Australian Government

Australian Security Intelligence Organisation

ASIO Annual Report 2017–18

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

Each year since 2014, ASIO has held a photography competition inviting staff to submit images for inclusion in the annual report. A selection of the images provided by staff appear as the part pages from part 2 through to the Appendices.

ASIO ANNUAL REPORT 2017–18

Australian Government
Australian Security Intelligence Organisation

Director-General of Security

The Hon. Peter Dutton MP
Minister for Home Affairs
Parliament House
CANBERRA ACT 2600

25 September 2018
Ref: A15228889

Dear Minister,

ASIO annual report 2017-18

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 2017–18

This report contains information required by the PGPA Rule 2014 and section 94 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). In order to ensure compliance with the Determination made by the Minister for Finance under section 105D of the PGPA Act, the statements required under subsection 94(2A) of the ASIO Act relating to special intelligence operations and telecommunications data authorisations have been removed from the annual report tabled in the Parliament in order to avoid prejudice to ASIO's activities These statements will be separately provided to you and, as required by the ASIO Act, to the Leader of the Opposition. The statement relating to telecommunications data authorisations will also be provided to the Parliamentary Joint Committee on Intelligence and Security.

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

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

Contents

1 DIRECTOR-GENERAL'S REVIEW *1*

2 OVERVIEW OF ASIO *9*

3 AUSTRALIA'S SECURITY ENVIRONMENT AND OUTLOOK *17*

4 REPORT ON PERFORMANCE *29*

ASIO annual performance statement 2017–18 31

Key activity 1: counter terrorism 33

Key activity 2: counter espionage, foreign interference and malicious insiders 38

Key activity 3: counter serious threats to Australia's border integrity 44

Key activity 4: provide protective security advice to government and industry 47

Analysis of performance 51

Report on financial performance 53

5 MANAGEMENT AND ACCOUNTABILITY *55*

Corporate governance 57

External scrutiny 61

Management of human resources 66

Property and procurement 73

6 *FINANCIAL STATEMENTS* *77*

A *APPENDICES* *105*

Appendix A: agency resource statement 107

Appendix B: expenses by outcomes 108

Appendix C: workforce statistics 109

Appendix D: ASIO's salary classification structure 112

Appendix E: report of the Independent Reviewer of Adverse Security Assessments 113

Appendix F: report on use of questioning warrants and questioning and detention warrants 114

List of annual report requirements under schedule 2 of the Public Governance, Performance and Accountability Rule 115

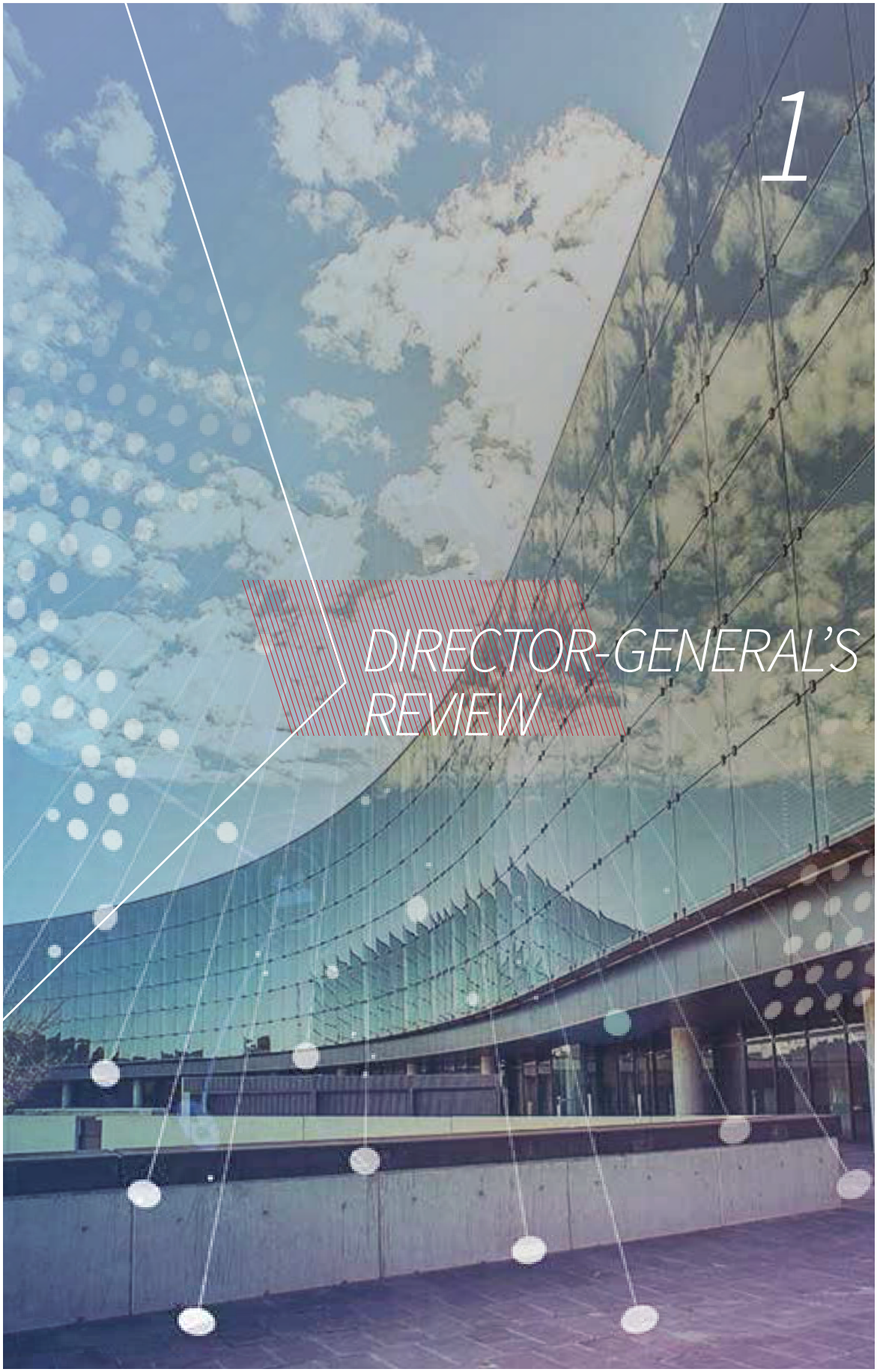
List of annual report requirements under other legislation 121

