners who have kept Australia and Australians safe. I commend them for their work and their sacrifices in a year that presented significant challenges.

The security and operating environment

During this reporting period, a range of factors contributed to the steadily worsening overall security and operational environment. These factors included:

- heightened terrorism, espionage and foreign interference threats to Australians and Australian interests, at home and overseas;
- our unprecedented security intelligence caseload—in terms of both the volume and seriousness of the threats we investigated; and
- an increasingly complex and resource-intensive operating environment.

Countering terrorism

Since the national terrorism threat level was raised in September 2014, there have been five onshore terrorist attacks targeting people in Australia and 13 disruption operations in response to imminent terrorist attack planning in Australia. All but one of these cases have been linked to or inspired by the Islamic State of Iraq and the Levant (ISIL).

The heightened terrorism threat environment, combined with the trend towards 'low-capability' attacks by individuals or small groups requiring limited planning, sustained the high volume and tempo of ASIO's counter-terrorism investigations and operations. During this reporting period, our security intelligence contributed directly to the disruption by law enforcement partners of three planned terrorist attacks in Australia, as well as the disruption or containment of other terrorism-related activities.

Notwithstanding these successes, the difficulty of identifying preparations for low-capability attacks by individuals or small groups, and the imperative to respond quickly when preparations are detected, placed considerable pressure on ASIO and law enforcement partners' staff and resources. It is important to reinforce that, due to the nature of these types of attacks, security and law enforcement agencies cannot guarantee that preparations will be detected in time to prevent future attacks.

While low-capability attacks have become more common, complex attacks remained a significant threat during this reporting period. This was demonstrated by the disrupted attack planning in Melbourne in December 2016.

Turning our attention offshore, we saw during this reporting period the tragic loss of Australian lives in terrorist attacks in the United Kingdom and Iraq. This reinforces the global nature of the threat posed by terrorism to Australians and Australian interests.

I am concerned in particular about the terrorist threat in South-East Asia. We must remember that more Australians have been killed in terrorist attacks in Indonesia than anywhere else. The re-emerging threat in the region can be attributed to several factors, including:

- the ongoing influence of ISIL;
- the significant number of South-East Asian foreign fighters involved in the conflict in Syria and Iraq and their potential return to the region;
- the release from prison of a significant number of convicted terrorists who remain capable and influential; and
- the utility and attractiveness of possible ungoverned spaces in the region—which can be used as safe havens for planning and logistic support by terrorists.

ASIO is supporting a broader Australian Government commitment to work closely with South-East Asian partners to combat violent extremism in the region. This commitment has been displayed most recently by the government's offer of support to the Philippine Government's response to the conflict in Marawi.

Throughout this reporting period, ASIO worked closely with our security partners in South-East Asia to counter the threat in the region and will continue to support their efforts, and the Australian Government's broader strategy of engagement in the region, in 2017–18.

Countering espionage, foreign interference and malicious insiders

Australia continued to be a target of espionage and foreign interference during this reporting period. Foreign intelligence services sought access to privileged and/or classified information on Australia's alliances and partnerships, our position on international diplomatic, economic and military issues, our energy and mineral resources, and our innovations in science and technology. While the harm from espionage and foreign interference is immediately evident in some cases, in other instances the harm may take years to eventuate. Espionage and foreign interference is an insidious threat—activities that may appear relatively harmless today can have significant future consequences.

During this reporting period, ASIO identified a number of states and other actors conducting espionage and foreign interference against Australia. Our investigations revealed countries undertaking intelligence operations to access sensitive Australian Government and industry information. We identified foreign powers clandestinely seeking to shape the

opinions of members of the Australian public, media organisations and government officials in order to advance their country's own political objectives. Ethnic and religious communities in Australia were also the subject of covert influence operations designed to diminish their criticism of foreign governments. These activities—undertaken covertly to obscure the role of foreign governments—represent a threat to our sovereignty, the integrity of our national institutions and the exercise of our citizens' rights.

Through our work in the Australian Cyber Security Centre (ACSC), we regularly observed cyber espionage activity targeting Australia. Foreign state-sponsored adversaries targeted the networks of the Australian Government, industry and individuals to gain access to information and progress other intelligence objectives. ASIO provided support to the ACSC's investigations of these harmful activities as well as the centre's work to remediate compromised systems. The number of countries pursuing cyber espionage programs is expected to increase, as these programs can offer significant returns with relatively low cost and plausible deniability. As technology evolves, there will be an increase in the sophistication and complexity of attacks.

We remained alert to and promptly investigated threats from malicious insiders—those trusted employees and contractors who deliberately breach their duty to maintain the security of privileged information. These investigations continued to be complex, resource-intensive and highly sensitive. A critical element of our response to this threat has been to conduct targeted outreach with government and industry executives and agency security advisers, to improve their capabilities to detect malicious insiders and mitigate the harm caused by their actions.

Operating environment

Rapid technological change continued to provide people who are engaging in activities that threaten Australia's security with new tools to conceal their activities from security and law enforcement agencies. The widespread use of encrypted communications by security intelligence targets remains an area of particular concern to ASIO. We provided support during this reporting period to the Australian Government's examination of policy options to respond to this issue.

Technology offered security and law enforcement agencies new opportunities to identify activities of security concern. Building and maintaining technical collection capabilities to stay ahead of the threats, however, was resource intensive. Transforming existing agency information and communications technology (ICT) infrastructure to effectively exploit new capabilities, manage the large volume and variety of data available, and to be adapted easily to new technologies is a major challenge, and one that will require significant, ongoing investment.

In addition to technological challenges in the operating environment, we faced heightened threats to our staff, facilities and information. This requires the diversion of resources to ensure the security and effectiveness of our operations.

National security partnerships

Close collaboration among Australia's national security partner agencies has been essential in responding to these security challenges. Collaboration among Australian partner agencies continued during 2016–17 to be at an all-time high. This has included work to progress shared national security objectives through joint agency bodies such as the federal, state and territory Joint Counter Terrorism Teams (JCTT), the National Threat Assessment Centre (NTAC), the Jihadist Network Mapping and Targeting Unit and the ACSC.

ASIO's international partnerships also remained critical to our work and delivered significant benefits for Australia's security. We maintained relationships with more than 350 partner agencies in 130 countries. The exchange of information on security threats with our partners contributed to the identification and disruption of planned terrorist attacks, both in Australia and overseas. The sharing and joint development of intelligence capabilities also strengthened our individual and collective abilities to detect, monitor and respond to threats.

Security awareness

Raising awareness of threats to Australians and Australian interests among Australian federal, state and territory parliaments, government agencies, and industry remained a significant focus for ASIO. Security and law enforcement agencies cannot identify and prevent all harmful activities affecting all Australians and Australian interests—finite resources must necessarily be focused on the areas of greatest overall harm. It is important that security risk managers within government and industry understand the threats and take steps to detect and defend against harmful activities.

During this reporting period, I and my senior ASIO colleagues briefed a range of government ministers, parliamentarians and industry leaders on terrorism, espionage and foreign interference–related issues. I addressed a number of forums on security issues, including the Australian Davos Connection and the launch of the Australian Strategic Policy Institute's counter-terrorism handbook.

ASIO's security outreach and engagement with government and industry continued through our Business and Government Liaison Unit (BGLU). The unit provided advice to stakeholders through its website, which provides subscriber access to intelligence-informed security advice. The unit also conducted briefing days tailored for at-risk industry sectors, focusing on security threats to aviation, places of mass gathering, defence industry, energy and resources, mass passenger transport, communications, and banking and finance. These briefings were highly valued by government and industry stakeholders.

Our ASIO–T4 Protective Security Directorate (ASIO–T4) provided a range of practical, physical protective security advice to support government and industry security managers, as well as assistance to strengthen the capabilities of our partners' protective security units.

ASIO's performance

Overall, ASIO performed effectively during this reporting period in what could be considered challenging circumstances. The major survey of 64 of our federal, state and territory government and industry stakeholders supported this assessment and showed that our work was held in high regard.

Notwithstanding this assessment of ASIO's performance, we carried considerable risk within our investigative caseload and faced significant resourcing pressures in other areas of our business. These pressures reflect the challenge of simultaneously responding, with finite resources, to two major types of security threat—the terrorism threat, which shows no sign of diminishing, and the espionage and foreign interference threat, which is expanding in its scope and complexity.

During this reporting period, we addressed these pressures by rigorously prioritising our efforts and allocating resources to address the highest sources of threat or potential harm. The practical consequence of this is that we had limited scope to address a range of other known or emerging risks. We will continue to review our priorities to best address risk as we proceed through 2017–18.

Our annual performance statements, contained in Part 4 of this report, provide further information on our performance during 2016–17. A report on our financial performance is provided in Part 4 and our financial statements are provided in Part 6.

Organisational reform

Within ASIO, we continued to progress strategic reforms to ensure we are focused on work that provides clear value for our stakeholders and that we have the right culture, people and systems to effectively achieve the Organisation's purpose. In July 2016, we launched the ASIO2020 program to progress these reforms. Some of the major issues addressed under the banner of ASIO2020 were:

- We re-examined our value proposition to better reinforce with our staff, our partners and the public the unique contribution we deliver to protect Australia. This value proposition is now at the heart of our corporate and public communications, exemplified by the launch in July 2017 of our new asio.gov.au website, which explains clearly what ASIO does, how we do it, and why it matters.
- We placed a strong emphasis on reinforcing a culture of innovation across our Organisation to position us to face the diverse challenges of the future. I appointed our Deputy Director-General for Counter-Terrorism as my Innovation Champion, and we are now supporting a range of ongoing innovation initiatives, programs and networks across ASIO.
- We reviewed our career management system to ensure we source, recruit, and retain the best people and enable our staff to pursue fulfilling careers. We made progress in developing a competency-based model of career management and the systems required to support our workforce into the future.

- We also worked to build an enterprise technology program that will enable ASIO to excel in using technology and data to achieve our purpose. Given the increasing opportunities and challenges brought about by rapid advances in technology, it is imperative that ASIO is a 'data-enabled organisation', connected to its partners, accountable to the people, innovative in its approach, and sustainable for the long term. During this reporting period, we agreed our strategy and began implementing the actions necessary to take us towards our vision.

In last year's annual report, I put on record my commitment to achieve gender equity across all levels of ASIO by 2020. As part of this commitment, I joined the Male Champions of Change program, which aims to provide innovative leadership in addressing challenging gender equity issues such as:

- the low representation of women in senior leadership positions;
- realising the economic and social benefits of greater female workforce participation;
- poor take-up and progression of women's careers in non-traditional sectors; and
- developing a strong culture of respect, engagement and inclusion for women across our communities.

During this reporting period, I addressed the Public Sector Women in Leadership Conference, conducted 'listen and learn' focus groups within ASIO, and attended Male Champions of Change meetings to share experiences and ideas with other senior chief executive officers.

We established the ASIO Diversity and Inclusion Standing Committee, chaired by my Deputy Director-General for Strategy, to develop, implement and review strategies to strengthen diversity and inclusion within ASIO. The committee, which forms part of ASIO's governance structure, commenced late in this reporting period.

Release of The secret cold war: the official history of ASIO 1975–1989

In October 2016, we were delighted to host the release of the third and final volume of ASIO's history, authored by Dr John Blaxland and Dr Rhys Crawley. The book was launched by the Attorney-General at ASIO's headquarters. The launch was attended by former Directors-General of Security as well as a small group of officers who joined ASIO at the Organisation's inception in 1949.

While at times challenging and confronting, the history of ASIO project has proved to be a rewarding and valuable endeavour for the Organisation. The three volumes have provided the public with insights into the reality of ASIO's business and, importantly, the personal commitment made by many nameless ASIO officers who have made significant contributions to keeping Australia and Australians safe.

Outlook

Looking forward to 2017–18, an important focus for ASIO will be supporting the establishment of the Australian Government's new Home Affairs portfolio and implementing the 2017 Independent Intelligence Review recommendations. I believe these measures will play an important role in strengthening our strategic direction, effectiveness and coordination of Australia's national security and intelligence efforts, at a time when the nation is facing complex, long-term threats to our security.

During the next reporting period, I look forward to working together with national security partners to protect Australia, our people and our interests.

2

OVERVIEW OF ASIO

Overview of ASIO

ASIO's purpose is to protect the nation, its people and its interests from threats to security through intelligence collection and assessment, and to provide advice to the Australian Government, government agencies and business.[1] Our functions are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act[2]).

In 2016–17, we pursued our purpose through five activities:[3]

- 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.

Countering terrorism and the promotion of communal violence

Since the late 1960s, when terrorism began to directly affect Australia, we have been working to prevent terrorist attacks and disrupt the activities of terrorists who threaten Australia and its interests. The recent rise of Islamist extremist terrorism has resulted in several successful terrorist attacks against Australians both here and overseas. One of our key focuses is the threat from a small number of Australians, both in Australia and in the Syria–Iraq conflict zone, who have the potential to conduct or inspire attacks. However, we also remain alert to the potential for acts of violence which are not linked to Islamist extremist terrorism.

Our unique contribution to the fight against terrorism is our ability to predict and anticipate emerging threat, to collect and assess intelligence, and to provide advice to our partners that enables them to take timely action to protect Australians and their interests. Our intelligence has been instrumental in disrupting numerous terrorist attacks in Australia and overseas.

[1] This purpose statement was included in our corporate plan for 2016–2017 and reflects our outcome in the ASIO portfolio budget statement 2016–17. This outcome is supported by Program 1.1: security intelligence.

[2] 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.

[3] For 2017–2018, we have adopted a four–activity structure.

Countering espionage, foreign interference and malicious insiders

Australia has long been a target of espionage and foreign interference by hostile foreign intelligence services. Espionage can involve the theft of sensitive, privileged or classified information which results in harm to Australia's national interests. Foreign interference can involve undue influence of our political processes or public opinion to the benefit of a foreign power. Malicious insiders can exploit their trusted access to intentionally or unintentionally assist a foreign power, or to harm Australia's interests.

ASIO has specific legislative responsibility for countering espionage and foreign interference. We work closely with partners in Australia and overseas to detect and degrade the harmful activities of our adversaries. We have recently detected and degraded significant hostile foreign intelligence activity against Australia's interests. We also work across government and private industry to increase awareness of the threat, and develop effective countermeasures.

Countering serious threats to Australia's border integrity

Australia's prosperity relies upon the movement of people and goods across its border. But some adversaries—such as its terrorists or people smugglers—may try to exploit our border to further their own interests or harm us.

We work with partners to protect Australia from serious threats to its border integrity. We provide security assessments on people seeking visas to come to Australia, and we support whole-of-government efforts to counter and disrupt people smugglers.

Providing protective security advice to government and business

Protective security advice helps government, business, and owners of critical infrastructure to make decisions about how they protect their information, people and assets.

We deliver protective security advice to government and the private sector through our security assessments on people seeking access to classified information, support to the Australian Government's foreign investment decision-making processes, and through our ASIO–T4 and BGLU.

Collecting foreign intelligence in Australia

Foreign intelligence is intelligence about the capabilities, intentions or activities of people and organisations offshore. ASIO assists other members of the Australian Intelligence Community (AIC) to collect foreign intelligence in Australia.

We harness our expertise in security, unique intelligence collection capabilities, strong national and international partnerships, and all-source intelligence analysis capabilities to provide trusted, actionable advice for our stakeholders.

A snapshot of what ASIO does and how we do it is provided at Chart 1.

ASIO exists to protect Australia, its people and its interests from threats to security

What we do

- Counter terrorism and the promotion of communal violence
- Counter espionage, foreign interference and malicious insiders
- Counter serious threats to Australia's border integrity
- Provide protective security advice to government and business
- Collect foreign intelligence in Australia

How we do it

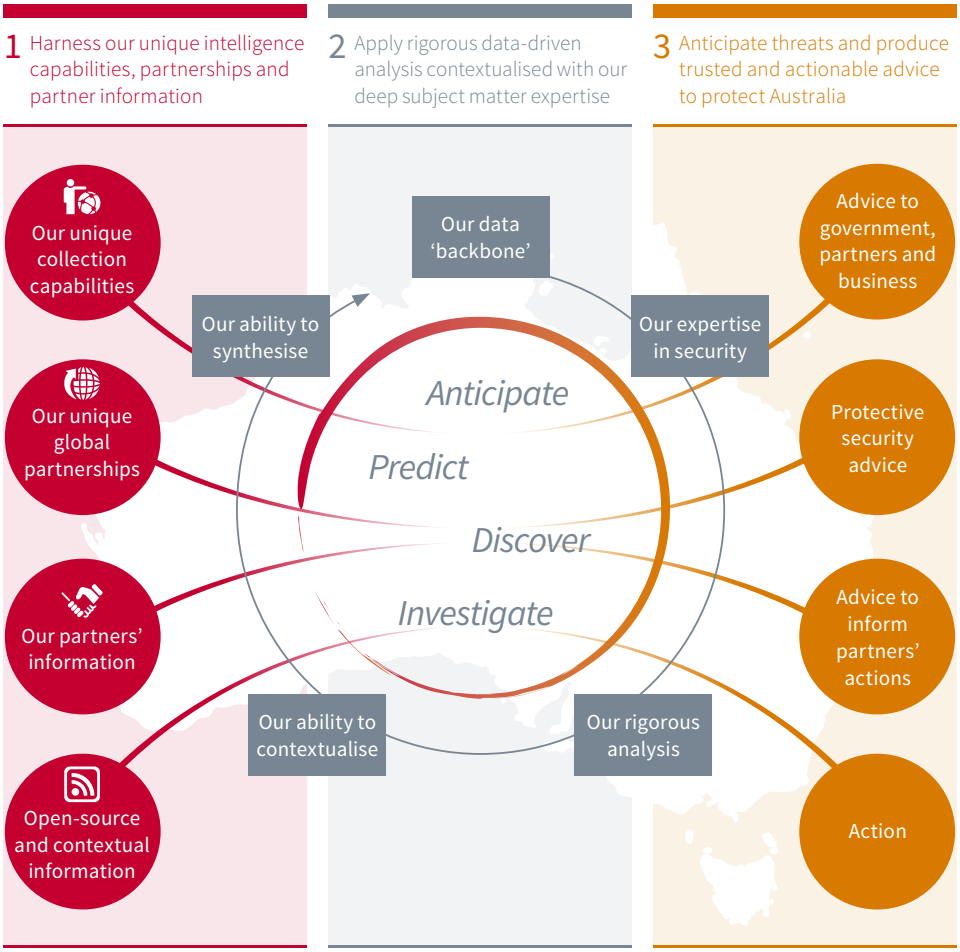


Chart 1: ASIO—what we do and how we do it.

Organisational structure

as at 30 June 2017

Duncan Lewis

DIRECTOR-GENERAL OF SECURITY

Deputy Director-General
STRATEGY

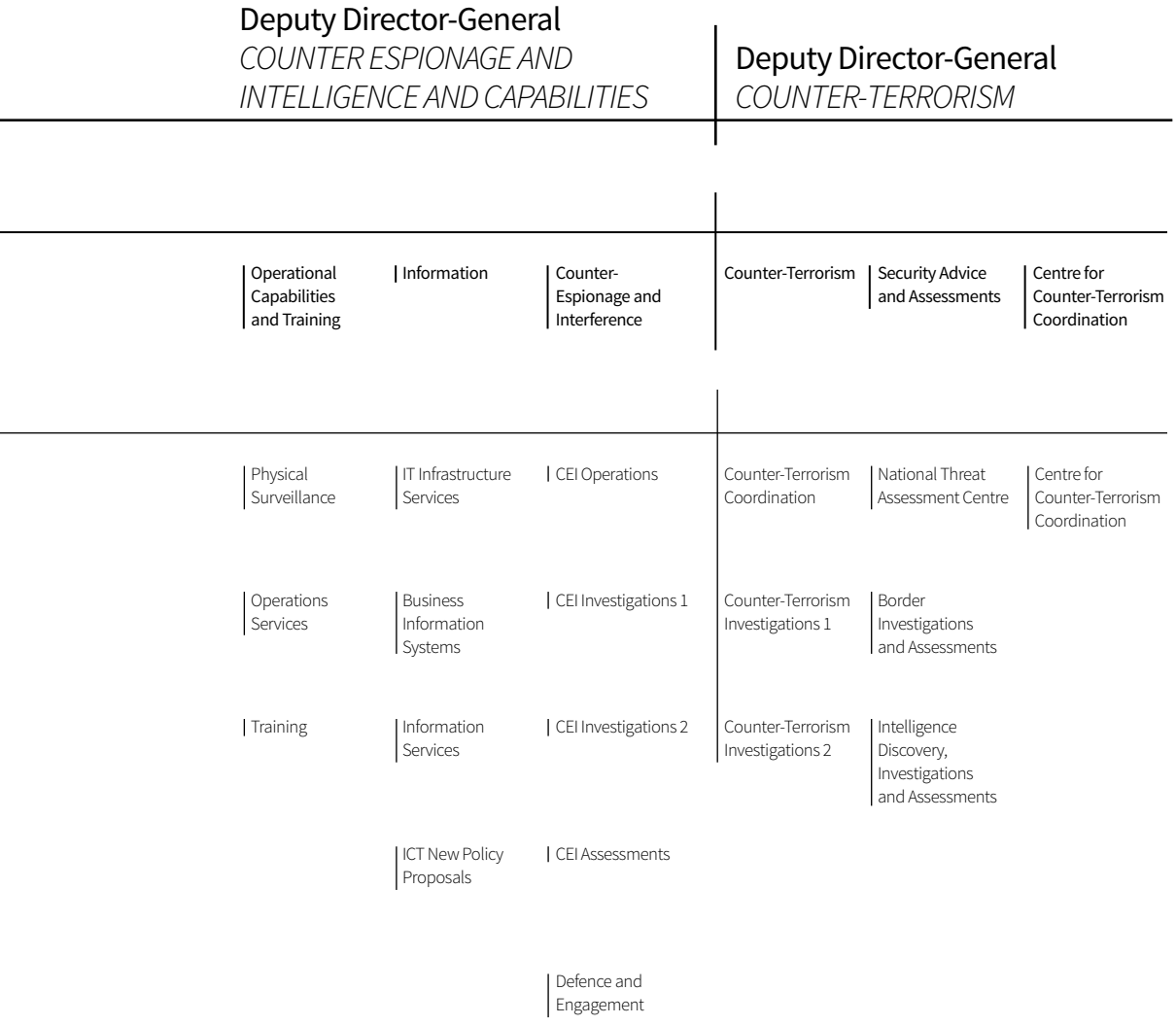
First Assistant Director-General

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

Assistant Director-General

	Office of the Senior Executive		Internal Security	Assessments, Corporate Law and Capability Protection	Data and Technical Analysis
	Strategic Partnerships and Production	State and Territory Managers	Financial Management	Operations Law	Telecommunication Operations
	ASIO2020		Human Resources	Litigation	Computer Operations
Overseas			Property		Close Access Operations
Seconded Officers					Strategy and Performance

Chart 2: ASIO's organisational structure.


Deputy Director-General
COUNTER ESPIONAGE AND INTELLIGENCE AND CAPABILITIES
Deputy Director-General
COUNTER-TERRORISM
Operational Capabilities and Training
Information
Counter-Espionage and Interference
Counter-Terrorism
Security Advice and Assessments
Centre for Counter-Terrorism Coordination
Physical Surveillance
IT Infrastructure Services
CEI Operations
Counter-Terrorism Coordination
National Threat Assessment Centre
Centre for Counter-Terrorism Coordination
Operations Services
Business Information Systems
CEI Investigations 1
Counter-Terrorism Investigations 1
Border Investigations and Assessments
Training
Information Services
CEI Investigations 2
Counter-Terrorism Investigations 2
Intelligence Discovery, Investigations and Assessments
ICT New Policy Proposals
CEI Assessments
Defence and Engagement

3

AUSTRALIA'S SECURITY ENVIRONMENT AND OUTLOOK

Australia's security environment and outlook

Terrorism—the Australian security environment

The Islamist extremist terrorism threat in Australia remains elevated with little prospect of significant improvement in the near term. We see little indication that the attraction of the Islamist extremist narrative is substantially declining—and we expect a very small number of Australian Islamist extremists will continue to plan and aspire to conduct terrorist attacks in Australia.

- The national terrorism threat level is currently **PROBABLE**—credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to conduct a terrorist attack in Australia. Since the national terrorism threat level was raised in September 2014, there have been five onshore terrorist attacks targeting people in Australia and 13 disruption operations in response to imminent terrorist attack planning in Australia (refer Chart 3). All but one have been linked to or inspired by ISIL.

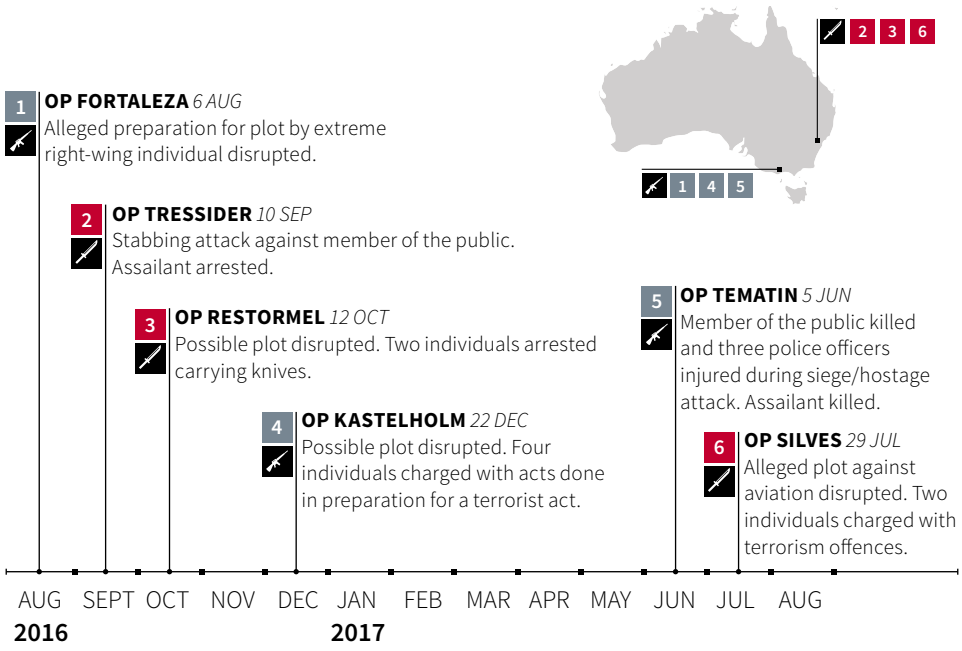


Chart 3: onshore terrorist attacks and disruptions.

While experience over recent years suggests the most likely form of terrorism in Australia remains an attack by an individual or small group, recent disrupted attack plots—in December 2016 in Melbourne and July 2017 in Sydney—remind us that we must be prepared for terrorist attacks across the spectrum of tactics and capabilities.

Globally, there has been a continued reduction in the perceived threshold of what is deemed a successful Islamist extremist terrorist attack—from complex to basic weapons, and targeting the public in relatively non-secured locations. Such attacks can emerge with little or no forewarning and are highly challenging to identify and prevent.

In response to the military pressure and losses faced by Islamist extremist groups, we continue to see in Islamist extremist English-language propaganda—particularly from ISIL. These are clear calls for terrorist attacks in Western countries, including Australia. We expect such propaganda will remain accessible and justify violence for years to come.

- The recent change in ISIL propaganda tone, from its success in establishing an Islamic caliphate and controlling territory to victimhood and the need for supporters to respond, is particularly noticeable.
- ISIL propaganda provides specific and direct guidance on particular attack methodologies and targeting to improve the lethality of terrorist attacks. Publicity surrounding terrorist attacks in the West is likely to provide further guidance.

We have seen a substantial decline in the number of Australians successfully travelling to join ISIL in Syria and Iraq. We continue to assess that most Australians with ISIL will remain there, either as a conscious choice or because they are currently unable to safely depart. In the longer term, further ISIL military losses are likely to lead to the death of many of these individuals, although we can expect considerable uncertainty about their circumstances.

Freedom of movement from the conflict zone will continue to be extremely limited. A small number of Australians may successfully depart Syria and Iraq, or may be detained there as ISIL loses territory. Of these:

- A very small number may return to Australia voluntarily, but are unlikely to hold valid travel documents, so will find this difficult. Others may be returned through deportation. It is unlikely large numbers will return in concentrated periods, but rather small numbers periodically—this will include non-combatant women and children.
- Some will go to third countries. Their destinations will be influenced by their background, ethnicity and language skills, or through connections that give them access to new destinations.
- Other Australians will stay long term with ISIL and other Islamist extremist groups in Syria and Iraq. A small handful of these are or may become involved in ISIL's external terrorist planning.

Any defeat of ISIL will not be absolute—some remnants of the group will remain, probably focused on a local insurgency, but still projecting a global terrorist threat. It will not eliminate the terrorist threat posed by Islamist extremist groups to Australia and Australian interests globally. This threat, including from those Australians who have spent time with ISIL in Syria and Iraq, will endure in the long term.

Additional factors bringing complexity and challenge to the Australian terrorism security environment include the increasing numbers of radicalised individuals incarcerated for terrorism or other offences, and the increasing availability and use of encrypted communication applications.

Terrorism—the international security environment

The international terrorism threat environment remains fraught. ISIL has been the dominant driver of terrorist attacks in Western countries. We have seen a multitude of attacks in Western countries—not only in European countries but also the United States—as well as significant attacks in Bangladesh, Turkey and the Philippines.

The July 2016 attack in Nice, France, where an individual drove a truck through a crowd killing over 80 people, exemplifies that 'simple' attacks can be highly lethal. 2016–17 has also seen the first instances of ISIL affiliates being involved in successful attacks in Western countries.

- Globally, we are confronted with increasing ungoverned spaces in Africa, the Middle East, South Asia and South-East Asia, which can be exploited by terrorist groups—and in some of these locations the situation will get worse.

While ISIL continues to be the principal source of terrorist threat to the West and Middle East, it is also a serious threat in South Asia, South-East Asia and Africa. Al-Qa'ida, however, continues to steadily rebuild and is positioning itself to resume the leadership of global jihad upon the demise of ISIL. Through its affiliates, al-Qa'ida is stronger than it has been for over a decade. Al-Qa'ida is building support and influence among Sunni populations across the Middle East, Africa and South Asia, and is an ongoing threat to the West.

Europe

Violent Islamist extremists continue to view Europe as a legitimate target for attack, particularly those countries involved in military activities in Syria and Iraq—numerous attacks occurred in 2016–17, including in the United Kingdom, France, Belgium, Germany, Sweden and Russia. Individuals inspired and encouraged by Islamist extremist groups—primarily ISIL—will continue to plan attacks targeting Europe. These attacks will most likely use basic weapons (such as knives and vehicles), firearms and explosives. Such attacks are likely to continue to target police and military targets, and crowded places such as shopping centres, transport hubs and sporting or entertainment events.

South Asia

The security environment in South Asia continues to deteriorate. Afghanistan faces a persistent threat from the Taliban and Haqqani Network, while Islamic State—Khorasan Province has increased its capability to conduct complex attacks in Kabul. Extremist groups in Pakistan continue to conduct attacks against government targets and minorities—while the number of extremist attacks in Pakistan has reduced, the lethality of these attacks has increased

substantially. India faces threats from domestic groups—such as Hindu extremists and north-east separatists—as well as broader regional threats from al-Qa'ida and ISIL, and their affiliates. Lashkar-e-Tayyiba also presents an ongoing threat. Al-Qa'ida in the Indian Subcontinent and ISIL continue to influence groups in Bangladesh, and extremists maintain the intent and capability to conduct attacks against both domestic and foreign targets there.

South-East Asia

In South-East Asia the influence of ISIL has continued to grow. The attack on Marawi City in the Philippines demonstrates the strength of ISIL's influence, and its ability to coalesce extremists and encourage them to undertake large-scale acts of violence. It is possible foreign fighters will seek to travel to the Philippines to undertake further terrorist acts or training. ISIL-inspired terrorists have continued to conduct attacks in Indonesia, some of which are linked to foreign fighters in Syria and Iraq. Hundreds of individuals from South-East Asia have travelled to Syria and Iraq to fight with militant groups, including ISIL, with some openly advocating attacks in South-East Asia. Some will continue to encourage and direct terrorist attacks in South-East Asia—including against Australian interests—meaning the terrorist threat is unlikely to abate in the near future. Some of these individuals will return from the conflict in Syria and Iraq, and this may increase the likelihood of a terrorist attack against Australians or Australian interests.

Africa

In Africa, al-Qa'ida- and ISIL-aligned groups continue to pose a significant security threat. Regional groups are expanding their areas of operation through increasing cooperation. Ongoing campaigns of attacks are aimed at destabilising regional governments, and extremists maintain their intent and capability to attack Western interests. Despite ongoing international and regional counter-terrorism operations, global jihadist ideology continues to resonate as a justification for violent responses to perceived regional grievances.

Middle East

The Middle East security environment remains highly complex with numerous threat groups of varying capability and intent posing an ongoing threat across the region. The Syria and Iraq conflict continues to dominate the security environment, and countries in the Middle East are likely to be adversely affected by the displacement of fighters from the conflict zone. ISIL remains capable of mounting complex attacks in Syria and Iraq against a range of targets, despite territorial losses and degradation of resources. ISIL and affiliated or aligned groups and individuals have conducted highly lethal attacks—including in Iran, Egypt, and Jordan—aimed at destabilising ruling governments and exacerbating sectarian divisions. Turkey remains a high-threat environment with both Kurdish groups and ISIL retaining the intent and capability to conduct attacks, including in metropolitan centres such as Istanbul and Ankara. In Yemen, both al-Qa'ida in the Arabian Peninsula and ISIL-Yemen continue to take advantage of the country's endemic instability.

Communal violence and violent protest

Most Australian protests, while occasionally employing disruptive tactics, comply with regulations and conclude without significant incident. However, ongoing hostility between extreme left-wing and anti-Islam/extreme right-wing proponents at protests occasionally results in confrontational behaviour. While protests relating to other issues are mostly peaceful and counter-protests are rare, disruptive tactics are occasionally used by various issue-motivated groups and violence remains possible.

- Minimal violence at left- and right-wing protests and events occurred through 2016–17. This was probably due to a number of factors including large police contingents keeping groups separate at events and peaceful left-wing attendees significantly outnumbering anti-Islam and right-wing opponents at a number of events.
- Anti-Islam/right- and left-wing proponents will continue to hold protests and counter-protests about issues relevant to their interests in the next 12 months. While we do not expect violence between extreme left- and right-wing proponents to escalate significantly, we note violence remains possible when these interest groupings meet.
- Protests relating to other issues—such as government policy, Indigenous rights and the environment—are mostly peaceful, and counter-protests are rare. Occasionally disruptive tactics are employed and incidental acts of violence may occur from time to time.

Australia continues to experience low levels of communal violence, although incidents in response to specific local or international events that resonate with expatriate communities do occur occasionally. In particular, high-level international visits have resulted in instances of provocative and small-scale violence in Australia-based diaspora communities.

While extreme right-wing groups in Australia have not engaged in or advocated terrorist-related activities, in 2016 a Melbourne-based man became the first person motivated by extreme right-wing ideology to be charged with terrorism offences . Any further extreme right-wing terrorist plots or attacks in Australia over the next 12–18 months would probably target the Muslim or left-wing community, be low-capability, and be more likely to be perpetrated by a lone actor or small group on the periphery of organised groups.

Espionage and foreign interference

The threat from espionage and foreign interference to Australian interests is extensive, unrelenting and increasingly sophisticated. In addition to traditional espionage efforts to penetrate government, foreign intelligence services are targeting a range of Australian interests, including clandestine acquisition of intellectual property, science and technology, and commercially sensitive information. Foreign intelligence services are also using a wider range of techniques to obtain intelligence and clandestinely interfere in Australia's affairs, notably including covert influence operations in addition to the tried and tested human-enabled collection, technical collection, and exploitation of the internet and information technology.

Australia continues to be a target of espionage through cyber means. The cyber threat is persistent, sophisticated and not limited by geography—Australian individuals and organisations can be targeted regardless of the physical location of the perpetrators. Increasingly, foreign states have acquired or are in the process of acquiring cyber espionage capabilities designed to satisfy strategic, operational and commercial intelligence requirements. We assess the number of cyber security incidents either detected or reported represents a fraction of the total threat Australia faces.

Espionage can cause severe harm to Australia's national security and economic well-being, and can have long-term implications if not detected. Interference by foreign actors can undermine Australia's sovereignty by advancing a foreign state's cause through covertly interfering in Australia's political system and seeking to unduly influence public perceptions of issues. Foreign interference in Australia's diaspora communities through harassment or other means can erode the freedoms enjoyed by all people living in Australia.

The clandestine nature of espionage and foreign interference means that the aggregate cost is difficult to quantify, particularly in dollar terms. However, the harm caused by hostile intelligence activity can undermine Australia's national security and sovereignty, damage Australia's international reputation and relationships, degrade its diplomatic and trade relations, inflict substantial economic damage, degrade or compromise nationally vital assets and critical infrastructure, and threaten the safety of Australian nationals.

Emerging espionage and foreign interference in Australia's economy is an area of growing concern, particularly with the increase of investment flows. Australia's economy is open and transparent, and foreign investment is both a welcome and important contributor to Australia's national wealth. However, it is not without national security risks. For example, foreign intelligence services are interested in accessing bulk data sets and privileged public or private sector information, including Australian intellectual property. Developing and implementing effective mitigation strategies for these issues is critical to reducing the threat to an acceptable level. Another emerging issue of potential national security concern is the lack of diversity of ownership within certain infrastructure sectors.

Espionage against the Australian defence industry is an enduring threat. The Australian Government's decades-long military modernisation program—which includes niche research and development capabilities within the sector—is of interest to a wide range of foreign intelligence services seeking to obtain or compromise sensitive technologies.

Border integrity

The people-smuggling environment is characterised by a continuing suppressed demand among potential illegal immigrants (PIIs) for travel by illegal maritime venture to Australia; however, Operation Sovereign Borders (OSB) and offshore regional processing constitute a significant and ongoing deterrent. Demand among PIIs for travel to Australia has fallen but is not universally or permanently suppressed. Illegal maritime ventures to Australia continue to be organised mainly from Sri Lanka and Indonesia, with the greatest interest in illegal travel being shown by PIIs from Sri Lanka, Bangladesh, Afghanistan, Myanmar and Vietnam. As such, planned and actual illegal maritime ventures to Australia will remain an enduring challenge over the next decade.

There will be a growing need to manage downstream security risks associated with the flow of people seeking entry to Australia and applying for citizenship. There will be some complex cases, including ones where we recommend against entry, visa retention or citizenship on security grounds. Enhancements in the way people of security concern are identified will represent an important aspect of ASIO's activities in support of border security. The size and scale of international migration has challenged state boundaries and jurisdictions, and will challenge Australia for the years ahead. ASIO's border security focus will continue to be on partnering with other Australian Government agencies such as the Department of Immigration and Border Protection (DIBP), in supporting the delivery of the annual migration program.


4
REPORT ON
PERFORMANCE

Part 4 reports on ASIO's performance in meeting our purpose. In line with the requirements of PGPA Rule 2014 subsection 17AD(c), it includes a copy of ASIO's annual performance statements for 2016–17 and a report on our financial performance.

In addition to these statements, a performance narrative is included which provides additional background information to support our performance claims.

Annual performance statements

Introductory statement

I, as Director-General of Security and the accountable authority of ASIO, present the 2016–17 annual performance statements for ASIO, as required under subsection 39(1)(a) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). In my opinion, these statements accurately present the performance of ASIO in achieving its purpose and comply with subsection 39(2) of the PGPA Act.

In accordance with determinations made by the Attorney-General and the Minister for Finance under section 105D of the PGPA Act, classified material has been removed from the performance statements provided in the annual report tabled in Parliament to avoid prejudicing ASIO's activities.

Full annual performance statements are provided in our classified annual report to the Attorney-General, which is also received by the Minister for Finance, other national security ministers, relevant senior national security officials and the Inspector-General of Intelligence and Security (IGIS). The classified annual report is accessible to the Australian National Audit Office.

Duncan Lewis
Director-General of Security

3 October 2017

ASIO's purpose

ASIO's purpose is to protect the nation, its people and its interests from threats to security through intelligence collection and assessment, and the provision of advice to the Australian Government, government agencies and business. In 2016–17, we pursued this purpose 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.

Results for 2016-17

Our corporate plan for 2016–17 established the measures and targets we have used to assess our performance in meeting our purpose. The following tables provide our high-level statements of performance in relation to the measures and targets established for the five activities described above. The tables also address our performance against additional performance measures from our corporate plan that apply across all of our activities.

In developing these statements we have drawn on internal performance-related reporting and an independent survey of our senior government and industry stakeholders conducted during May and June 2017.

1 Activity 1: countering terrorism and the promotion of communal violence

Measure	Results against targets	Refer
Effective identification and investigation of threats to Australia's security *Source: ASIO corporate plan 2016–17 (p. 16)*	**Target achieved:** new security leads are identified and consistently prioritised and pursued	PAGE 48

Our intelligence discovery and investigative efforts during 2016–17 contributed directly to law enforcement partners disrupting three planned terrorist attacks targeting people in Australia. We also identified a range of terrorism-related linkages between Australia and the conflict in Syria and Iraq.

During 2016–17, we received over 12 000 lead referrals and resolved or investigated approximately 15 000 leads.

The volume and tempo of our counter-terrorism investigations remained high, requiring rigorous prioritisation and a focus on the most significant threats. There was a high level of risk in our investigative caseload, which has continued beyond this reporting period. In particular, low-capability attacks by lone actors or small groups of like-minded individuals present a significant risk. These attacks can occur with little or no forewarning and we cannot guarantee preparations for such attacks will be detected.