Correction of errors in 2016–17 annual report 122

Abbreviations and short forms 123

Glossary 125

Index 127



1

DIRECTOR-GENERAL'S REVIEW

Director-General's review

In 2017–18 we saw the significant challenges posed by espionage and foreign interference come to prominence in Australia in public and parliamentary debates. It was an important debate for the nation, and one that ASIO—as the nation's security service responsible for protecting Australia from these threats—welcomed. Espionage and foreign interference represent a serious threat to Australia's sovereignty and security and the integrity of our national institutions. Foreign actors are aggressively seeking access to privileged and classified information on Australia's alliances and partnerships; position on international diplomatic, economic and military issues; energy and mineral resources; and innovations in science and technology. They are also attempting to clandestinely influence the opinions of members of the Australian public and media, Australian Government officials, and members of Australia-based diaspora communities.

During this reporting period, ASIO continued to discover, investigate and disrupt harmful espionage and foreign interference affecting Australia's national interests. We worked with Australian Government policymakers and provided advice to support parliament's consideration of legislative measures to strengthen Australia's efforts to counter these threats. The passage of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* and the *Foreign Influence Transparency Scheme Act 2018* represents a significant reform that will assist ASIO and our law enforcement partners to more effectively respond to harmful espionage and foreign interference, including through prosecution, and provide greater public transparency of foreign influence in Australia.

The July 2017 disruption of a plot to use an improvised explosive device against an Etihad flight departing Sydney and a potential plot to use toxic gas in a terrorist attack (Operation Silves) reinforced the persistent and serious nature of the terrorist threat to Australians and Australian interests. In addition to identifying a key individual involved in the plot and providing support for the disruption by law enforcement agencies, ASIO provided a wide range of assessments and advice to assist regulators, policymakers and industry develop improved aviation, air cargo and international mail security arrangements. We also worked closely with law enforcement partners to successfully disrupt a separate plot to conduct a terrorist attack in Melbourne.

Terrorism also remained a significant security issue beyond our shores in 2017–18, despite the welcome decline in the Islamic State of Iraq and the Levant's (ISIL) capability in Syria and Iraq. In Australia's immediate region, we saw a pro-ISIL Indonesian network conduct the deadliest terrorism campaign in Indonesia in over a decade. In the Philippines, the ISIL-backed seizure of territory in the southern Philippines city of Marawi from May to October 2017 was the first time ISIL had held territory outside the Middle East and Africa. ASIO continued to provide advice and assessments to inform Australian Government efforts to support our regional security partners. On 8 September 2017, we provided an assessment that underpinned the proscription of Islamic State—East Asia (IS-EA) under the *Criminal Code Act 1995*. The proscription of IS-EA criminalises a range of activities that would provide support to the group and enables the prosecution of Australians undertaking activities on behalf or in support of the organisation.