In our 2017 stakeholder survey, stakeholders said our work in relation to the identification and investigation of terrorism-related security threats was highly regarded. They said our investigations provided an integral and vital service for their organisations and cited recent disruption operations as examples of our counter-terrorism successes.

Target achieved: security assessment regimes enable action by other agencies to prevent security risks to Australia PAGE 49

Target achieved: national security partners use our advice to disrupt travel of Australians or locally based support for terrorism overseas

During this reporting period, we issued security assessments that provided the basis for the Minister for Foreign Affairs to temporarily suspend passports and cancel or refuse passports for extremists who would otherwise have travelled to the conflict zone in Syria and Iraq.

We also issued adverse security assessments in relation to visas for individuals on the basis of terrorism concerns, which assisted DIBP to manage security risks in those cases (refer Activity 3: countering serious threats to Australia's border integrity).

Stakeholders said we had made a significant contribution to the disruption of individuals wishing to travel to the Middle East to join proscribed terrorist groups.

Measure	Results against targets	Refer
Effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security *Source: ASIO corporate plan 2016–17 (p. 16);* *Portfolio Budget Statement*	**Target achieved:** the Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice We provided comprehensive advice to support Australian Government counter-terrorism policies and responses, including in relation to the conflict in Syria and Iraq, the potential return of Australian foreign fighters to Australia, the government's citizenship loss policy, the Australia – New Zealand Counter Terrorism Committee's (ANZCTC) National Strategy for Crowded Places, countering violent extremism (CVE) programs, as well as security planning for major national and sporting events. We provided assessments to the Australian Government and partner agencies on emerging threats and trends impacting on the Australian and global security environment. We also delivered 76 briefings to government and industry partners on indicators of mobilisation to violence, building a greater collective awareness and understanding among stakeholders of terrorist behaviour. In addition to advice on counter-terrorism matters, we coordinated intelligence advice to support the Australian Government's responses to Australians who had been kidnapped overseas. Stakeholders said our intelligence and assessments were credible, influential and respected. The work of ASIO's NTAC was noted as being both influential and essential in assisting stakeholders to manage terrorism-related security risks. There was a desire from stakeholders for us to produce more 'preliminary assessments' in the immediate wake of domestic and international terrorist incidents. To address this feedback, NTAC developed a new line of reporting that captures information available primarily through media, provides preliminary assessments and outlines the work being undertaken by ASIO and the Australian Federal Police (AFP) in response to the incident.	PAGE 50
	Target achieved: law enforcement, border and other national security partners use our advice to manage and disrupt security risks During this reporting period, we provided advice to law enforcement partners that contributed directly to the disruption of three planned terrorist attacks as well as assisting with the disruption of other terrorist-related activities in Australia. We provided evidence to support counter-terrorism prosecutions in New South Wales, Victoria and Queensland. We also provided intelligence to international partners to disrupt attack planning in their countries. Our law enforcement stakeholders said our advice was effective and that recent counter-terrorism successes had been achieved as a result of our close collaboration with law enforcement.	PAGE 51
	Target achieved: business and industry adopt our security advice and are satisfied with their engagement Results for this target are reported against 'Activity 4: providing protective security advice to government and business'.	PAGE 39

Measure	Results against targets	Refer
Effective work with partners to generate tangible counter-terrorism effects for Australia and partner countries *Source: ASIO corporate plan 2016–17 (p. 16)*	**Target achieved:** partners can readily access our intelligence In 2016–17 we published 1433 intelligence reports for Australian partner agencies covering a range of terrorism, espionage, foreign interference and border security issues. Reporting was distributed to more than 130 federal, state and territory government organisations. We also shared reporting with over 130 foreign liaison partner agencies in 60 countries, with 643 intelligence reports released to one or more partner agencies. To support stakeholders and broaden the reach of our advice, where possible we produced versions of our highly classified reports at lower classification levels, including versions for industry stakeholders to inform their security arrangements. Stakeholders said our intelligence reports were accessible, with the exception of some reporting produced out-of-hours that was not as readily accessible to some stakeholders. Stakeholders acknowledged work was underway to address this issue. **Target achieved:** partners view joint operations with us as an effective way to achieve shared outcomes Our partners said we were an effective and valuable counter-terrorism partner. In addition to working effectively with our law enforcement partners—especially through JCTTs and the AFP-led National Disruption Group (NDG)—we supported the work of our intelligence partners by leading the prioritisation of the Australian Government's counter-terrorism intelligence activities. In recognition of the significant terrorist threat to Australian interests in South-East Asia, a particular focus for us during this reporting period was developing prioritisation and intelligence collection requirement documents to assist partners to prioritise their resources in South-East Asia. Internationally, we continued to work jointly with foreign partners on counter-terrorism operations, the exchange of intelligence and knowledge of terrorist threats and behaviours, and the development of technical and other capabilities to identify and counter threats.	PAGE 52 PAGE 52

2 Activity 2: countering espionage, foreign interference and malicious insiders

Measure	Results against targets	Refer
Effective identification and investigation of threats to Australia's security *Source: ASIO corporate plan 2016–17 (p. 17)*	**Target achieved:** new security leads are identified and consistently prioritised and pursued	PAGE 54

During this reporting period, we continued to identify and investigate harmful espionage and foreign interference directed against Australia. Due to the scale of the activities directed at Australia, we could not investigate all activities of potential concern. We rigorously prioritised our efforts, pursuing activities that represented the greatest potential harm to Australian interests.

Our analysis of reports received through the whole-of-government Contact Reporting Scheme (CRS) generated new leads into potential foreign intelligence activity.

Target partially achieved: security assessment regimes enable action by other agencies to prevent security risks to Australia — PAGE 54

Our personnel security assessments played a critical role in supporting the integrity of Australian Government business by providing advice to vetting agencies on the security implications of individuals being granted a security clearance. In 2016–17, we completed 27 182 assessments.

We did not meet key performance indicators agreed with the Australian Government Security Vetting Agency (AGSVA) as a result of the significant growth (129 per cent increase) in assessment demand for Top Secret positive vetting (PV) clearances. PV clearances are the most resource intensive for security assessment because of the need to provide a high level of assurance in relation to individuals accessing highly classified information and capabilities.

We worked closely with AGSVA during this reporting period to improve the efficiency of the security assessment process while maintaining an appropriate level of assurance in relation to vetting candidates. However, with further increases in vetting demand expected, additional resourcing will be required to provide the necessary assessment capacity.

This view was shared by our stakeholders, who considered our personnel security assessment work to be effective but in need of greater resourcing to meet demand.

Measure	Results against targets	Refer
Effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security *Source: ASIO corporate plan 2016–17 (p. 17);* *Portfolio Budget Statement*	**Target achieved:** the Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice	PAGE 56
	Target achieved: law enforcement, border and other national security partners use our advice to manage and disrupt security risks We published analytical reports, threat assessments and intelligence reports during this reporting period to assist the Australian Government and national security partner agencies to manage risks related to espionage, foreign interference and malicious insiders. We supported the Australian Government's foreign investment policy framework in 2016–17 by providing 265 assessments, through the Foreign Investment Review Board (FIRB) process, on the potential for a foreign power to conduct espionage, foreign interference or sabotage through its involvement in specific investments. We engaged extensively with federal, state and territory governments and industry on foreign investment issues, conducting 53 briefings during this reporting period. We also supported Australian Government decision-making on proposed policy and legislative reforms to counter the espionage and foreign interference threat to Australia, and the government's response to threats to Australia's defence industry. Australian Government and partner agency stakeholders said our advice on espionage, foreign interference and malicious insider threats was of a high quality. However, some felt that more resources should be devoted to the task, especially when compared with resources currently devoted to countering the terrorist threat. In relation to FIRB processes, stakeholders said our engagement and support to the FIRB was much improved, with better tailored and more nuanced assessments and effective support for FIRB members.	
	Target achieved: business and industry adopt our security advice and are satisfied with their engagement Results for this target are reported against 'Activity 4: providing protective security advice to government and business'.	PAGE 39

Measure	Results against targets	Refer
Effective work with partners to counter clandestine foreign activity *Source: ASIO corporate plan 2016–17 (p. 17)*	**Target achieved:** partners can readily access our intelligence In 2016–17, we published a total of 1433 intelligence reports for Australian partner agencies covering a range of terrorism, espionage, foreign interference and border security issues. Reporting was distributed to more than 130 federal, state and territory government organisations. We also shared reporting with over 130 foreign liaison partner agencies in 60 countries, with 643 intelligence reports released to one or more partner agencies.	PAGE 57
	Target achieved: partners view joint operations with us as an effective way to achieve shared outcomes We continued in 2016–17 to cooperate closely with national and international security partners, improving our shared knowledge of hostile foreign intelligence service activities and our capabilities to counter the threat.	PAGE 57

3 Activity 3: countering serious threats to Australia's border integrity

Measure	Results against targets	Refer
Effective identification and investigation of threats to Australia's security *Source: ASIO corporate plan 2016–17 (p. 18)*	**Target achieved:** new security leads are identified and consistently prioritised and pursued	PAGE 59

We supported the identification of threats to Australia's border integrity by contributing intelligence on persons of security concern, who may seek to travel to or remain in Australia, to the travel alert systems managed by DIBP and the Australian Border Force (ABF).

We commenced projects with DIBP to improve the efficiency and effectiveness of travel alert processes, including through automation of aspects of the alert listing, management and notification process.

Our border security stakeholders said we were a valued and capable partner that is effective in identifying and assessing threats to Australia's border integrity. Collaboration on counter-terrorism–related border threats was perceived as being at an all-time high. They said shared investment in ICT systems had facilitated more effective engagement between us but considered more work was needed to address other shortfalls in ICT connectivity. Work to address these issues was continuing at the end of this reporting period.

Target achieved: security assessment regimes enable action by other agencies to prevent security risks to Australia — PAGE 59

We conducted visa, citizenship and other border-related security assessments to inform the management of security risks by DIBP, AusCheck, AFP and other agencies in relation to the granting or retention of a visa, the granting of citizenship, and access to security-controlled areas and substances. During this reporting period we completed:

- 14 358 visa security assessments;
- 132 088 access security assessments relating to border security, most of which related to applicants for Aviation Security Identification Cards (ASIC) or Maritime Security Identification Cards (MSIC); and
- 9696 access security assessments relating to sensitive chemicals, biological agents or nuclear sites.

Stakeholders said we had been effective in the provision of security assessments.

Measure	Results against targets	Refer
Effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security *Source: ASIO corporate plan 2016–17 (p. 18);* *Portfolio Budget Statement*	**Target achieved:** the Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice	PAGE 61
	Target achieved: law enforcement, border and other national security partners use our advice to manage and disrupt security risks We provided advice and assessments to support the Australian Government's border security policies, including in relation to the intake of an additional 12 000 refugees from Syria and Iraq and the agreement between the Australian and United States governments to resettle detainees from Manus Island and Nauru facilities. We also continued to support national security partner agencies through our contribution to OSB by identifying individuals involved in maritime people-smuggling networks and supporting disruption activities. Stakeholders said we had been effective in providing advice on border security–related policy and legislative issues.	
We support DIBP to meet its migration program and refugee and humanitarian resettlement goals *Source: ASIO corporate plan 2016–17 (p. 18)*	**Target achieved:** security advice to DIBP is timely and meets the agreed service level agreements and is responsive to DIBP's other priorities We worked closely with DIBP to successfully meet the terms of our service level agreement and its migration program priorities. As part of this work, we reformed our visa security assessment business processes and implemented a new case management system which reduced a large number of cases by the end of this reporting period. DIBP welcomed our effective implementation of these reforms.	PAGE 62

4 Activity 4: providing protective security advice to government and business

Measure	Results against targets	Refer
We provide effective protective security advice, reporting and services that inform security by design by government, business, and industry *Source: ASIO corporate plan 2016–17 (p. 19)*	**Target achieved:** our expertise and advice informs security policies and approaches within government agencies, business and industry	PAGE 63
	Target achieved: business and industry adopt our security advice and are satisfied with their engagement	
	Target achieved: protective security resources are directed at protecting the assets, infrastructure and systems judged by us to be most at risk	

We continued, through our BGLU, to provide risk management decision-makers in government and industry with the most current intelligence on security threats and protective security advice. BGLU's secure website made intelligence-backed reporting available to over 2000 subscribers, with an almost equal subscription by government and industry. Sixty-four reports were published on the website during this reporting period.

BGLU also coordinated nine industry briefings on security threats to aviation, places of mass gathering, defence industry, energy and resources, mass passenger transport, communications, and banking and finance. We consulted closely with stakeholders to ensure briefings met the requirements of attendees and responded to their highest priority issues.

ASIO–T4 protective security advice remained in high demand, and a new intelligence-led prioritisation model was adopted to ensure our advice supported the assets, infrastructure and systems most at risk from terrorism, espionage and foreign interference–related threats.

ASIO–T4 provided a range of advice during this reporting period including 179 security product evaluations, 80 Zone 5 (Top Secret) facility inspections, technical surveillance countermeasures (TSCM) inspections, four protective security training courses and a range of protective security publications which were posted on the Govdex and BGLU websites.

Stakeholders said our protective security advice, reporting and services were highly regarded. In particular, the BGLU, NTAC and ASIO–T4 were recognised as sources of authoritative protective security advice. Briefings by senior ASIO officers were highly sought after and their presentations were viewed as being appropriate, balanced, informative and often very influential. Our industry briefing days were highly valued by stakeholders.

Measure	Results against targets	Refer
	Target achieved: the annual program of physical security certifications is achieved	PAGE 65
	We met all Zone 5 physical security certification inspection requests during this reporting period. Eighty inspections were conducted, with 39 certifications issued and advice provided in other cases on measures needed to meet certification requirements.	

5 Activity 5: collecting foreign intelligence in Australia

Measure	Results against targets	Refer
We provide intelligence that is useful to progress Australia's national security, foreign relations, or economic wellbeing *Source: ASIO corporate plan 2016–17 (p. 20)*	**Target achieved:** we are responsive to the requirements of our clients The details of our performance in relation to this activity are classified and reported separately in our classified annual report.	PAGE 67

Measures across all activities

Measure	Results against targets	Refer
The safety of our staff is maintained *Source: ASIO corporate plan 2016–17 (p. 14)*	**Target achieved:** our senior leaders continue to be exemplars and drive a work culture, systems, and individual conduct which promote officer safety During this reporting period, we appointed our Deputy Director-General for Counter-Terrorism as ASIO's Senior Safety Officer to provide improved leadership and coordination of staff safety programs within ASIO. Staff safety initiatives pursued by our Senior Safety Officer and other senior leaders included the reviewing and updating of a range of safety-related policies and procedures, the establishment of an officer safety portal on our intranet (a one-stop shop for officer safety information) and the launch of a counter-terrorism innovation hub to support new ideas for improving processes in ASIO, including in relation to officer safety.	PAGE 68
	Target achieved: we maintain high levels of work health and safety capacity, and provide ongoing training of staff We maintained a high level of work health and safety (WHS) capacity through a comprehensive suite of WHS-related training programs, staff health and wellbeing programs and our health and safety representative network. An internal audit of our rehabilitation management system, processes and outcomes confirmed our compliance with the Safety, Rehabilitation and Compensation Act 1988 and Comcare's Guidelines for Rehabilitation Authorities 2012. No areas of non-compliance were identified.	PAGE 68
Legality and propriety of our activities and effectiveness of our engagement with oversight and accountability bodies *Source: ASIO corporate plan 2016–17 (p. 14)*	**Target achieved:** our senior leaders continue to be exemplars and drive a work culture, systems, and individual conduct that are legal, ethical, and respectful of human rights Our senior leaders continued to convey their expectations of staff conduct that is legal, ethical and respectful of human rights, including reinforcing this expectation during their direct involvement in training programs, and through their support for the involvement of the IGIS and ASIO Ombudsman in staff training. Our senior leaders also conducted an annual review of the human rights performance of our foreign security and intelligence service counterparts, to ensure we take due regard of human rights in our cooperation with foreign partners.	PAGE 70

Measure	Results against targets	Refer
	Target achieved: we proactively engage with oversight and accountability bodies and provide as much information as possible for use in the public domain We engaged extensively with a range of oversight and accountability bodies, including the Parliamentary Joint Committee on Intelligence and Security (PJCIS), Senate Legal and Constitutional Affairs Committee, IGIS, Independent National Security Legislation Monitor (INSLM), and Independent Reviewer of Adverse Security Assessments. We provided classified and unclassified submissions and appeared publicly and in private hearings to support the work of these bodies (outlined further in the 'External scrutiny' section of our annual report).	PAGE 71
The security of our activities *Source: ASIO corporate plan 2016–17 (p. 14)*	**Target achieved:** our senior leaders continue to be exemplars and drive a work culture, systems, and individual conduct which embody security Our senior leaders continued to drive a culture of security, in particular through our Security Committee which oversaw our security policies and practices and ensured security risk management best practice was incorporated into all aspects of our business.	PAGE 71
	Target achieved: we continue to meet the requirements of the Australian Government's Protective Security Policy Framework We continued to manage the security of our people, information and assets in line with the requirements of the Protective Security Policy Framework (PSPF).	PAGE 71

Analysis of performance

Overall, we performed effectively in 2016–17 across all key activities that contribute to our purpose: to protect the nation and its interests from threats to security through intelligence collection and assessment, and to provide advice to the Australian Government, government agencies and business. This assessment was supported by our 2017 stakeholder survey—conducted by an independent person with extensive national security experience.

The survey comprised 66 interviews with stakeholders from 64 federal, state and territory government and industry organisations. It concluded that without exception, ASIO is regarded as an effective, capable and reliable partner offering high-quality and largely unique services.

Our close engagement and integration of effort with national and international security partners contributed directly to counter-terrorism, counter-espionage and border security successes during this reporting period, which included:

- the disruption of three planned terrorist attacks targeting people in Australia and other terrorist-related activities, including attempted travel by Australian extremists to the conflict zone in Syria and Iraq; and
- the identification and degradation of harmful espionage and foreign interference directed against Australia, and an increase in government, industry and public awareness of these activities.

Ongoing work within government to prioritise intelligence and operational efforts across Australia's national security agencies improved the effectiveness and efficiency of the national response. We contributed to this work by coordinating the prioritisation of Australia's counter-terrorism intelligence efforts. We also worked within ASIO to streamline our business practices and adopted a rigorous 'intelligence-led' approach across all activities to ensure our efforts were focused on areas of most significant security risk, as well as to assist us to meet the terms of service-level agreements such as those relating to visa security assessments.

Despite these successes there remained considerable risk across our investigative caseload and significant resourcing pressures in some areas of our business. These pressures had an impact on our performance during 2016–17 and will continue to do so in 2017–18.

Counter-terrorism

During this reporting period, we managed a counter-terrorism caseload which was significantly higher than our historical average, with a large number of cases involving high levels of risk, including planning for attacks in Australia. The nature of the threat and operating environment exacerbated the challenge presented by the volume of work.

- Easily accessible Islamist extremist English-language propaganda calling for and justifying terrorist attacks in Western countries—including Australia—continued to widen the potential number of individuals and groups that are inspired by it.
- Low-capability lone-actor attacks require little preparation and can move from concept to execution very quickly.

It is therefore not always possible for intelligence and law enforcement agencies to detect attack preparations or respond in time to prevent attacks.

- While low-capability attacks have become more common, more complex attacks also remained a significant threat—as demonstrated by the disrupted December 2016 attack plan in Melbourne and the July 2017 attempt to place an improvised explosive device on a plane leaving Australia.
- Rapid technological development and the increasing use of encrypted communications devices by individuals planning attacks impacted on intelligence and law enforcement agencies' efforts to detect their activities.

We routinely prioritised our efforts and allocated resources to address the areas of most significant security risk. However, this provided us limited scope to address a range of other known or emerging risks.

We will need to further develop our counter-terrorism capabilities to ensure we continue to achieve our purpose in the years ahead and to meet stakeholder expectations.

Counter-espionage and foreign interference

While we had a number of successes in identifying and degrading the harmful effects of espionage and foreign interference, the scale of the threat to Australia and its interests is unprecedented.

The heightened terrorist threat this past decade, which has been further elevated in Australia since 2014, has limited our scope to redirect resources towards counter-espionage and foreign interference. At the end of this reporting period, we were no longer meeting key performance indicators for personnel security assessments as agreed to with AGSVA. Stakeholders commented that more resources should be devoted not only to personnel security assessments in particular, but also to our broader counter-espionage and foreign interference efforts more generally. This will be a major focus for ASIO in the coming years.

While close collaboration with national and international partners, stronger prioritisation of effort and improvements to business processes have improved the effectiveness of our current counter-espionage responses, an overall increase in the scale of our response is required to better address the threat to Australia's interests.

Increasing costs of doing business

Changes in the security and operating environments drove up the costs of doing business during this reporting period, affecting the conduct of our operations and resourcing available for operational activities. In the current heightened threat environment, intelligence and law enforcement personnel are terrorist targets. We redirected resources to ensure the safety of our operational activities, enhance our building security and provide safety training for staff.

Rapid changes in technology and the widespread adoption of encrypted communication devices by our targets also affected our resourcing and operations. Developments in technology will continue to affect our performance.

Increasing demand for advice and services

While our stakeholders said we were an effective partner that provided high-quality advice, many across both government and industry were seeking even higher levels of tailored engagement and collaboration. This is driven by the heightened threat environment in Australia, the range of security threats now affecting the work of our stakeholders, and a desire for their responses to these threats to be informed by our security intelligence advice and expertise.

During this reporting period we prioritised our advice and services for stakeholders by consulting them on their priorities and focusing on the areas of greatest security risk. We will need to continue this approach and manage expectations of what is possible with our current resourcing, which will remain overextended responding to the significant threats to Australia's national security.

Report on financial performance

4

In 2016–17, we effectively managed our expenditure in a challenging operating environment, with unprecedented levels of security threat, high investigative workloads and stakeholder demands, and increasing business costs placing considerable pressure on ASIO's resources and financial sustainability.

We achieved a small surplus of $2.5 million (excluding depreciation), which represents 0.6 per cent of our budget. This result would have broken even except for favourable interest rate movements that had a positive impact on the accounting required under Australian Accounting Standards Board (AASB) standard AASB119 in relation to employee leave provisions. Interest rate movements also had a significant impact on the previous financial year's result, which was an operating loss of $5.4 million ($4.4 million due to interest rate movement).

The 2016–17 financial year was the third year of the new policy proposal, *Enhancing security intelligence capabilities to counter the Islamist terrorism threat*. During 2016–17, we received $45.3 million in operating funding and an equity injection of $14.1 million for capital activities. Ongoing annual funding from 2017–18 of $52.0 million in operating and $13.5 million in capital is expected for this measure. Additionally, during the 2016–17 reporting period, we received final operating funding of $0.6 million relating to the *Syrian and Iraqi humanitarian crises* new policy proposal. This additional funding made an important contribution to our efforts to identify and investigate counter-terrorism threats during this reporting period.

However, there are significant resourcing pressures in other areas of our work (refer 'Annual performance statements') that will be exacerbated by changes to our budget over the forward estimates.

We will continue to contribute to Australian Government savings measures, including the efficiency dividend, which will have a significant impact on ASIO's Departmental Capital Budget (DCB), 2017–18 operating budget, and across the forward estimates ($65.5 million).

Our DCB will remain under particular pressure as we work to replace assets that provide the capability needed to operate effectively in a rapidly changing security and technological environment. These rapid changes contributed to an increase in our capital expenditure in 2016–17, a trend that we expect to continue over the forward estimates. While our DCB will increase from $28.1 million in 2016–17 to $68.6 million next financial year as a result of the previous year's appropriation re-phasing, from 2019–20 it will stabilise at a lower figure of approximately $44 million annually, which includes $13.5 million from the *Enhancing security intelligence capabilities to counter the Islamist terrorism threat* new policy proposal.

We will continue to identify and implement efficiencies and rigorously prioritise our activities to ensure we operate within future budget allocations. However, further consideration will be given during 2017–18 to the sustainability of our current operations in light of our projected DCB and operating budget, and our anticipated future operating environment.

A table summarising ASIO's total resources for 2016–17 is provided at Appendix A. Our total payments for this reporting period are at Appendix B.

Performance narrative

1	Activity 1: countering terrorism and the promotion of communal violence
Measure	Effective identification and investigation of threats to Australia's security
Target	New security leads are identified and consistently prioritised and pursued

Identification of leads

Our intelligence discovery efforts over this reporting period contributed to the disruption of planned terrorist attacks in Australia and identified terrorism-related linkages between Australia and the Syria–Iraq conflict area. During 2016–17, we received over 12 000 leads[4] and resolved or investigated approximately 15 000 lead referrals.

The discovery of lead intelligence—through the continuous review of incoming all-source intelligence reporting and information to identify non-obvious connections, patterns, trends and anomalies as well as new investigative and operational opportunities—is more critical than ever in the current security environment, where the timeline for an individual to mobilise towards conducting a terrorist attack can be very short.

During this reporting period, we commenced lead discovery projects to proactively identify unknown individuals who may pose a terrorism-related threat.

To provide greater consistency in the way lead referrals are processed between ASIO and federal, state and territory law enforcement partners, we published our counter-terrorism leads triage and assessment framework. The framework uses terminology that aligns with the ANZCTC operational threat assessment guidelines, and the counter-terrorism person of interest prioritisation tool guidelines.

[4] Lead information refers to all information received that may contain security indicators relating to politically motivated violence and promotion of communal violence as defined in the ASIO Act. This includes referrals from the National Security Hotline, calls to ASIO's public line, write-ins, information provided by ASIO's human sources as well as government, private sector and foreign liaison reporting.

Counter-terrorism investigations

The volume and tempo of our counter-terrorism investigations and operations remained high during 2016–17, at a rate significantly higher than the historical average.

This high tempo is expected to continue, with no significant reduction in the current terrorist threat to Australia and Australian interests expected in the coming years. As a result, we continued work during this reporting period to refine our prioritisation process to ensure investigative resources remained focused on the most significant threats.

Although our investigations contributed to three successful disruptions, there remained a high level of risk in our investigative caseload which has continued beyond this reporting period.

- Lone actors or small groups of like-minded individuals can mount low-capability attacks with little or no forewarning.
- The use of encrypted communication devices and other secure communications practices can obscure the activities of group members.

We are continuing to work with our national and international counter-terrorism partners to mitigate these risks. However, given the nature of the current threat and operating environment, the risks cannot be completely eliminated.

Targets	Security assessment regimes enable action by other agencies to prevent security risks to Australia National security partners use our advice to disrupt travel of Australians or locally based support for terrorism overseas

In 2016–17, our security assessments supported the Department of Foreign Affairs and Trade's (DFAT) recommendations to the Minister for Foreign Affairs to temporarily suspend passports and cancel or refuse passports for extremists who otherwise would have travelled to engage in the conflict in Syria and Iraq. We also issued adverse security assessments in relation to visas for individuals on the basis of terrorism concerns, which assisted DIBP to manage security risks in those cases (refer Activity 3: countering serious threats to Australia's border integrity).

Measure	Effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security
Target	The Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice

During this reporting period we provided advice to support the Australian Government's counter-terrorism policies and responses. This included:

- providing advice to support policy development in relation to the conflict in Syria and Iraq, the government's response to the use of encrypted communication devices by individuals of security concern, national counter-terrorism response arrangements, national security legislative amendments, and Australia's counter-terrorism engagement in South-East Asia;
- providing advice to support implementation of the Australian Government's citizenship loss policy under the Australian Citizenship Amendment *(Allegiance to Australia) Act 2015*;
- supporting the Australian Government's planning in relation to Australian foreign fighters who may return to Australia, including by providing threat assessments on returnees that determine the level of government response to their return;
- contributing to the development of the ANZCTC National Strategy for Crowded Places, including through the production of a specific threat assessment on crowded places in March 2017;
- supporting Australian Government security planning for Anzac Day commemorations and major sporting events such as the Rio Olympics, international cricket, the 2017 Rugby League World Cup and Gold Coast 2018 Commonwealth Games; and
- supporting the Australian Government's CVE policies by providing tailored intelligence assessments to help build and support CVE programs and capabilities.

In addition to supporting the Australian Government's responses to terrorism-related issues, we played a coordination role in relation to the provision of intelligence on Australians who had been kidnapped overseas. We regularly convened multi-agency intelligence working groups to collate relevant intelligence, share assessments and set information collection requirements for agencies.

Our advice and published intelligence assessments also informed the Australian Government's broader understanding of local and international terrorist threats and potential implications for Australian interests globally. We provided assessments on emerging threats and trends impacting on the Australian and global security environment, including:

- emerging terrorist methodologies observed in offshore attacks with the potential to motivate similar attacks in Australia and overseas;
- foreign fighters returning from the Syria–Iraq conflict to Australia and our region;
- mental health factors in counter-terrorism; and
- linkages between crime and terrorism (joint assessments with the Australian Criminal Intelligence Commission).

We delivered 76 briefings to Australian Government and industry partners on indicators of mobilisation to violence, to build a collective understanding of terrorist behaviour. These briefings directly supported whole-of-government counter-terrorism efforts and we received strong, positive feedback from across government and industry on their value and utility.

Throughout this reporting period we implemented new, innovative ways to deliver influential advice, including through the use of information graphics to communicate complex advice and data. We received positive feedback from Australian Government partners on these initiatives and on the value and relevance of our reporting.

Target	Law enforcement, border and other national security partners use our advice to manage and disrupt security risks

In 2016–17, our intelligence and threat advice directly supported our law enforcement partners in disrupting three planned terrorist attacks in Australia. These disruptions included the arrest of:

- four individuals in Melbourne on 22 December 2016, who were charged with acts in preparation for, or planning of, a terrorist attack;
- two 16-year-olds in Sydney on 12 October 2016, who were charged with acts done in preparation for, or planning of, a terrorist act, and membership of a terrorist organisation; and
- an extreme right-wing identity on 6 August 2016, who was charged with acts done in preparation for, or planning of, a terrorist act and membership of a terrorist organisation.

We worked closely with law enforcement partners to disrupt or contain other terrorism-related threats in Australia.

In addition to supporting the disruption of attack planning in Australia, we provided intelligence to international partners to disrupt attack planning in their countries.

We also had an ongoing role in assisting counter-terrorism prosecution in New South Wales, Victoria and Queensland, including providing evidence on telecommunications intercepts, physical surveillance, listening and tracking devices whilst protecting our capabilities from public disclosure.

Measure	Effective work with partners to generate tangible counter-terrorism effects for Australia and partner countries
Target	Partners can readily access our intelligence

In 2016–17, we published a total of 1433 intelligence reports for Australian partner agencies covering a range of terrorism, espionage, foreign interference and border security issues. Reporting was distributed to more than 130 federal, state and territory government organisations. We also shared reporting with over 130 foreign liaison partner agencies in 60 countries, with 643 intelligence reports released to one or more partner agencies.

We engaged continuously with our stakeholders during this reporting period to ensure we delivered the right products to the right people, in the right way and at the right time. To support stakeholders and broaden the reach of our advice, we produced versions of highly classified reports at lower classification levels when possible. This included producing 'For Official Use Only' reports for industry stakeholders to inform their security posture. We also tailored our report delivery arrangements to ensure our reporting was received by stakeholders in the most timely and efficient manner.

Target	Partners view joint operations with us as an effective way to achieve shared outcomes

Our national and international partners continued during this reporting period to regard us as a valuable counter-terrorism partner.

Counter-terrorism intelligence coordination

As part of the Australian Government's counter-terrorism governance arrangements, we lead the counter-terrorism intelligence mission. In 2016–17, this role included developing a number of prioritisation and collection requirements mechanisms that were used by other agencies to prioritise their resources against terrorist threats that could affect Australian interests. Our joint work with partners on prioritisation strengthened our efforts to achieve shared counter-terrorism outcomes.

A particular area of focus during this reporting period has been the terrorist threat within South-East Asia. We coordinated the development of biannual information requirements and strategic disruption priorities, which were used to prioritise partners' resources in South-East Asia.

National partners

We worked closely with the AFP and state and territory police in JCTTs to ensure a coordinated approach to combating terrorism in Australia. Our intelligence was used to inform, support and drive JCTT operational activities, including the disruption of planned terrorist attacks in Australia during this reporting period (refer 'Law enforcement, border and other national security partners use our advice to manage and disrupt security risks' target).

We also contributed to the AFP-led NDG. During this reporting period, our intelligence contributed to the establishment of a significant NDG investigation and subsequent disruption.

International partners

Our international counterparts also continued to perceive us as a valuable partner. In 2016–17, we were authorised by the Attorney-General to cooperate with over 350 agencies in 130 countries. During this reporting period we:

- cooperated closely with partners to improve our shared understanding of terrorist behaviour, including by exchanging information on specific terrorist incidents and different methodologies used to study terrorist behaviour; and
- were invited to participate in, and contributed to, international forums on horizon scanning for future terrorist threats.

Technical partnerships

As the lead Australian Government agency for telecommunications interception technical advice, we worked with and on behalf of our partners to ensure data derived from legal interception activities in Australia was consistent and reliable.

To strengthen our shared response to terrorism threats, we continued to work closely with national and international partners on the development of technical collection capabilities and the sharing of data on threats.

Activity 1: stakeholder views on performance

Stakeholders said that we were highly regarded in relation to the identification and investigation of terrorism-related security threats. Our investigations and threat assessments form an integral and vital service for many of the stakeholders interviewed. Senior officials, including police officers, were strong in their praise for the effectiveness of our work, citing a number of recent operations as examples of our counter-terrorism successes. Many of the successes were achieved through our close collaboration with partner agencies.

Favourable mention was made of our significant contribution to the disruption of those wishing to travel to the Middle East to join proscribed terrorist groups.

Stakeholders said our intelligence and assessments were credible, influential and respected. The work of NTAC was noted as being both influential and essential in assisting stakeholders to manage counter-terrorism–related security risks. The reporting we distribute from our overseas counterparts is also highly regarded.

Our intelligence reports were considered to be accessible, with the exception of some reporting produced out of hours that was not as readily accessible to all stakeholders. Stakeholders acknowledged this issue was being addressed.

There was a desire from stakeholders for an increase in preliminary assessments in the immediate wake of domestic and international terrorist events, to fill a void that is otherwise covered by mainstream and social media. This desire reflected stakeholders' needs to have confidence that threat levels for Australia and Australian interests overseas were appropriate and being reviewed. Stakeholders who sought this additional reporting recognised the practical difficulties of producing such assessments soon after an event, when facts were still being established and investigations only just commencing.

2 Activity 2: countering espionage, foreign interference and malicious insiders

Measure	Effective identification and investigation of threats to Australia's security
Target	New security leads are identified and consistently prioritised and pursued

During 2016–17, we continued to identify and investigate espionage and foreign interference activity directed against Australia. These activities included:

- espionage focused on accessing classified or privileged information about Australia's alliances; partnerships; positions on international diplomatic, economic and military issues; energy and mineral resources; and innovations in science and technology; and
- attempts to clandestinely influence public and official opinions and decision-making, including by interfering in migrant communities within Australia.

We could not respond to all espionage and foreign interference—the scale of hostile intelligence activity being directed against Australia is unprecedented. Therefore, we continued during this reporting period to rigorously prioritise our efforts by focusing on the activities assessed to represent the most harm to the nation's interests.

Contact reporting scheme

The whole-of-government CRS, managed by ASIO, continued in 2016–17 to provide leads into potential espionage and hostile foreign intelligence activity directed against Australia, including attempts to cultivate or recruit Australian Government employees.

The contact reports contained unique leads relevant to national security that would not otherwise have been identified, which were subject to further investigation.

Target	Security assessment regimes enable action by other agencies to prevent security risks to Australia

We finalised 27 182 security assessments during 2016–17 in relation to Australian Government personnel, and others who require access to nationally classified, sensitive and privileged government information and areas. The security clearance regime plays a critical role in protecting the integrity of Australian Government business, providing a defence against a range of security threats including espionage, foreign interference, malicious insiders and terrorism.

The demand for security assessments increased five per cent overall during this reporting period. However, within that caseload there was a 129 per cent increase in requests for assessments for Top Secret PV clearances—from 975 in 2015–16 to 2234 in 2016–17. These PV assessments were considerably more resource intensive than other assessments, given the requirement to provide a higher level of assurance to the government regarding the protection of the most highly classified national security information and capabilities.

We implemented a range of efficiency initiatives, informed by risk assessments, to manage the high PV caseload. This allowed us to complete 57 per cent more PV cases in 2016–17 than were completed during the previous reporting period. However, due to the volume and complexity of the caseload, there was an overall 13 per cent decrease in security assessment completions across all categories, year on year. As a result, we were unable to meet key performance indicators agreed with AGSVA.

During this reporting period we worked closely with AGSVA on initiatives to improve the efficiency of the security assessment process while maintaining an appropriate level of assurance in relation to vetting candidates. We:

- contributed, at the planning stage, to the Defence Vetting Transformation Program, a major project that will deliver improvements and efficiencies for personnel security vetting;
- integrated an AGSVA secondee within ASIO's personnel security assessment team to help identify efficiencies;
- allocated additional resources to triage security assessment referrals and to finalise less complex cases; and
- introduced a new 'personnel security assessments' case type within our case management system to further improve oversight of our assessments caseload.

These measures have enhanced the efficiency of the personnel security assessment process. However, an overall increase in our assessments capacity will be required to meet projected further increases in demand for assessments arising from implementation of policies that will require an increase in the number of individuals requiring higher level security clearances. These policies include growth in Defence and defence industry associated with the implementation of the Defence integrated investment plan; and implementation of measures from the 2017 Independent Intelligence Review.

In addition to the provision of personnel security assessments, we raised awareness across the Australian Government of techniques employed by foreign intelligence services, manifestations of espionage and foreign interference, and the associated risks as they relate to personnel security. We also increased the number of our defensive security briefings to clearance holders with personal factors that potentially heighten their susceptibility to foreign intelligence service exploitation. These briefings improved their security awareness and understanding of threats and reiterated clearance holder obligations, including responsibilities under the CRS.

Measure	Effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security
Targets	The Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice Law enforcement, border and other national security partners use our advice to manage and disrupt security risks

We published analytical reports, threat assessments and intelligence reports during this reporting period to provide advice to the Australian Government and partners on the threat posed by espionage, foreign interference and malicious insiders.

In particular, we published the report *Global threat from foreign intelligence services* in September 2016. This assessment provides a foundational understanding for all government departments about the threat posed by hostile foreign intelligence services.

During this reporting period we conducted an extensive program of defensive briefings for stakeholders in government and industry to increase awareness of this threat. This included the provision of specific briefings for Australian Government and state politicians on foreign interference and risks while travelling overseas.

Our assessments and advice directly informed Australian Government decision-making during this reporting period, including in relation to a significant package of policy and legislative reforms to deal with the espionage and foreign interference threat to Australia.

This will increase the Australian Government's ability to mitigate the current espionage and foreign interference threat by providing further deterrents to agents of foreign powers or those contemplating engaging in these activities.

National security implications of foreign investment

We supported the Australian Government's foreign investment policy framework throughout 2016–17 by providing assessments—through the FIRB process—on the potential for a foreign power to conduct espionage, foreign interference or sabotage through its involvement in specific investments.

We completed 265 assessments of FIRB referrals during the review period. The proportion of assessments within this caseload considered complex—that is, involving investment proposals of a topical or sensitive nature—increased this reporting period.

We engaged extensively with federal, state and territory governments and industry on foreign investment issues, conducting 53 briefings during this reporting period.

We supported the work of the multi-agency Critical Infrastructure Centre, based within the Attorney-General's Department (AGD), by seconding an ASIO officer to the centre and providing advice and tailored assessments to support the centre's risk assessments and policy advice.

Telecommunications sector security

In 2016–17, we continued to work closely with telecommunications companies regarding the security risks associated with the use of certain companies in their supply chains and risks arising from foreign ownership arrangements. We provided sensitive briefings to the Australian Government and the telecommunications sector to outline the threat and, where possible, recommended appropriate mitigation measures.

Australian Defence Industry Security Assurance Review

During this reporting period, the Director-General of Security commissioned a review to identify security vulnerabilities within Australia's defence industry and to make recommendations to mitigate identified risks. The review was conducted to support the Australian Government's policy commitment to invest significantly in defence capabilities over the coming decade, with a view to providing greater assurance to the government in relation to its investment, and to the Australian Defence Force in relation to the integrity of its capabilities.

The joint ASIO – Department of Defence review found that the existing policies and frameworks in place to secure classified technologies within Defence and defence industry were strong and well established.

The review formed the basis of our advice to the Australian Government on the foreign intelligence services threat to Australia's defence industry, the measures already in place to mitigate security risks, and additional measures to enhance the response to the threat.

Measure	Effective work with partners to counter clandestine foreign activity
Target	Partners can readily access our intelligence

In 2016–17, we published a total of 1433 intelligence reports for Australian partner agencies covering a range of terrorism, espionage, foreign interference and border security issues. Reporting was distributed to more than 130 federal, state and territory government organisations. We also shared reporting with over 130 foreign liaison partner agencies in 60 countries, with 643 intelligence reports released to one or more partner agencies.

Target	Partners view joint operations with us as an effective way to achieve shared outcomes

We continued during this reporting period to cooperate closely with national and international security partners, improving our shared knowledge of hostile foreign intelligence service activities and capabilities to counter the threat.

We collaborated with a range of international security partners on the identification of foreign investments that raise potential security issues.

Activity 2: stakeholder views on performance

There was generally a high level of confidence among our stakeholders that counter-espionage and foreign interference–related leads are being identified and pursued. However, in contrast with our counter-terrorism efforts, stakeholders know little about our work in this area. Most stakeholders said they understood the sensitivity of our counter-espionage operations and the difference between the higher levels of sophistication of the state-based espionage threat when compared with potential homegrown terrorists.

Stakeholders commented on the high quality of our security advice for countering espionage, foreign interference and the threat from malicious insiders. Some felt, however, that more resources should be devoted to the task, especially when compared with the resources currently devoted to countering the terrorist threat.

Stakeholders noted that our engagement and support to the FIRB was much improved, with better tailored and more nuanced assessments and effective support for FIRB members, including through briefing programs conducted at our headquarters building.

Our security assessment work was perceived by stakeholders as being generally effective. However, among the security vetting community, there was the strongly held view that we need to increase resourcing for our security assessments work to meet personnel security vetting demands.

3 Activity 3: countering serious threats to Australia's border integrity

Measure	Effective identification and investigation of threats to Australia's security
Target	New security leads are identified and consistently prioritised and pursued

We continued to support the identification of threats to Australia's border integrity by contributing intelligence on persons of security concern who may seek to travel to or remain in Australia, to the travel alert systems managed by DIBP and ABF. The alerts generated by these systems provided leads into activities of potential security concern, which we prioritised, assessed and, where appropriate, further investigated to determine the nature of the threat to Australia's security.

We also pursued projects to improve the efficiency and effectiveness of our travel alert–related activities, including:

- the commencement of two projects with DIBP to automate aspects of the alert listing, management and notification process, which are scheduled for completion during 2017–18; and
- the deployment of an enhanced case management system, which has improved work-flow management and oversight of our travel alert activities.

Target	Security assessment regimes enable action by other agencies to prevent security risks to Australia

We undertook visa, citizenship and other border-related security assessments to inform the management of security risks by DIBP, DFAT and other agencies in relation to the granting or retention of a visa, the granting of citizenship, and access to security-controlled areas at airports and ports. Assessments were undertaken either in response to requests from those agencies or on the basis of indicators of security concern that we identified in the course of our other activities.

We issued adverse security assessments when we assessed an individual posed a direct or indirect threat to security. Qualified security assessments were issued in circumstances where we possessed information that was, or could be, prejudicial to the interests of a person in relation to an administrative action by another agency—such as the granting of a visa—but did not make a prejudicial recommendation.

Visa security assessments

In 2016–17, we furnished 14 358 visa security assessments (refer Table 1). A refinement of our visa security assessment processes contributed to a reduction in the number of visa applications referred to us for assessment, and enabled us to redirect resources to higher risk cases. This refinement process will continue throughout 2017–18.

Type of entry	Number of assessments completed 2016–17[5]
Temporary visas	3782
Permanent residence and citizenship	2248
Onshore protection (air)	212
Offshore refugee/humanitarian	2265
Illegal maritime arrivals	546
Other referred visa caseloads	5305
TOTAL	14 358

Table 1: ASIO visa security assessments by type

The majority of border-related security assessments we conducted resulted in a non-prejudicial security assessment. In 2016–17, we furnished a small number of adverse and qualified border-related assessments, most of which were provided on the basis of concerns relating to politically motivated violence. A small number were furnished on the grounds of foreign interference concerns and people smuggling.

4 Security assessments for access to security-controlled places and substances

Our access security assessments are focused on supporting decision-making by partner agencies in relation to providing individuals access to:

- security-controlled places, such as sensitive air or maritime port areas or facilities or areas associated with special events—for example, the upcoming 2018 Gold Coast Commonwealth Games; and
- security-sensitive chemicals, biological agents or nuclear sites.

In 2016–17, we completed 132 088 access security assessments relating to border security, most of which involved providing advice to AusCheck, within AGD, on applicants for ASICs or MSICs.

We also completed 9696 access assessments in relation to security-sensitive chemicals, biological agents or nuclear sites. The majority of these assessments related to access to security-sensitive ammonium nitrate, which may be used in explosives or research activities or in the agriculture industry. We provided these assessments to the AFP to inform decision-making by states and territories under licensing arrangement principles agreed to by the Council of Australian Governments in 2005. A smaller number of assessments were issued on proposed access to security-sensitive biological agents under a regulatory scheme administered by the Department of Health under the *National Security Health Act 2007*, and on access to the Australian Nuclear Science and Technology Organisation nuclear facility in Lucas Heights.

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

During this reporting period we commenced preparations to support accreditation arrangements for the Gold Coast 2018 Commonwealth Games, as well as the Association of South-East Asian Nations and the Rugby League World Cup events in 2018, which will involve provision of a significant number of access security assessments.

Internal review of adverse visa security assessments

We continued to review adverse visa security assessments issued to 'eligible persons' and to issue new assessments informed by updated information or changes in the security environment. Persons eligible for review are those who remain in immigration detention, having been found by DIBP to be owed protection obligations under international law but who are 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.

During this reporting period, our new assessments supported DIBP's decision-making in relation to the immigration status of these persons.

The annual report of the Independent Reviewer of Adverse Security Assessments is provided at Appendix E of our annual report.

Measure	Effective advice, reporting and services that assist the Australian Government and our partners manage security risks and disrupt activities that threaten Australia's security
Targets	The Australian Government is satisfied its security responses and policies are informed and supported by our expertise and advice Law enforcement, border and other national security partners use our advice to manage and disrupt security risks

We continued to support the Australian Government's counter–people-smuggling policies, in particular through our contribution to OSB. We conducted onshore intelligence collection and supported OSB partners' disruption activities.

We provided advice to support Australian Government policy measures such as the intake of an additional 12 000 refugees from Syria and Iraq, and the agreement between the Australian and United States governments to resettle detainees from Manus Island and Nauru facilities. We also provided advice to border security agencies on Australia's security environment and threats to maritime and aviation security, which informed policy and operational responses to these threats.

Measure	We support DIBP to meet its migration program and refugee and humanitarian resettlement goals
Target	Security advice to DIBP is timely and meets the agreed service level agreements and is responsive to DIBP's other priorities

In 2016–17, we worked closely with DIBP to successfully meet the terms of our service level agreement and their migration program priorities. This work involved the prioritisation, triage and assessment of a large visa security assessment caseload (refer Table 1), and included security checking of illegal maritime arrivals currently residing in the Australian community, and responding to the additional priority of advice in relation to 12 000 Syrian/Iraqi refugees.

To assist in meeting our service level agreement, we reformed our visa security assessment business processes and implemented a new case management system that allowed large caseloads to be reduced by the end of this reporting period.

Activity 3: stakeholder views on performance

In our 2017 stakeholder survey, border security partners said that ASIO was a valued and capable partner. We are perceived as effective in identifying and assessing threats to Australia's border integrity, providing security assessments, and providing advice on border security–related policy and legislative issues. Engagement between senior officers of our respective organisations was perceived as strong and continuing to improve.

Collaboration on counter-terrorism issues at the border was perceived as being effective and at an all-time high.

Stakeholders also said that shared investment in ICT systems had facilitated more effective engagement between us, but that more work was needed to address other shortfalls in ICT connectivity. This work is currently underway.

4	Activity 4: providing protective security advice to government and business
Measure	We provide effective protective security advice, reporting and services that inform security by design by government, business, and industry
Targets	Our expertise and advice informs security policies and approaches within government agencies, business, and industry Business and industry adopt our security advice and are satisfied with their engagement Protective security resources are directed at protecting the assets, infrastructure and systems judged to be most at risk

In 2016–17, BGLU continued to provide an interface between ASIO and stakeholders, providing risk management decision-makers in government and industry with the most current intelligence on security threats as well as protective security advice. The BGLU was previously known as the Business Liaison Unit but was renamed BGLU in 2017 in recognition of the unit's outreach within government as well as industry.

During this reporting period, BGLU provided information to stakeholders through a subscriber-controlled website, ASIO-hosted briefings, face-to-face engagement and participation in joint government/industry forums.

The BGLU's secure website hosted intelligence-backed reporting drawn from the full range of our information holdings and experts, including NTAC and ASIO–T4. It also included reports and products from other Australian Government agencies, such as the ACSC. Sixty-four reports were published during this reporting period. On 30 June 2017, the website had 2046 active subscribers with an almost equal subscription of government and industry.

We also reviewed the format of BGLU's briefings on national security threats to key critical infrastructure sectors and other national security issues. To maximise their value and effect, we sharpened briefings and timed them to align with the AGD–led Trusted Information Sharing Network (TISN) sectoral meetings in Canberra. We also met with key stakeholders to ensure briefings met the requirements of attendees and responded to their highest priority issues.

BGLU coordinated nine sectoral briefings on security threats to aviation, places of mass gathering, Defence industry, energy and resources, mass passenger transport, communications, and banking and finance. The average number of attendees at briefings was around 100. Feedback from attendees reflected overwhelming satisfaction with the new briefing format; 100 per cent of respondents stated that 'the session met my expectations'; 84 per cent of respondents stated that the length of the presentations was 'just right'; and 99 per cent of respondents stated that the briefing 'is relevant to my work'.

In early June 2017, the BGLU delivered its first jurisdiction-specific briefing in Western Australia in response to advice that local stakeholders faced difficulties in travelling to attend briefings in Canberra. BGLU arranged for a small team of ASIO subject matter experts to travel to Perth to brief around 70 government and industry representatives. Feedback from attendees showed a high level of satisfaction with the brief: 97 per cent of respondents stated that 'the session met my expectations'; 84 per cent of respondents stated that the length of the presentations was 'just right'; and 97 per cent of respondents stated that the briefing 'is relevant to my work'.

During this reporting period, BGLU also contributed protective security advice to stakeholders through a range of government and industry forums including the ANZCTC Business Advisory Group, the TISN, and Critical Infrastructure Advisory Council meetings; and supported the Office of Transport Security and the Australian Airports Association and key aviation sector meetings such as Airport Security Committee meetings, the Aviation Security Advisory Forum and Regional Industry Consultative Meetings.

ASIO–T4 protective security

In 2016–17, ASIO–T4 adopted a revised prioritisation model to manage the high stakeholder demand for our protective security advice. The new model ensures ASIO–T4's protective security work is 'intelligence-led' and directed at protecting the assets, infrastructure and systems we consider to be most at risk from terrorism, espionage and foreign interference–related threats.

During this reporting period, ASIO–T4 released protective security guidance documents on the BGLU and Govdex websites on:

- hostile vehicle mitigations—redeployable vehicle security barriers;
- vehicle security barriers—active and passive;
- protective security assessment inspections;
- perimeter intrusion detection systems;
- the engagement of a security consultancy service—protective security reviews;
- the facilitation of TSCM inspections; and
- agency security adviser newsletters.

During this reporting period, ASIO–T4 continued to:

- provide protective security training to government;
- conduct security equipment testing and evaluation, the results of which were published in the *Security equipment evaluated product list*. One hundred and seventy-nine security products were evaluated in 2016–17; and
- conduct TSCM inspections to provide a high level of assurance that security classified or sensitive discussions and information is not technically compromised.

A summary of ASIO–T4's protective security advice is provided at Table 2.

Target	The annual program of physical security certifications is achieved

The Australian Government PSPF's physical security management protocol requires government agencies to obtain ASIO–T4 certification for Zone 5 (Top Secret) areas.

During this reporting period, ASIO–T4 met all agency requests for Zone 5 area inspections and either provided certification for those areas or advice to the relevant agency on further measures required to meet certification requirements. Eighty inspections were conducted and 39 certifications issued.

ASIO–T4 also provided a range of services to assist agencies gain Zone 5 certification, including the provision of guidelines, equipment catalogues and training for consultants.

Advice	Results for 2016–17
Physical security certification program	**Zone 5 facilities:** 80 site inspections and reports 39 certifications issued **Destruction services:** 9 site inspections and reports 8 certifications issued **Lead agency gateway facilities:** 3 site inspections and reports 2 certifications issued **Courier services:** 3 site inspections and reports
Technical surveillance countermeasures	Details of this activity are reported in our classified annual performance statement
Security services and equipment evaluation	179 security products evaluated
Protective security review reports	1 protective security risk review
Communications	**Publications:** 6 protective security circulars posted on Govdex for government 5 security managers guides posted on the BGLU website for industry and government 2 technical note annexes posted on Govdex for government 1 security equipment guide posted on Govdex for government Revised courier service criteria **Training:** 4 protective security training courses 2 safe maintainer courses 1 Security Construction and Equipment Committee (SCEC)–approved locksmith briefing 1 SCEC-approved consultant briefing

Table 2: ASIO–T4 protective security advice

Activity 4: stakeholder views on performance

Stakeholders said that our protective security advice, reporting and services were highly regarded. In particular, the BGLU, NTAC and ASIO–T4 were recognised as sources of authoritative protective security advice.

Our stakeholder briefing days, particularly those conducted for law enforcement partners and industry sectors dealing with transport and crowded places, are valued and the quality of presentations are considered by stakeholders to be generally of a high standard. Where the quality of presenter or presentation has not met expectations, it has been the exception.

Stakeholders also said briefings by senior ASIO officers were highly sought after, and their presentations were viewed as being appropriate, balanced, informative and often very influential. Federal, state and territory senior officials expressed their gratitude for frank and focused briefings provided for federal ministers and state and territory premiers and ministers, especially on terrorism, espionage, foreign interference and cyber threats.

5	Activity 5: collecting foreign intelligence in Australia
Measure	We provide intelligence that is useful to progress Australia's national security, foreign relations, or economic wellbeing
Target	We are responsive to the requirements of our clients

Under the ASIO Act, we are responsible for the collection of foreign intelligence in Australia on matters relating to Australia's national security, foreign relations or economic wellbeing. The details of our performance in relation to this activity are classified and reported separately in our classified annual report.

Measures across all activities

Measure	The safety of our staff is maintained
Target	Our senior leaders continue to be exemplars and drive a work culture, systems, and individual conduct that promote officer safety

In February 2017 we appointed our Deputy Director-General for Counter-Terrorism as ASIO's Senior Safety Officer, to improve leadership and coordination in relation to staff safety programs within ASIO.

The Senior Safety Officer's top priorities during this reporting period, developed by our Operational Risk Steering Committee (ORSC), included updating safety-related policy and procedures, reviewing inter-agency cooperation and emergency response arrangements and enhancing personal safety, security and first aid training. The Senior Safety Officer also supported a number of new initiatives in relation to nationally consistent operational officer responsibilities and procedures, and official motor vehicle safety.

In April 2017, the Chair of the ORSC launched the Officer Safety Portal on ASIO's Intranet, a 'one-stop shop' for officer safety information, capabilities and issues across the Organisation. In the same month the Deputy Director-General for Counter-Terrorism also launched the Counter-Terrorism Innovation Hub to encourage counter-terrorism group staff to submit innovation proposals for improving processes in ASIO, including processes relating to officer safety. These leadership initiatives fostered a strong focus on officer safety within ASIO during this reporting period and attracted a range of new proposals designed to enhance our staff safety arrangements.

Target	We maintain high levels of work health and safety capacity and ongoing training of staff

We continued during this reporting period to enhance our WHS arrangements through a layered approach that begins at induction training for staff and is supplemented thereafter by a suite of courses and refresher training consistent with the nature of each officer's work. In 2016–17, we delivered the following personal security and safety training courses:

Course	Courses delivered	Number of participants
ASIO situational awareness	22	217
General personal security	13	121
De-escalation training	9	108
Trauma first aid	3	37
Hostile environment awareness training	3	29

Additionally, where required, staff received training in 'spontaneous protection', functional first aid and driver training.

Work health and safety

During this reporting period we maintained a high level of WHS capacity, including through initiatives such as our health and safety representative network, first aid officers and health and wellbeing program, which continued during this reporting period to deliver cost-effective initiatives such as the annual influenza vaccination program and campaigns to raise awareness among staff about the benefits of a healthy lifestyle.

In 2016–17, we conducted a strategic review of our WHS performance. The review evaluated the appropriateness of our WHS governance, communication and coordination arrangements. The review found that WHS is integrated effectively into our day-to-day work activities and that the Organisation has a sound WHS culture.

The effectiveness of our approach to WHS continues to be reflected in a Comcare premium rate that remains well below that of the overall premium rate for Australian Government agencies (refer Chart 4) and the outcomes of rehabilitation audits. In 2016–17 an internal rehabilitation audit examined ASIO's rehabilitation management system, processes and outcomes, and validated our compliance with the *Safety, Rehabilitation and Compensation Act 1988* and Comcare's Guidelines for Rehabilitation Authorities 2012. No areas of non-compliance were identified.

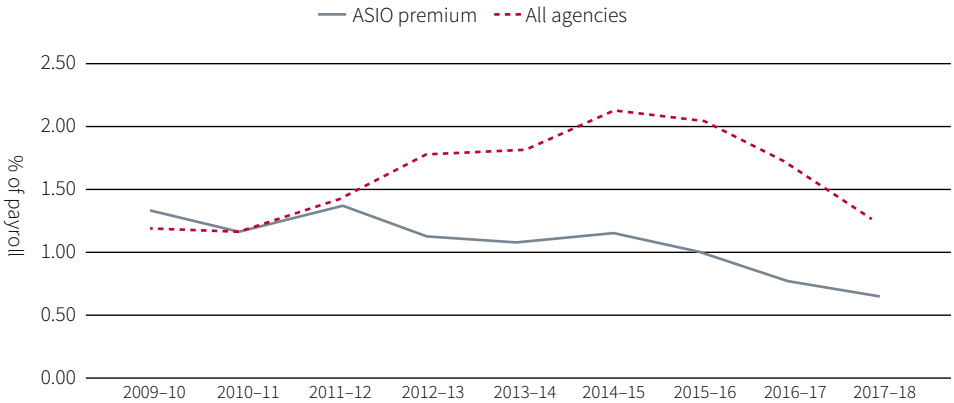


Chart 4: comparison of Comcare premium rates 2009–10 to 2017–18.

Note: ASIO's Comcare premium rate has fallen from 0.79 per cent of payroll in 2016–17 to 0.69 per cent of payroll in 2017–18. This premium rate compares favourably with the overall premium rate for Australian Government agencies in 2017–18, which is 1.23 per cent. The percentage of payroll for 2017–18 is indicative only.

In line with legislated notification obligations, ASIO reported eight incidents to Comcare in 2016–17. 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*.

Measure	Legality and propriety of our activities and effectiveness of our engagement with oversight and accountability bodies
Target	Our senior leaders continue to be exemplars and drive a work culture, systems, and individual conduct that are legal, ethical, and respectful of human rights

In 2016–17, our senior leaders continued to support initiatives that convey to staff our expectations of individual conduct that is legal, ethical and respectful of human rights. This included contributing to our induction training programs, our Management and Leadership Strategy 2017–2020 programs, and presenting sessions on ethical decision-making in ASIO.

All staff, including our senior leaders, are required to complete various mandatory e-learning programs which:

- promote our values and code of conduct requirements;
- ensure employees are aware of the mechanisms to make disclosures under the *Public Interest Disclosure Act 2013*;
- explain WHS obligations; and
- identify and provide strategies for managing workplace discrimination, harassment and bullying.

Furthermore, both the IGIS and ASIO's Ombudsman were involved across the suite of our training programs in providing advice on ethical and accountable behaviour in the workplace.

During this reporting period our senior leaders also conducted a review of the human rights performance of the countries of our foreign security and intelligence service counterparts. This review is undertaken annually to ensure that we take due regard of human rights in our cooperation with foreign partners.

Target	We proactively engage with oversight and accountability bodies and provide as much information as possible for use in the public domain

During this reporting period we engaged extensively with a range of oversight and accountability bodies, including the:

- PJCIS;
- Senate Legal and Constitutional Affairs Committee;
- IGIS;
- INSLM; and
- Independent Reviewer of Adverse Security Assessments.

We provided classified and unclassified submissions and appeared publicly and in private hearings to support the work of these bodies. Further details on our engagement with these bodies is provided in the 'External Scrutiny' section of our annual report. A copy of the Independent Reviewer of Adverse Security Assessments' annual report is provided at Appendix E.

Measure	The security of our activities
Target	Our senior leaders continue to be exemplars and drive a work culture, systems, and individual conduct that embody security

Our senior leaders continued to foster a positive protective security culture where security is considered in all decision-making and perceived as a shared responsibility. This included supporting ongoing security management and training and ensuring that 'promoting a security culture' is treated as a core capability requirement for all staff.

Our leaders also continued to drive a culture of security through the ASIO Security Committee, which is a senior-level committee that oversees our security policies and practices and ensures security risk management best practice is incorporated into all aspects of our business.

Target	We continue to meet the requirements of the Australian Government's Protective Security Policy Framework

Throughout this reporting period, we managed the security of our people, information and assets, in line with the requirements of the PSPF. We reviewed and updated our policies and procedures to reflect changes in broader government policy and our risk environment. We provided staff security awareness training at their commencement with ASIO, and required them to undertake refresher training at regular intervals. We conducted annual reviews of staff clearances and provided mechanisms for staff to report security incidents or concerns.

5

MANAGEMENT AND ACCOUNTABILITY

Corporate governance

The Director-General of Security is the accountable authority for ASIO under the PGPA Act. Our corporate governance committees supported the Director-General during this reporting period to fulfil his responsibilities under the PGPA Act.

ASIO Executive Board

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

The board met on a monthly basis during this reporting period, setting the overall strategic direction for ASIO and overseeing the management of resources. It received regular reporting from our corporate committees on matters such as developments in the security environment, our budget, capability development and risk management, as well as progress toward our ASIO2020 and diversity and inclusion goals.

Intelligence Coordination Committee

The Intelligence Coordination Committee supported the Director-General through its management of ASIO's security intelligence program. During this reporting period the committee provided strategic direction for our intelligence programs, managed risks, coordinated efforts across work areas, evaluated intelligence performance, reviewed intelligence capability programs and providing guidance on priorities for our investment program.

The committee was chaired by our Deputy Director-General for Counter-Terrorism.

Workforce Capability Committee

The Workforce Capability Committee's focus during this reporting period was ensuring our workforce was sufficiently sized, skilled, equipped and accommodated to meet the current and future needs of the Organisation. The Work Health and Safety Committee was a subcommittee responsible for ensuring better health and safety policies and practices across ASIO (refer 'Work health and safety').

The committee was chaired by the Deputy Director-General for Strategy.

Security Committee

The Security Committee provided advice to the Executive Board on the evolving security environment and matters relating to the security of our operational activities, people, property and information technology. It also approved revised security policies and procedures and reviewed our compliance with Australian government security standards.

The committee was chaired by the Deputy Director-General for Strategy.

Finance Committee

The Finance Committee provided advice to the Executive Board on financial strategy, resource allocation within ASIO, accommodation and assets.

The committee was chaired by the Deputy Director-General for Strategy.

Audit and Risk Committee

In line with the requirements of section 45 of the PGPA Act, the Director-General established the Audit and Risk Committee. During this reporting period, the committee provided independent assurance and advice to the Director-General and the Executive Board on our financial and performance reporting responsibilities, risk oversight and management, and system of internal control.

The committee had four external members including an external chair, as well as observers from the Australian National Audit Office.

Fraud control and management

Our Fraud Management Group continued to oversee fraud control and management arrangements within ASIO, reporting to the Audit and Risk Committee. There were no allegations of fraud received during this reporting period.

During 2017, we completed the annual assurance mapping process, which examined all internal controls and assurance-related activities across ASIO. No new fraud risks were identified during this review, and existing risks, which are captured in the current fraud risk assessment, continued to be appropriately addressed through our security regimes, financial controls and human resource frameworks.

The ASIO Fraud Control Framework 2016–18, available online at www.asio.gov.au/asio-fraud-control-framework-2016-18.html, outlines our fraud control and management arrangements.

2017 review of governance arrangements

We conducted a review of our governance arrangements during the reporting period, with a new committee structure and reporting arrangements developed to strengthen our oversight of performance and risk management. The new arrangements will be implemented during the 2017–18 reporting period.

External scrutiny

Ministerial accountability

ASIO's ministerial accountability during this reporting period was 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 our 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, and we contributed to the review during this reporting period.

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

an 'issuing authority'. If we judge that a warrant is required, the Director-General presents a warrant request to the Attorney-General. Most warrant requests are 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, we must report to the Attorney-General on the extent to which the warrant assisted us in carrying out our functions.

We keep the Attorney-General informed of significant national security developments, as well as other important issues affecting ASIO. During this reporting period, we provided advice to the Attorney-General on a range of investigative, operational and administrative issues, primarily communicated through 288 formal submissions. The Director-General also briefed 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 provide them with a copy of ASIO's classified annual report. Throughout 2016–17, with the Attorney-General's knowledge, classified briefings on specific security cases were provided for shadow ministers.

Parliamentary Joint Committee on Intelligence and Security

The PJCIS plays a significant role in our oversight and accountability framework. Its annual review of administration and expenditure scrutinises the non-operational aspects of our work, particularly the effectiveness of our policies, governance and expenditure. The PJCIS also conducts inquiries into other matters relating to the intelligence agencies, as referred by the government or the parliament. The PJCIS reviews the listing of terrorist organisations under the *Criminal Code Act 1995* and key national security legislation.

During this reporting period, we made a submission to and appeared before the PJCIS to support its review of the re-listing of six terrorist organisations under the Criminal Code and ISIL being declared as a terrorist organisation under the *Australian Citizenship Act 2007*. In early 2017, we appeared before the committee for its review of the Telecommunications and Other Legislation Amendment Bill, for which we provided a classified submission. We also appeared before the PJCIS in closed and public hearings for its Review of Administration and Expenditure no. 15 (2015–16), providing a classified and an unclassified submission.

A key focus for the PJCIS in the latter part of 2016–17 was its review of our questioning and detention powers. We provided the committee with a classified and unclassified submission, a classified and unclassified supplementary submission, and classified and unclassified answers to written questions from the committee, as well as appearing before PJCIS hearings in relation to this matter. The review was ongoing at the end of this reporting period.

The PJCIS's recommendations from its inquiries are reported to each House of the parliament and to the responsible minister. Our evidence to the PJCIS 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

We appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate Estimates process on 18 October 2016, 28 February 2017 and 25 May 2017. Our evidence to the committee can be found in the estimates Hansard for those days (refer www.aph.gov.au/Parliamentary_Business/Senate_Estimates and navigate to the relevant hearing).

Independent oversight

Inspector-General of Intelligence and Security

The Hon. Margaret Stone was appointed as 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 2016–17, the IGIS undertook a regular inspection program of activities across our 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 National Security Legislation Monitor

The acting INSLM, Dr James Renwick SC, was appointed on 13 February 2017. He replaced the Hon. Roger Gyles AO QC, who held the role from 20 August 2015 until 31 October 2016. The INSLM'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 2016–17, we made submissions to the INSLM in relation to the following inquiries:

- certain questioning and questioning and detention powers in relation to terrorism; and
- the 2017 statutory review of Division 3A of Part IAA of the Crimes Act (Stop, Search & Seize powers), subsections 119.2 and 119.3 of the Criminal Code (Declared Areas), and Divisions 104 and 105 of the Criminal Code (Control Orders & Preventive Detention Orders) including the interoperability of the control order regime and the *Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016*.

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

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

Independent Reviewer of Adverse Security Assessments

The role of the Independent Reviewer of Adverse Security Assessments 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 Independent 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 our 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 Independent Reviewer's terms of reference.

In performing their task, the Independent Reviewer has access to all materials relied on by ASIO to make their assessment and any information obtained by ASIO since the adverse security assessment was completed or provided to the Independent Reviewer by the applicant or their legal representatives. Particularly for periodic reviews, the Independent 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 their time in detention.

The Independent Reviewer's terms of reference are available at www.ag.gov.au/asareview. The Independent Reviewer's annual report is at Appendix E of this report.

Significant legal matters impacting on ASIO's business

Tribunal reviews—security assessments

Over this reporting period, ASIO managed 20 adverse security assessment reviews before the Administrative Appeals Tribunal, including those relating to cancelled passports, visas and security clearances. Of these:

- six applicants withdrew their applications at various stages;
- five matters were pending at the end of this reporting period;
- five assessments were remitted back to ASIO by consent for new assessments to be prepared, which resulted in four non-prejudicial assessments being issued in this reporting period, and the fifth remains under reconsideration;
- two applications were dismissed for non-compliance;
- one matter was heard and its decision remained reserved at the end of this reporting period; and
- one review was stayed.

Judicial reviews—security assessments

Two further security assessments were reviewed in the Federal Court of Australia during this reporting period. Both applicants challenged the legal reasonableness of the assessments and our compliance with our security assessment policies, and alleged they had been denied procedural fairness during the making of the assessments.

BSX15 v Minister for Immigration and Border Protection and Director-General of Security [2016] FCA 1432

We assessed that BSX15, who had entered Australia as an irregular maritime arrival and claimed refugee status, was a member of ISIL and posed a risk to Australia's security. The court (heard by Justice Markovic) held that the applicant was not denied procedural fairness at his security assessment interviews because the purpose of the interviews was clearly explained and the applicant was given the opportunity to answer questions as fulsomely as he wished. On 25 May 2017, the applicant appealed the decision to the Full Federal Court, and the decision was reserved at the end of this reporting period.

El Ossman v Minister for Immigration and Border Protection and Director-General of Security [2017] FCA 636

We assessed that the applicant, a Lebanese national who entered Australia on a tourism then spousal visa, was a member of Jabhat Fatah al-Sham and posed a risk to Australia's security. During an interlocutory hearing, the Court (heard by Justice Wigney) upheld the Director-General's public interest immunity claim over some classified information. On 6 June 2017, the court held that the applicant had been denied procedural fairness during the security assessment interview, and set aside the security assessment. The court dismissed the applicant's unreasonableness and policy non-compliance challenges.

In light of these judicial findings, we introduced staff training and reviewed our processes to ensure they appropriately balanced the protection of sensitive classified information with the requirement to afford individuals procedural fairness.

Coronial inquests

Inquest into the deaths arising from the Lindt Café siege

On 24 May 2017, the New South Wales State Coroner concluded the inquest into the deaths of Tori Johnson, Katrina Dawson and Man Haron Monis at the Lindt Cafe in December 2014. We cooperated with the inquest and six of our employees gave evidence in closed court proceedings in December 2015 and September 2016.

The coroner concluded that:

- our 2008 investigation of Mr Monis was 'balanced, comprehensive and appropriate in the circumstances';
- the subsequent assessments we conducted relating to Mr Monis, and our consideration of him, were adequate and appropriate; and

- our treatment and management of the National Security Hotline reports in the period of their first receipt and the siege, including their triage, was adequate and appropriate.

The coroner also found that two significant aspects of our politically motivated violence risk assessment process (relating to triaging leads and the criteria used for assessing politically motivated violence) required recalibration, and that there were several examples of information that we ought to have shared with the New South Wales Police Force.

The coroner's recommendations relating to ASIO included that:

- the Commonwealth Attorney-General should liaise with ASIO to develop a policy to ensure that correspondence relevant to security be referred to ASIO and a fixated threat assessment centre;
- the Commonwealth Attorney-General and ASIO should confer with the Australian Psychological Society to enable psychologists to report risks of a terrorist nature; and
- the Premier of New South Wales should consider whether legislation can be amended to ensure that ASIO has appropriate access to information.

We accepted the coroner's conclusions and have commenced work with relevant agencies to implement the recommendations relating to ASIO.

Ahmed Numan Haider: Victorian coronial inquest

On 23 September 2014, Mr Haider was fatally shot by a member of Victoria Police. ASIO cooperated with the coronial investigation and provided the coroner with relevant material. Four ASIO witnesses gave evidence at the inquest. The coroner released his findings on 31 July 2017 and made no substantive adverse findings or recommendations for ASIO.

2017 Independent Intelligence Review

In 2016–17, the Prime Minister commissioned Professor Michael L'Estrange AO and Mr Stephen Merchant PSM to undertake an independent review of the AIC. Their review, was finalised and submitted to the Prime Minister at the end of this reporting period.

We provided one major submission and five supplementary submissions to the review, and supported its work by seconding a senior officer to the review team and providing advice in response to requests for information.

The review found that Australia's intelligence agencies were highly capable and staffed by skilled officers of great integrity. The review made 23 recommendations to strengthen the AIC's structural, resourcing, capability, legislative and oversight arrangements.

We supported the recommendations of the review. Since the public release of the review by the Prime Minister in July 2017, we have contributed to whole-of-government work to implement the recommendations of the review as well as to establish the new Home Affairs portfolio, which was also announced by the Prime Minister at the time of releasing the review.

Management of human resources

We continued during this reporting period to effectively manage and develop a highly capable workforce, facing significant security challenges in a complex operating environment. We further strengthened our recruitment arrangements to ensure that we continue to attract and effectively develop the people required for ASIO to continue to meet its objectives. We provided extensive training and development opportunities for staff, which were consistently rated highly by participants. We also assessed our workforce at all levels through a performance management framework that evaluated capability and performance, and provided pathways to further develop staff capabilities.

Recruitment

In 2016–17, we achieved a net growth of 59 staff. As of 30 June 2017, we employed 1794.3 full-time equivalent staff (refer Appendix C). Our separation rate at that time was 5.26 per cent.

During this reporting period, our focus was on recruiting difficult-to-fill intelligence, analytical, technical and information technology roles. To improve our ability to attract quality applicants, to meet our ongoing growth and people capability requirements and to ensure we continued to be an employer of choice, we:

- reviewed our selection and assessment methodologies for our graduate and trainee programs;
- undertook quantitative and qualitative market research into graduate employment preferences and ASIO's recruitment and marketing programs, which informed revisions to our recruitment marketing materials and the renewal of our website content; and
- commenced a review of our advertising and marketing strategies, including examining options to make better use of social media platforms for recruitment activity and marketing.

Training

During this reporting period, ASIO provided a broad and expanding range of personal and professional development opportunities for staff to meet the diverse needs of our workforce, informed by the findings of a training review commissioned by the Director-General in 2014–15.

In 2016–17:

- we approved or conducted 146 training courses, with 4256 face-to-face training activities attended by 1387 staff;
- Our staff completed 2839 mandatory and 1928 non-mandatory e-learning courses;
- we allocated $337 804 to 115 staff attending over 70 ASIO-supported study programs;
- we allocated $181 375 to 16 domestic and six international development opportunities attended by 19 members of ASIO's Senior Executive Service; and
- we allocated $291 661 to 34 employees under the Language Skills Development Program.

Our training programs were delivered by in-house learning and development and subject matter experts, as well as external training providers. We continued to review, evaluate and update programs as part of our

focus on continuous improvement and alignment of training with ASIO's objectives. The consistently positive feedback received from course participants and their line managers indicated that ASIO was effectively developing employees to perform the various roles which contribute to achieving our purpose.

Workforce and performance management

We reinforced our high-performance culture by enhancing the link between salary advancement and performance outcomes. Building on reforms implemented during 2015–16, we formalised the requirement for managers and employees to hold performance discussions and agree on performance expectations at the beginning of the performance cycle. These discussions provided the basis for developing staff and organisational capabilities by identifying capability needs and agreeing on training or other development programs to address those needs.

In 2016–17, we refreshed our career management framework and commenced a comprehensive review of the skills and capabilities required in our intelligence, technical, information and corporate roles. The objective of this work is to:

- assist individuals in their career planning;
- assist work areas in managing their capability needs;
- support skills gap analysis;
- support ASIO in its strategic workforce planning;
- inform recruitment targeting; and
- inform training needs and programming.

We are working to finalise our career management framework update and competency mapping by the end of 2017–18.

Diversity and inclusion

ASIO is committed to building a productive, innovative, capable and inclusive workforce that values difference and creates an environment where staff are supported in reaching their full potential.

In 2016–17, we undertook a range of work to support this vision, including:

- establishing a new corporate committee to oversee the development and implementation of diversity and inclusion strategies and initiatives, which is chaired by our Deputy Director-General for Strategy and reports to our Executive Board;
- continuing the development of our Diversity and Inclusion Strategy, to provide the framework for our program and alignment with existing actions and initiatives; and
- establishing an Executive Level 2 position dedicated to advancing ASIO's diversity and inclusion strategy and initiatives.

We launched our Gender Equity Bold Goals program, which reinforced our commitment to achieving gender equity across all levels of ASIO by 2020. Within this program, we:

- introduced the first stage of an 'if not, why not' approach to flexible working;
- specified a shortlisting ratio of 40 per cent female, 40 per cent male and 20 per cent of either gender for promotion rounds at Executive Level 1 and above;
- delivered unconscious bias training to senior executive officers and key functional areas;

- internally publicised detailed gender metrics for ASIO promotion, transfer and recruitment rounds;
- established our membership with the Diversity Council of Australia; and
- appointed a Senior Executive Service Band 2 officer as ASIO's Male Champions of Change Implementation Leader.

In 2016–17, we also provided opportunities for staff to broaden their understanding and awareness with presentations on gender equity issues by individuals including Her Excellency Menna Rawlings CMG, British High Commissioner to Australia, and Annabel Crabb, journalist, author and television presenter and commentator.

Statistics on the diversity of our workforce are provided at Appendix C.

Workplace agreement

We continued to operate under our 10th Workplace Agreement, which was agreed in 2016 and concludes in 2019. The agreement meets our requirements under the ASIO Act to adopt the employment principles of the Australian Public Service, when these are consistent with the effective performance of the Organisation.

ASIO Ombudsman

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

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

The ASIO Ombudsman provided valuable support and advice to employees and line managers. During this reporting year, the ASIO Ombudsman:

- provided advice and guidance in response to 23 informal contacts from staff;
- carried out four investigations related to the Code of Conduct;
- provided formal advice based on investigations into one additional matter; and
- provided assistance in relation to an IGIS inquiry.

The ASIO Ombudsman provided a valuable source of advice on the development and formulation of human resources policy. In addition, senior ASIO managers drew on the unique skills and experience of the ASIO Ombudsman to inform their decision-making on the application of policy.

In 2016–17, the ASIO Ombudsman did not participate in any work related to public interest disclosures.

Work health and safety

Our annual performance statement addresses the WHS matters we are required to address in our annual report under the *Work Health and Safety Act 2011*.

Disability reporting

Since 1994, non-corporate Australian Government 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 not been required to report on these functions.

The Commonwealth Disability Strategy has been replaced 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 a disability are faring. The first of these progress reports was published in 2014, and can be found at www.dss.gov.au.

Appendix C provides information on the diversity of our workforce, including statistics in relation to people with a disability.

Property and procurement

The Ben Chifley Building continued to support the evolving business and capability needs of ASIO and our partners. The corporate suites, including Australia's largest security-accredited auditorium, hosted a range of activities and events including briefings, industry forums and ministerial addresses. In 2016–17, the corporate suites were booked on 1506 occasions and received more than 5000 external visitors.

Environmental performance

We are committed to reducing ASIO's carbon footprint and improving our environmental performance. In 2016–17 we participated in the 10th consecutive Earth Hour event and:

- reduced our total energy consumption by 255 534 kilowatt hours through the use of solar panels, saving approximately $34 500 and 234 tonnes of carbon emissions;
- produced 52 100 kilowatt hours of electricity by a gas-fired co-generator plant, reducing grid electricity costs by a further $7050 and saving 45.3 tonnes in carbon emissions;
- used 21 986 kilolitres of captured stormwater for irrigation and toilet flushing, reducing reliance on potable water and bore water and saving approximately $114 900 of potable water costs;
- recycled 15 899 kilograms of waste, including paper products, printer toner cartridges, batteries, scrap metal and fluorescent light tubes; and
- increased efficiencies in our data centre through temperature adjustment and installation of blanking panels to reduce energy consumption and decrease maintenance requirements.

Procurement

Throughout 2016–17 we adhered to the Commonwealth Procurement Rules and associated policy and guidelines. Our compliance was monitored through our Audit and Risk Committee and Finance Committee. No significant issues were identified and overall compliance was acceptable.

ASIO supports small business participation in the Australian 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.

Our procurement practices that 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 28 new consultancy contracts involving total actual expenditure of $2.41 million (goods and services tax (GST-inclusive). In addition, six ongoing consultancy contracts were active during the period, involving total actual expenditure of $0.25 million (GST-inclusive).

We applied the Commonwealth Procurement Rules and Department of Finance guidance when selecting and engaging consultants. We also followed internal policy and associated procedures that provide guidance on identifying and determining the nature of a contract. This ensured that appropriate methods for engagement and contracting were executed. We engaged consultants when there was a need for professional, independent and expert advice or services that were not available from within the organisation.

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. We are not required to publish information on the AusTender website, in line with authorised exemptions to avoid prejudice to our national security activities. A list of consultancy contracts to the value of $10 000 or more during this reporting period, and the total value of each of those contracts over the life of each contract, is available on request for members of the PJCIS, which has oversight of our administration and expenditure.

Contracts

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

The Director-General has applied measures necessary to protect national security which exempt ASIO from publishing details of contract arrangements, including standing offers, in accordance with clause 2.6 of the Commonwealth Procurement Rules. Details of our agreements, contracts and standing offers are available on request for members of the PJCIS.

Advertising and market research spends

We spent $360 982 on advertising in 2016–17, predominantly on recruitment campaigns. ASIO does not fall within the definition of agencies covered by the reporting requirements of section 311A of the *Commonwealth Electoral Act 1918*.


6
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 2017 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

24 August 2017

Australian National Audit Office

INDEPENDENT AUDITOR'S REPORT

To the Attorney-General

Opinion

In my opinion, the financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2017:

(a) comply with Australian Accounting Standards – Reduced Disclosure Requirements 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 2017 and its financial performance and cash flows for the year then ended.

The financial statements of the Australian Security Intelligence Organisation, which I have audited, comprise the following statements as at 30 June 2017 and for the year then ended:

- Statement by the Director-General of Security;
- Statement of Comprehensive Income;
- Statement of Financial Position;
- Statement of Changes in Equity;
- Statement of Cash Flows;
- Notes to the financial statements, comprising a Summary of Significant Accounting Policies and other explanatory information.

Basis for Opinion

I conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the Australian Security Intelligence Organisation in accordance with the relevant ethical requirements for financial statement audits conducted by the Auditor-General and his delegates. These include the relevant independence requirements of the Accounting Professional and Ethical Standards Board's APES 110 *Code of Ethics for Professional Accountants* to the extent that they are not in conflict with the *Auditor-General Act 1997* (the Code). I have also fulfilled my other responsibilities in accordance with the Code. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

Accountable Authority's Responsibility for the Financial Statements

As the Accountable Authority of the Australian Security Intelligence Organisation 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 – Reduced Disclosure Requirements and the rules made under that Act. The Director-General of Security 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.

In preparing the financial statements, the Director-General of Security is responsible for assessing the Australian Security Intelligence Organisation's ability to continue as a going concern, taking into account whether the entity's operations will cease as a result of an administrative restructure or for any other reason. Director-General of Security is also responsible for disclosing matters related to going concern as applicable and using the going concern basis of accounting unless the assessment indicates that it is not appropriate.

Auditor's Responsibilities for the Audit of the Financial Statements

My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance

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

with the Australian National Audit Office Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

As part of an audit in accordance with the Australian National Audit Office Auditing Standards, I exercise professional judgement and maintain professional scepticism throughout the audit. I also:

- identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control;
- obtain an understanding of internal control relevant to the audit 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;
- evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Accountable Authority;
- conclude on the appropriateness of the Accountable Authority's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the entity's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the entity to cease to continue as a going concern; and
- evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

Australian National Audit Office

Lesa Craswell
Acting Executive Director

Delegate of the Auditor-General

Canberra
24 August 2017

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2017

	Notes	2017 $'000	Original Budget 2017 $'000	2016 $'000
EXPENSES				
Employee benefits	1.1.A	239 924	229 425	235 287
Suppliers	1.1.B	181 969	195 930	168 862
Depreciation and amortisation	2.2.A	88 335	76 166	76 111
Other	1.1.C	1291	-	1155
TOTAL EXPENSES		**511 519**	**501 521**	**481 415**
OWN-SOURCE INCOME				
Revenue				
Sale of goods and services	1.2.A	15 008	18 386	14 094
Other revenue	1.2.B	5115	3187	4162
Gains	1.2.C	2 553	762	614
TOTAL OWN-SOURCE INCOME		**22 676**	**22 335**	**18 870**
NET COST OF SERVICES		**488 843**	**479 186**	**462 545**
REVENUE FROM GOVERNMENT	3.1	**402 998**	**403 020**	**381 081**
DEFICIT ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT		**(85 845)**	**(76 166)**	**(81 464)**
OTHER COMPREHENSIVE INCOME				
Changes in asset revaluation surplus		-	-	15 117
TOTAL COMPREHENSIVE DEFICIT		**(85 845)**	**(76 166)**	**(66 347)**

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

STATEMENT OF FINANCIAL POSITION
as at 30 June 2017

	Notes	2017 $'000	Original Budget 2017 $'000	2016 $'000
ASSETS				
Financial assets				
Cash and cash equivalents	2.1.A	17 338	10 851	22 433
Trade and other receivables	2.1.B	76 702	84 323	93 868
Accrued revenue		1644	6664	711
Total financial assets		***95 684***	***101 838***	***117 013***
Non-financial assets				
Prepayments		25 911	12 864	20 870
Land and buildings	2.2.A	153 938	147 394	174 878
Property, plant and equipment	2.2.A	130 341	147 744	134 463
Computer software	2.2.A	50 616	45 651	44 441
Total non-financial assets		***360 806***	***353 653***	***374 652***
TOTAL ASSETS		**456 490**	**455 491**	**491 664**
LIABILITIES				
Payables				
Suppliers	2.3.A	11 865	25 752	6 083
Other payables	2.3.B	25 911	17 376	24 590
Total payables		***37 776***	***43 128***	***30 673***
Provisions				
Employee provisions	2.4.A	75 256	66 953	71 448
Restoration obligations	2.4.B	4938	5728	7374
Total provisions		***80 194***	***72 681***	***78 822***
TOTAL LIABILITIES		**117 970**	**115 809**	**109 495**
NET ASSETS		**338 520**	**339 682**	**382 170**
EQUITY				
Parent equity interest				
Contributed equity		668 644	668 644	626 449
Reserves		33 047	17 931	33 047
Retained deficit		(363 171)	(346 893)	(277 326)
TOTAL EQUITY		**338 520**	**339 682**	**382 170**

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

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2017

	2017	Original Budget 2017	2016
	$'000	$'000	$'000
RETAINED EARNINGS			
Opening balance	(227 326)	(270 727)	(195 863)
Comprehensive income			
Deficit for the period	(85 845)	(76 166)	(81 463)
Closing balance	***(363 171)***	***(346 893)***	***(277 326)***
ASSET REVALUATION RESERVE			
Opening balance	33 047	17 931	17 930
Other comprehensive income			
Changes in asset revaluation surplus	-	-	15 117
Closing balance	***33 047***	***17 931***	***33 047***
CONTRIBUTED EQUITY			
Opening balance	626 449	626 449	580 376
Transactions with owners			
Distributions to owners			
Returns of capital—reduction of appropriation	-	-	(3 000)
Contributions by owners			
Equity injection—appropriation	14 103	14 103	13 973
Departmental capital budget	28 092	28 092	35 100
Closing balance	***668 644***	***668 644***	***626 449***
CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT	**338 520**	**339 682**	**382 170**

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 2017

	Notes	2017 $'000	Original Budget 2017 $'000	2016 $'000
OPERATING ACTIVITIES				
Cash received				
Appropriations		421 916	405 137	415 985
Sales of goods and services		13 977	21 398	18 715
Net GST received		19 794	18 289	16 080
Other		2808	1151	4022
Total cash received		***458 495***	***445 975***	***454 802***
Cash used				
Employees		234 556	226 383	233 661
Suppliers		195 772	187 981	177 837
Section 74 receipts		26 493	19 674	26 338
Total cash used		***456 821***	***434 038***	***437 836***
NET CASH FROM OPERATING ACTIVITIES		**1674**	**11 937**	**16 966**
INVESTING ACTIVITIES				
Cash received				
Proceeds from sales of property, plant and equipment		760	-	3174
Total cash received		***760***	***-***	***3174***
Cash used				
Purchase of property, plant and equipment		51 850	56 237	25 945
Purchase of computer software		24 414	-	26 919
Total cash used		***76 264***	***56 237***	***52 864***
NET CASH USED BY INVESTING ACTIVITIES		**(75 504)**	**(56 237)**	**(49 690)**
FINANCING ACTIVITIES				
Cash received				
Contributed equity		68 732	42 195	33 135
Total cash received		***68 732***	***42 195***	***33 135***
NET CASH FROM FINANCING ACTIVITIES		**68 732**	**42 195**	**33 135**
Net increase (decrease) in cash held		**(5095)**	(2105)	410
Cash and cash equivalents at the beginning of the reporting period	2.1.A	22 433	12 956	22 023
CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD		**17 338**	**10 851**	**22 433**

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

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

OVERVIEW

The basis of preparation

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—Reduced Disclosure Requirements 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

Except for AASB 124 *Related Party Disclosures*, new or revised accounting 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 material effect on ASIO's financial statements. AASB 124 requires disclosure of key management personnel compensation and ASIO's transactions with related parties.

Revenue from Government—departmental appropriations

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.

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.

1. Financial Performance

	2017 $'000	2016 $'000
1.1 EXPENSES		
1.1.A Employee benefits		
Wages and salaries	186 995	178 953
Superannuation		
▷ Defined contribution plans	16 569	15 675
▷ Defined benefit plans	15 330	17 072
Leave and other entitlements	20 263	23 466
Separation and redundancies	767	121
Total employee benefits	**239 924**	**235 287**
1.1.B Suppliers		
Goods supplied	6211	5490
Services supplied	136 925	123 217
Operating lease payments	37 202	37 837
Workers' compensation premiums	1631	2317
Total supplier expenses	**181 969**	**168 862**

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.

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	54 853	51 552
Between 1 to 5 years	216 636	176 663
More than 5 years	371 083	343 982
Total operating lease commitments	***642 572***	***572 197***

1.1.C Other expenses		
Finance costs: unwinding of discount—restoration obligations	238	204
Write-down and impairment of assets from:		
▷ Impairment of receivables	6	-
▷ Write-down of property, plant and equipment	1039	951
Losses from asset sales	8	-
Total other expenses	**1291**	**1155**

	2017	2016
	$'000	$'000

1.2 OWN-SOURCE REVENUE AND GAINS

1.2.A Sale of goods and services

Sale of goods	49	10
Sale of services	14 959	14 084
Total sale of goods and services	**15 008**	**14 094**

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	3910	3063
Resources received free of charge—remuneration of auditors	145	140
Royalties	18	19
Other	1042	940
Total other revenue	**5115**	**4162**

Sublease rental income commitments

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

Commitments for rental income are receivable:

Within 1 year	5444	2031
Between 1 to 5 years	23 811	8752
More than 5 years	24 282	7545
Total rental income commitments	***53 537***	***18 328***

Accounting policy

Resources received free of charge are recognised as revenue 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.

1.2.C Gains

Gains from asset sales	-	555
Expiry of lease restoration obligation	2320	-
Other gains	233	59
Total gains	**2553**	**614**

Accounting policy

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

2. Financial Position

	2017 $'000	2016 $'000
2.1 FINANCIAL ASSETS		
2.1.A Cash and cash equivalents	**17 338**	**22 433**

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	**4753**	3423
Appropriation receivable	**67 000**	85 962
GST receivable	**4949**	4483
Total trade and other receivables (net)	**76 702**	**93 868**

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

Credit terms for goods and services were within 30 days (2016: 30 days).

Financial assets were assessed for impairment at 30 June 2017. 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.

2.2 NON-FINANCIAL ASSETS

2.2.A Reconciliation of Property Plant Equipment and Computer software

	Buildings	Buildings - leasehold improvement	Property plant & equipment	Computer software	Total
	$'000	$'000	$'000	$'000	$'000
As at 1 July 2016					
Gross book value	**4581**	**170 297**	**134 705**	**100 194**	**409 777**
Accumulated depreciation amortisation and impairment	**-**	**-**	**(242)**	**(55 753)**	**(55 995)**
Net book value 1 July 2016	***4581***	***170 297***	***134 463***	***44 441***	***353 782***
Additions by purchase	**-**	**2035**	**45 107**	**24 112**	**71 254**
Depreciation and amortisation expense	**(218)**	**(22 629)**	**(47 563)**	**(17 925)**	**(88 335)**
Disposals—other	**-**	**(129)**	**(1666)**	**(12)**	**(1807)**
Net book value 30 June 2017	**4363**	**149 574**	**130 341**	**50 616**	**334 894**
Gross book value	**4581**	**168 822**	**176 421**	**121 504**	**471 329**
Accumulated depreciation amortisation and impairment	**(218)**	**(19 248)**	**(46 080)**	**(70 889)**	**(136 434)**
Net book value 30 June 2017	**4363**	**149 574**	**130 341**	**50 616**	**334 894**

Computer software

The carrying value of computer software included $25.498m (2016 $19.620m) purchased software and $25.118m (2016 $24.821m) 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 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	**-**	**272**	**1885**	**1478**	**3636**
Between 1 to 5 years	**-**	**-**	**-**	**2781**	**2781**
Total capital commitments	***-***	***272***	***1885***	***4259***	***6417***

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:

	2017	2016
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 2017. 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 (2015–16: 1–10 years).

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.

An annual assessment is undertaken to determine whether the carrying amount of the assets is materially different from the fair value. ASIO engaged the services of the Australian Valuation Solutions (AVS) to conduct a materiality review of carrying amounts for all non-financial assets at 30 June 2017. Comprehensive valuations are carried out at least once every three years with the previous valuation conducted at 30 June 2016. AVS has provided written assurance to ASIO that the models developed are in compliance with AASB 13.

The methods utilised to determine and substantiate the unobservable inputs are derived and evaluated as follows:

Physical Depreciation and Obsolescence—Assets that do not transact with enough frequency or transparency to develop objective opinions of value from observable market evidence have been measured utilising the Depreciated Replacement Cost approach. Under the Depreciated Replacement Cost approach the estimated cost to replace the asset is calculated and then adjusted to take into account physical depreciation and obsolescence. Physical depreciation and obsolescence has been determined based on professional judgement regarding physical economic and external obsolescence factors relevant to the asset under consideration. For all Leasehold Improvement assets the consumed economic benefit / asset obsolescence deduction is determined based on the term of the associated lease.

The fair values of ASIO's assets at 30 June 2017 are detailed above in Note 2.2.A.

	2017 $'000	2016 $'000
2.3 PAYABLES		
2.3.A Suppliers		
Trade creditors and accruals	11 865	6083
Total suppliers	**11 865**	**6083**
Settlement is usually made within 30 days.		
2.3.B Other payables		
Salaries	1908	692
Superannuation	252	127
Unearned income	6719	9817
Amortisation of rent expense	13 198	11 111
Lease incentives	1512	742
Fringe benefits tax	2322	2101
Total other payables	**25 911**	**24 590**
2.4 PROVISIONS		
2.4.A Employee provisions		
Leave	75 256	71 186
Superannuation	-	261
Total employee provisions	**75 256**	**71 448**

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.

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 2017. 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.

	2017	2016
	$'000	$'000
2.4.B Restoration obligations	**4938**	**7374**
Carrying amount 1 July 2016	7374	6281
Additional provisions made	836	-
Provision utilised	(1000)	(1000)
Lease expiry	(2510)	-
Unwinding of discount or change in discount rate	238	204
Revaluation as at 30 June	-	1889
Closing balance	***4938***	***7374***

3. Funding

	Ordinary annual services	Capital budget	Equity injections
	$'000	$'000	$'000
3.1 APPROPRIATIONS			
3.1.A Annual Departmental appropriations			
2017			
Appropriation Act			
Annual appropriation[1]	**402 998**	28 092	14 103
PGPA Act			
Section 74 transfers	**26 493**	-	-
Total appropriation	**429 491**	**28 092**	**14 103**
Appropriation applied (current and prior years)	**(427 011)**	**(50 791)**	**(17 941)**
Variance	***2480***	***(22 699)***	***(3 838)***

1. Access to $22 000 withheld under section 51 PGPA Act.

Variances in 2016–17 are due to prior year Capital appropriations applied in the current year.

The following entities spend money from the Consolidated Revenue Fund on behalf of ASIO:
Department of Foreign Affairs and Trade relating to services overseas: $8.029m (2016: $7.249m).

2016			
Appropriation Act			
Annual appropriation[2]	381 081	35 100	13 973
PGPA Act			
Section 74	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***	***3838***

2. $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 Capital appropriations applied in the current year and appropriations unspent due to the timing of asset purchases.

	2017	2016
	$'000	$'000
3.1.B Unspent departmental annual appropriations (recoverable GST exclusive)		
Appropriation Act (No. 1) 2016–17	84 338	-
Appropriation Act (No. 1) 2015–16	-	99 214
Appropriation Act (No. 2) 2015–16	-	3838
Appropriation Act (No. 1) 2014–15	-	5342
Total	**84 338**	**108 394**

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 surplus (deficit) excluding depreciation and amortisation	**2490**	**(5352)**
Depreciation and amortisation	(88 335)	(76 111)
Deficit as per statement of comprehensive income	(85 845)	(81 463)

4. Managing uncertainties

	2016 $'000	2015 $'000

4.1 CONTINGENT ASSETS AND LIABILITIES

Quantifiable contingencies

ASIO has no quantifiable contingent assets or liabilities as at 30 June 2017 (2016: Nil).

Unquantifiable contingencies

At 30 June 2017, 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.

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

	2016 $'000	2015 $'000
Financial assets		
Loans and receivables		
Cash	**17 338**	22 433
Trade receivables	**4753**	3423
Accrued revenue	**1644**	711
Total financial assets	**23 735**	**26 567**
Financial liabilities		
At amortised cost		
Trade creditors and accruals	**11 865**	6083
Total financial liabilities	**11 865**	**6083**

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 2017 (2016: Nil).

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.

5. Other information

	2017	2016
	$'000	$'000

5.1 KEY MANAGMENT PERSONNEL REMUNERATION

Key management personnel are those persons having authority and responsibility for planning, directing and controlling the activities of ASIO, directly or indirectly. ASIO has determined key management personnel to be the Director-General and members of the Executive Board.

Short-term employee benefits	1606	1536
Long-term employee benefits	189	186
Post-employment benefits	264	283
Total key management personnel remuneration expenses[1]	**2059**	**2005**

The total number of key management personnel included above is 7. (2016: 4)

Several key management positions were occupied by different officers for portions of the year. The number of key management positions remains at 4.

1. The above key management personnel remuneration excludes the remuneration and other benefits of the:

- Portfolio Ministers whose remuneration and other benefits are set by the Remuneration Tribunal and are not paid by ASIO; and
- External member of ASIO's Executive Board who is an executive of another Australian Government entity. No remuneration or other benefits are paid by ASIO.

5.2 RELATED PARTY DISCLOSURES

Related party relationships

ASIO is an Australian Government controlled entity. ASIO's related parties are Key Management Personnel including the Portfolio Ministers and Executive Board, and other Australian Government entities.

Transactions with Key Management Personnel

Given the breadth of Government activities, Key Management Personnel and their associates may transact with the government sector in the same capacity as ordinary citizens. Such transactions include the payment or refund of taxes, receipt of a Medicare rebate or higher education loans. These transactions are not disclosed in this note.

There were no transactions with Key Management Personnel during 2016–17.

Transactions with other Australian Government entities

ASIO transacts with Commonwealth Government entities at arm's length for the provision of goods and services in the normal course of business. These transactions are not disclosed in this note.

ASIO has a significant relationship with the Department of Finance as lessor of the organisation's headquarters in Canberra. Lease payments were $21.442m in 2016–17.

5.3 MAJOR BUDGET VARIANCES

The nature and timing of the Commonwealth's budget process meant the original Budget in the 2016–17 Portfolio Budget Statements was published in May before the closing 2015–16 and opening 2016–17 Statement of Financial Position was known. As a consequence, the opening balances of the Statement of Financial Position were estimated and in some cases variances between the 2016-17 final outcome and original Budget can, in part, be attributed to the flow on effects of unanticipated movement in prior year figures.

The Budget Statement of Comprehensive Income, net of unfunded depreciation, presumed a balanced operating result in 2016–17 consistent with the requirement under the Commonwealth budgeting framework. Variances between the 2016–17 final outcome and original Budget can, in part, be attributed to this assumption.

Departmental expenses

The total variation between departmental expenses and the original Budget estimate is an increase of $9.998m (2 per cent). The overall increase in expenses can be attributed to:

- the budgeted number of (full time equivalent) employees was lower than actual due to a higher than anticipated growth of ASIO employees in late 2015–16, resulting in higher than the Budget employee expenses.
- supplier expenses were less than anticipated in the original Budget largely as the result of a re-prioritisation of resources to the completion of non financial assets. The increase to depreciation resulting from the re-prioritisation of expenditure was also not budgeted for ($12.169m).

Departmental revenue

The total variation between departmental revenue and the original Budget estimate is $0.319m (less than 1 per cent). This consists mainly of own-source revenue:

- sales of goods and services is $3.378m (18 per cent) lower than budgeted due to a 2016–17 change in the cost recovery policy for protective security activities.
- the end of ASIO's obligation for its previous headquarters resulted in a gain on settlement of the lease of $2.320m. This was not anticipated in the original Budget.

Departmental assets

Total departmental assets are $0.999m (less than 1 per cent) less than the original Budget position. The variance for financial assets is $6.154m below the Budget estimate mostly as a result of the interrelationship with departmental expenses and revenue. Non financial assets are higher by $7.153m (2 per cent) due to:

- a net increase in software ($4.965m) due to redirection of resources to complete software work in progress.
- a net increase in land and buildings ($6.544m) mainly attributable to additional office operating leases and resulting restoration obligations which were unknown at the time of Budget preparation.
- higher than expected prepayments ($13.047m) due to realignment of the timing of large software maintenance contract renewals.

These positive variances to non-financial assets were offset by negative variances to property, plant and equipment ($17.403m) mainly because of higher than budgeted depreciation as a result of the re-prioritisation of resources noted above. The higher depreciation was a result of reductions to the useful lives of some assets (accelerating depreciation) and a higher asset base as some of these assets were put into service.

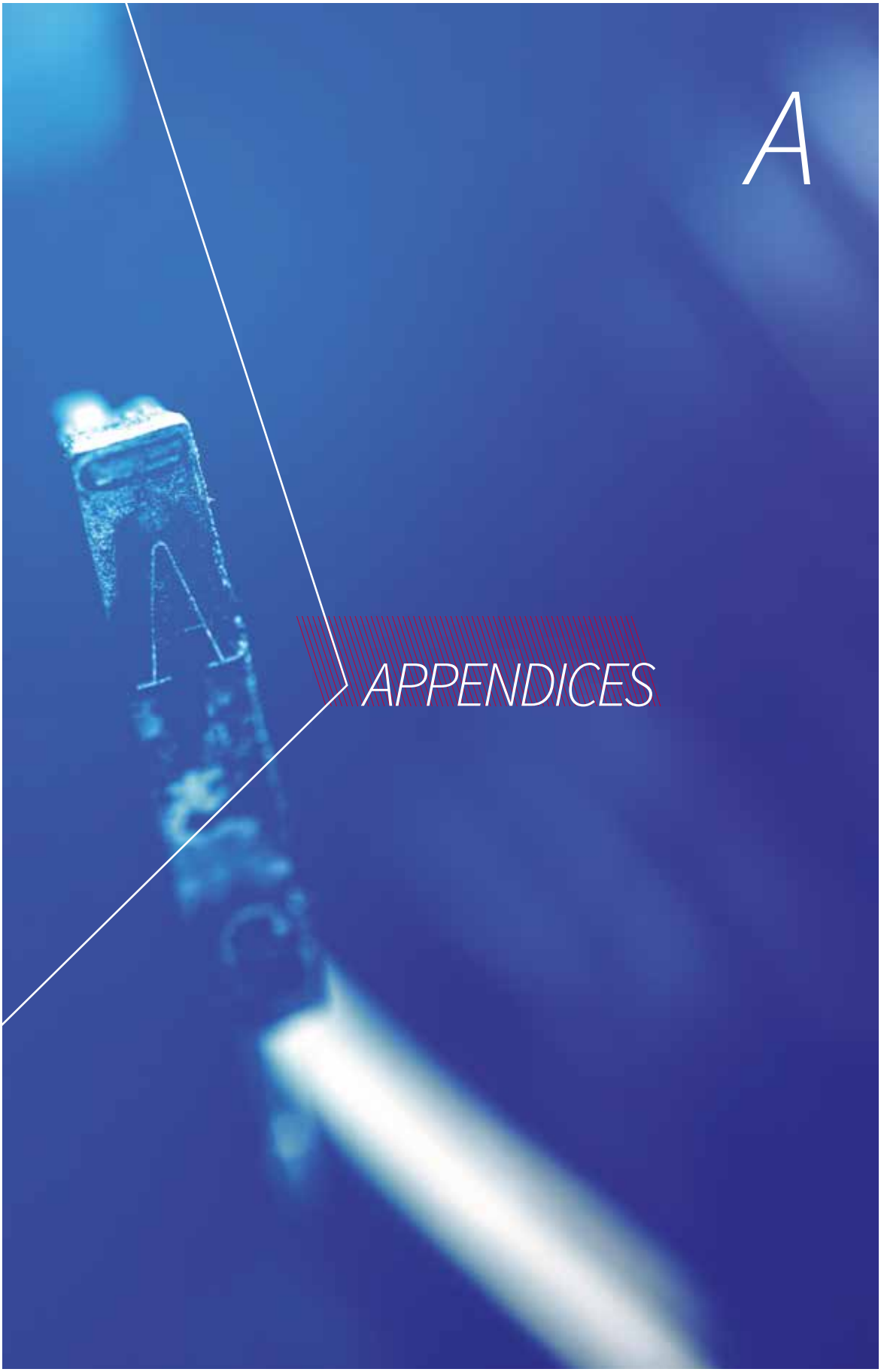
Departmental liabilities

Total departmental liabilities are $2.161m (2 per cent) more than the original Budget position. Significant (offsetting) variances within the result include:

- lower supplier payables and accrued expenses ($13.887m) due to the flow on of:
  - movement in prior-year figures; and
  - lower than anticipated supplier expenses.
- higher employee provisions due to unanticipated growth of the employee base in late 2015–16.
- higher salaries and superannuation payable ($1.341m) due to the timing of pay days and year ends.
- higher amortisation of rent expense ($2.087m) as a result of the extension of several leases.

Statement of Cash Flows

The amounts reported in the Statement of Cash Flows are interrelated with figures disclosed in the Statement of Comprehensive Income and Statement of Financial Position. Consequently, variances in this Statement will be attributable to the relevant variance explanations provided above and under departmental expenses, departmental revenue, departmental assets and departmental liabilities.



A

APPENDICES

Appendix A—agency resource statement

	Actual available appropriation 2016–17 $'000	Payments made 2016–17 $'000	Balance remaining 2016–17 $'000
ORDINARY ANNUAL SERVICES[1]			
Departmental appropriation			
Prior year appropriation[2]	76 781*	82 123	(5342)
2016–17 appropriation[3]	402 998*	340 998	62 000
S74 relevant agency receipts[4]	26 493*	26 493	-
2016–17 capital budget	28 092*	23 092	5000
Cash on hand	22 433	5095	17 338
Total ordinary annual services	***556 797***	***477 802***	***78 996***
OTHER SERVICES			
Departmental non-operating[5]			
Prior year equity injections	3838*	3838	-
Equity injections	14 103*	14 103	-
Total other services	***17 941***	***17 941***	***-***
TOTAL NET RESOURCING AND PAYMENTS	**574 738**	**495 743**	

[1] Appropriation Bill (No.1), Appropriation Bill (No.3), Supply Bill (No.1) and Supply Bill (No.3).

[2] Includes an amount of $27.1m from 2015–16 for the Departmental Capital Budget. For accounting purposes this amount has been designated as 'contributions by owners'.

[3] $403.020m per Portfolio Budget Statement less $0.022m withheld under PGPA Act section 51.

[4] $21.398m per Portfolio Budget Statement plus $5.095m underestimate at time of PBS.

[5] Appropriation Bill (No.2) & Appropriation Bill (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* 2016–17 $'000	Actual Expenses 2016–17 $'000	Variation 2016–17 $'000
Program 1.1: Security Intelligence			
Departmental expenses			
Appropriation[1]	402 998	402 998	-
Expenses not requiring appropriation in the Budget year	76 311	88 480	(12 169)
Total for Program 1.1	***479 309***	***491 478***	***(12 169)***
Total expenses for Outcome 1	**479 309**	**491 478**	**(12 169)**

***** as per Portfolio Budget Statements including adjustments made at Additional Estimates and reductions under PGPA Act section 51.

[1] Ordinary annual services (Appropriation Act no.s 1 and 3 including reductions under PGPA Act section 51) and Retained Revenue Receipts under section 74 of the PGPA Act 2013.

Appendix C—workforce statistics

Full-time equivalent actual

2015–16	**1746.3**
2016–17	**1794.3**

Note:
Figures reported in this table are FTE actual. Data for 2015–16 has been retrospectively amended from FTE nominal for consistency in reporting.

Head count of staff by load and employment status

	2015–16			2016–17		
	Ongoing	**Non-ongoing**	**Total**	**Ongoing**	**Non-ongoing**	**Total**
Full-time	1567	10	**1577**	1611	12	**1623**
Part-time	225	15	**240**	240	18	**258**
Casual	N/A	59	**59**	N/A	50	**50**
Total	**1792**	**84**	**1876**	**1851**	**80**	**1931**

Note:
To align the reporting of ASIO's workforce metrics, the following changes apply compared to the 2015–16 Annual Report. Data has been retrospectively amended for 2015–16 for comparative purposes.
• Data includes the Director-General.
• Non-ongoing employees do not include locally engaged staff and secondees.

Head count of staff by gender and employment status

	2015–16				2016–17			
	Ongoing	**Non-ongoing**	**Casual**	**Total**	**Ongoing**	**Non-ongoing**	**Casual**	**Total**
Female	811	8	14	**833**	844	10	14	**868**
Male	981	17	45	**1043**	1007	20	36	**1063**
Total	**1792**	**25**	**59**	**1876**	**1851**	**30**	**50**	**1931**

Note:
To align the reporting of ASIO's workforce metrics, the following changes apply compared to the 2015–16 Annual Report. Data has been retrospectively amended for 2015–16 for comparative purposes.
• Data includes the Director-General.
• Non-ongoing employees do not include locally engaged staff and secondees.

Head count of employees by classification and employment status

		2015–16				2016–17			
		Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Director-General		1	0	0	**1**	1	0	0	**1**
Senior Executive Service	SES Band 3	2	0	0	**2**	2	0	0	**2**
	SES Band 2	12	1	0	**13**	11	0	2	**13**
	SES Band 1	34	2	1	**37**	34	2	1	**37**
Senior officers	AEE2/3	156	3	1	**160**	175	3	1	**179**
	AEE1	373	3	4	**380**	365	3	3	**371**
Employees	AE1 to AE6 (including technical specialists)	1214	16	53	**1283**	1 263	22	43	**1328**
Total		**1792**	**25**	**59**	**1876**	**1851**	**30**	**50**	**1931**

Note:
To align the reporting of ASIO's workforce metrics, the following changes apply compared to the 2015–16 Annual Report. Data has been retrospectively amended for 2015–16 for comparative purposes.
• Data includes the Director-General.
• Non-ongoing employees do not include locally engaged staff and secondees.

A

Head count of employees by location and employment status

	2015–16				2016–17			
	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Canberra-based	1263	17	42	**1322**	1320	18	37	**1375**
Other locations	529	8	17	**554**	531	12	13	**556**
Total	**1792**	**25**	**59**	**1876**	**1851**	**30**	**50**	**1931**

Note:
To align the reporting of ASIO's workforce metrics, the following changes apply compared to the 2015–16 Annual Report. Data has been retrospectively amended for 2015–16 for comparative purposes.
• Data includes the Director-General.
• Non-ongoing employees do not include locally engaged staff and secondees.

Diversity of ASIO employees showing head count and percentage

	2015–16		2016–17	
Available data	1751	93.0%	1805	93.5%
Identify as Indigenous	10	0.6%	12	0.7%
People with a disability	9	1.1%	19	1.1%
Non-English speaking background	106	6.1%	324	18.0%

Notes:

1. Percentage of available data calculated using the total head count.
2. Percentages of employees identifying as Indigenous, with a disability, or from a non-English speaking background calculated using the head count of available data.
3. Data includes the Director-General and excludes secondees, locally engaged staff and contractors.
4. Provision of EEO data is voluntary. Data is considered 'available' if a staff member has provided information on at least one diversity category.

Appendix D—ASIO's salary classification structure

Senior Executive Service	
SES Band 3	$317 781 minimum point
SES Band 2	$247 250 minimum point
SES Band 1	$197 800 minimum point
Senior employees	
AEE3	$152 177
AEE2	$128 592–152 177
AEE1	$112 198–125 377
Employees	
AE6	$88 268–99 459
AE5	$79 862–85 731
AE4	$72 767–78 088
AE3	$64 360–70 337
AE2	$56 610–62 694
AE1	$48 859–54 266
Intelligence employees	
IE	$88 268–99 459
IE trainees	$77 862–94 030
Information technology employees	
SITEA	$152 177
SITEB	$128 592–152 177
SITEC	$112 198–125 377
ITE2	$88 268–99 459
ITE1	$76 873–84 517
Engineers	
SIE(E)5	$152 177
SIE(E)4	$128 592–152 177
SIE(E)3	$112 198–125 377
SIE(E)2	$88 268–99 459
SIE(E)1	$76 873–84 517

Notes: Figures at 30 June 2017. 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 Independent Reviewer, Robert Cornall AO, conducts an independent advisory review of ASIO adverse security assessments furnished to the Department of Immigration and Border Protection in relation to those 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 Independent Reviewer's terms of reference are available at www.ag.gov.au/asareview.

The terms of reference provide for an initial primary review of each adverse security assessment and subsequent periodic reviews every 12 months for the duration of that assessment.

In performing his task, the Independent Reviewer examines all of the ASIO material that was relied upon by ASIO in making the adverse assessment as well as other relevant material, which may include submissions or representations made by the eligible person. The Independent 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.

On 1 July 2016, there were only four matters remaining within the Independent Reviewer's jurisdiction and no new matters arose during the year. The four cases were all finalised during 2016–17.

Dealing first with the two periodic reviews, it is important to note that ASIO also undertakes internal reviews of adverse security assessments of its own volition. Pursuing a periodic review at the same time as ASIO is processing an internal review can generate unnecessary work for the applicant and his or her advisers because:

- if the ASIO review results in a qualified or non-prejudicial security assessment, there is no need for the proposed periodic review of the earlier adverse assessment, or
- if the ASIO review results in renewed adverse security assessment, that new assessment will be subject to a primary review in accordance with the Independent Reviewer's terms of reference.

The solicitors for both applicants agreed to defer the periodic review until the completion of ASIO's internal review. In each case, ASIO furnished the Department of Immigration and Border Protection with a qualified security assessment in respect of the applicant and the Independent Reviewer's role in those two matters came to an end.

In relation to the two primary reviews, the Independent Reviewer disagreed with ASIO's assessment. The Reviewer expressed the opinion that the adverse security assessment was not an appropriate outcome and recommended that ASIO furnish a qualified security assessment instead.

The Independent Reviewer provides only an advisory opinion and advice. However, following consideration of each primary review report, the Director-General of Security decided to furnish a qualified security assessment for both applicants.

In summary, in the 57 matters referred to the Independent Reviewer since December 2012, the applicants have all received a qualified or non-prejudicial security assessment.

As a result, there were no matters falling within the Independent Reviewer's terms of reference on 30 June 2017.

Appendix F—report on use of questioning warrants and questioning and detention warrants

ASIO is required under section 94 of the ASIO Act to provide in its annual report details of its use of questioning warrant and question and detention warrants during this reporting period. The details are provided in the following table.

Subsection	Description	2015–16	2016–17
94(1)(a)	The total number of requests made under Division 3 of Part III to issuing authorities for the issue of warrants under that division.	0	0
94(1)(b)	The total number of warrants issued under that division.	0	0
94(1)(c)	The total number of warrants issued 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 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 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 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 them under warrants issued .	0	0

List of annual report requirements under schedule 2 of the PGPA Rule

Below is the table set out in Schedule 2 of the PGPA Rule. Subsection 17AJ(d) of the PGPA Rule requires annual reports of Australian Government entities to include this table as an aid for accessibility.

PGPA Rule reference	Part of Report	Description	Requirement	Part of this report
17AD(g)	**Letter of transmittal**			
17AI		A copy of the letter of transmittal signed and dated by an accountable authority on the date final text was approved, with a statement that the report has been prepared in accordance with section 46 of the PGPA Rule and any enabling legislation that specifies additional requirements in relation to the annual report.	Mandatory	Letter of transmittal
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	Preliminaries
17AJ(f)		Entity's website address	Mandatory	Preliminaries
17AJ(g)		Electronic address of report	Mandatory	Preliminaries
17AD(a)	**Review by accountable authority**			
17AD(a)		A review by the entity's accountable authority.	Mandatory	Part 1
17AD(b)	**Overview of the entity**			
17AE(1)(a)(i)		A description of the entity's role and functions.	Mandatory	Part 2
17AE(1)(a)(ii)		A description of the entity's organisational structure.	Mandatory	Part 2
17AE(1)(a)(iii)		A description of the entity's outcomes and programs administered.	Mandatory	Part 2
17AE(1)(a)(iv)		A description of the entity's purposes as included in ASIO's corporate plan.	Mandatory	Part 2
17AE(1)(b)		An outline of the structure of the portfolio of the entity.	Mandatory for portfolio departments	N/A

PGPA Rule reference	Part of Report	Description	Requirement	Part of this report
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 reporting period, details of the variation and reasons for changes are provided.	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 PGPA Act and section 16F of the PGPA Rule.	Mandatory	Part 4
17AD(c)(ii)	***Report on financial performance***			
17AF(1)(a)		A discussion and analysis of the entity's financial performance.	Mandatory	Part 4
17AF(1)(b)		A table summarising the entity's total resources and total payments.	Mandatory	Appendices A and B
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 are provided, 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 can reasonably be anticipated will have a significant impact on the entity's future operation or financial results.	If applicable, mandatory	N/A
17AD(d)	**Management and accountability**			
	Corporate governance			
17AG(2)(a)		Information on compliance with section 10 (fraud systems).	Mandatory	Letter of transmittal and Part 5
17AG(2)(b)(i)		Certification by an accountable authority that fraud risk assessments and fraud control plans have been prepared.	Mandatory	Letter of transmittal
17AG(2)(b)(ii)		Certification by an 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 of this report
17AG(2)(b)(iii)		Certification by an 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	Part 5
17AG(2)(d)–(e)		A statement of significant issues reported to the minister under paragraph 19(1)(e) of the PGPAAct 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	Part 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 entity's operations.	If applicable, mandatory	Part 5
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.	If applicable, mandatory	Part 5
	Management of human resources			
17AG(4)(a)		An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives.	Mandatory	Part 5

PGPA Rule reference	Part of Report	Description	Requirement	Part of this report
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; and ▶ 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	Part 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 the 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	Part 5

PGPA Rule reference	Part of Report	Description	Requirement	Part of this report
		Consultants		
17AG(7)(a)		A summary statement detailing the number of new contracts engaging consultants entered into during this reporting period; the total actual expenditure (inclusive of GST) on all new consultancy contracts entered into during this reporting period; the number of ongoing consultancy contracts that were entered into during the previous reporting period; and the total actual expenditure (inclusive of GST) on the ongoing consultancy contracts in this reporting period.	Mandatory	Part 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 , involving total actual expenditure of $[specified million]'.	Mandatory	Part 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	Part 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	Part 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	Part 5

PGPA Rule reference	Part of Report	Description	Requirement	Part of this report
	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 Freedom of Information Act (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	Part 5
	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	Part 5
17AG(10)(b)		An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	Part 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	Part 5
	Financial statements			
17AD(e)		Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act.	Mandatory	Part 6

PGPA Rule reference	Part of Report	Description	Requirement	Part of this report
17AD(f)	**Other mandatory information**			
17AH(1)(a)(i)		If the entity conducted advertising campaigns, a statement that, 'During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity's website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website'.	If applicable, mandatory	Part 5
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)		An outline of mechanisms of disability reporting, including reference to a website for further information.	Mandatory	Part 5
17AH(1)(d)		A website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found.	Mandatory	N/A (FOI exempt)
17AH(1)(e)		Correction of material errors in the previous annual report.	If applicable, mandatory	Appendices
17AH(2)		Information required by other legislation.	Mandatory	Appendices

List of annual report requirements under other legislation

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 authorities; and authorisations for telecommunications data.

Requirement	Refer to
Report on questioning warrants and questioning and detention warrants.	Appendix F
Report on special intelligence operation authorities.	Appendix G
Report on authorisations for telecommunications data.	Appendix H

In line with determinations made by the Attorney-General and the Minister for Finance under the PGPA Act, Appendices G and H have been deleted from the public version of the annual report to avoid prejudice to ASIO's activities.

Correction of errors in 2015–16 annual report

Our 2015–16 annual report stated that:

> 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.*

This statement requires clarification. There are some instances involving highly sensitive cases where, at the discretion of the Director-General, warrants are provided directly to the Attorney-General without being reviewed by AGD. In these cases, the Attorney-General is informed that the department has not been involved in progressing the respective warrants. There is no legislative requirement for AGD to review each warrant.

Abbreviations and short forms

A

AASB—Australian Accounting Standards Board

AASB119—Australian Accounting Standards Board Standard 'Employee Benefits'

ABF—Australian Border Force

ACSC—Australian Cyber Security Centre

AE—ASIO employee

AEE—ASIO executive employee

AFP—Australian Federal Police

AGD—Attorney-General's Department

AGSVA—Australian Government Security Vetting Agency

AIC—Australian Intelligence Community

ANZCTC—Australia–New Zealand Counter-Terrorism Committee

ASIC—Aviation Security Identification Card

ASIO Act—*Australian Security Intelligence Organisation Act 1979*

ASIO2020—ASIO's strategic organisational reform program

ASIO—Australian Security Intelligence Organisation

ASIO–T4—ASIO's Protective Security Directorate

B

BGLU—Business and Government Liaison Unit

C

CRS—Contact Reporting Scheme

CVE—countering violent extremism

D

DCB—Departmental Capital Budget

DFAT—Department of Foreign Affairs and Trade

DIBP—Department of Immigration and Border Protection

E

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

F

FIRB—Foreign Investment Review Board

G

GST—Goods and services tax

I

ICT—information and communications technology

IE—intelligence employees

IGIS—Inspector-General of Intelligence and Security

INSLM—Independent National Security Legislation Monitor

ISIL—Islamic State of Iraq and the Levant

ITE—information technology employee

J

JCTT—Joint Counter-Terrorism Team

M

MSIC—Maritime Security Identification Card

N

NDG—National Disruption Group

NTAC—National Threat Assessment Centre

O

OSB—Operation Sovereign Borders

ORSC—Operational Risk Steering Committee

P

PBS—Portfolio Budget Statement

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

PIIs—potential illegal immigrants

PJCIS—Parliamentary Joint Committee on Intelligence and Security

PSPF—Protective Security Policy Framework

PV—Top Secret 'positive vetting' security clearance

S

SES—senior executive service

SIE(E)—specialist intelligence employee (engineer)

SITE—senior information technology employee

T

TISN—trusted information sharing network

TSCM—technical surveillance countermeasures

W

WHS—work health and safety

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

espionage—the theft of Australian information or capability by person/s acting either 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 interference—activities relating to Australia that are carried on by, or on behalf of, a foreign power; are directed or subsidised by a foreign power; or are undertaken in active collaboration with a foreign power. These activities:

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.

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 enable preventative action, including by partner agencies.

jihadist—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—trusted employees and contractors who deliberately and wilfully 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—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