A significant undertaking for ASIO during this reporting period was supporting security planning and accreditation for special events held in Australia, including the Gold Coast 2018 Commonwealth Games (GC18) and the ASEAN–Australia Summit. As part of this work we conducted over 70 000 assessments of individuals requiring accreditation for the events.

Movement into the Home Affairs portfolio

On 11 May 2018, ASIO officially transitioned into the Home Affairs portfolio. Within the portfolio, ASIO remains an independent statutory authority, operating under the *Australian Security Intelligence Organisation Act 1979*.

This move was an historic change for ASIO, having been in the Attorney-General's portfolio since the Organisation's inception in 1949. Along with the formation of the Office of National Intelligence (ONI), the creation of the Home Affairs portfolio reflects the need for Australia's security apparatus to become increasingly integrated and flexible to respond to the complex security issues facing the nation. The new arrangements provide an opportunity to further strengthen existing high levels of cross-agency cooperation on counter-terrorism, countering foreign interference and border security issues.

Transformation

In 2017, I commissioned Mr David Thodey AO to conduct a review of our approach to technology and its relationships with our approach to people, culture and collaboration. Mr Thodey's report, *A digital transformation of the Australian Security Intelligence Organisation*, recommended

that we change our business model to capitalise on the benefits of augmented decision-making and data science; establish a strong, digitally enabled culture; reform our human resources practices; establish strategic partnerships with industry, academia and government; and strengthen innovation within the Organisation.

In line with the review's recommendations, during this reporting period we commenced preparations for a major transformation to ensure ASIO remains fit for purpose in an increasingly complex security and operating environment.

Performance

We achieved or substantially achieved eight out of nine of the performance objectives outlined in our 2017–18 corporate plan. This assessment of our performance was confirmed by responses in our 2018 annual stakeholder survey. The survey was conducted by an independent senior reviewer with extensive national security experience, who interviewed 74 senior stakeholders from 66 federal, state and territory government bodies; industry; and academia. The reviewer found that ASIO:

- continues to be highly regarded as an effective partner offering high-quality and largely unique services; and
- is perceived as a very credible organisation, with officers that are customer-focused, well trained and professional.

We partially achieved one performance objective relating to foreign intelligence collection. This assessment of our performance recognises that, while our stakeholders valued our contributions in this area, we could not meet all of their requests to collect foreign intelligence.

The annual performance statements in part 4 of this annual report provide further detail on our achievements during 2017–18 and the value of our work to our national security partners.

In relation to financial performance, ASIO achieved a small surplus of $0.972 million (excluding depreciation), which represents 0.2 per cent of our budget (see the report on financial performance in part 4). In 2018–19 we will review and further consider the sustainability of our current operations in light of our anticipated future operating environment and significant pressures on our operating and departmental capital budgets.

Outlook

Australia's security and operating environment will remain complex and challenging for the foreseeable future, with heightened terrorism, espionage and foreign interference threats compounded by rapidly changing technologies that assist adversaries to cause harm, conceal their activities and uncover our efforts to discover them.

The implementation of ASIO's organisational transformation program will be a major priority in 2018–19. The transformation will play a vital role in ensuring ASIO stays ahead of the security threats facing the nation. We will work with our Home Affairs and our national security partners to ensure our collective knowledge and capabilities continue to be effectively coordinated and deployed to safeguard Australians and Australian interests. We will also contribute to the Comprehensive Review into the Legal Framework of the National Intelligence Community, led by former Director-General of Security Mr Dennis Richardson AO, to inform that review's consideration of whether Australia's intelligence legislation remains fit for purpose.

Our core business—identifying and investigating security threats, and providing security intelligence and advice to our national security partners in federal, state and territory governments; law enforcement; industry; and academia—will continue at a fast tempo. The increased awareness of the espionage and foreign interference threat has come with an increasing demand from partners for ASIO assessments and advice. We will continue in 2018–19 to build our capability and capacity to service this growing demand.

ASIO at a glance 2017–18

2 **Disruptions of planned terrorist attacks** in Australia with law enforcement partners

14 227 Counter-terrorism leads resolved or investigated

Assessments and reporting

5454 Visa security assessments

32 153 Personnel security assessments

160 Evaluations of security products and Zone 5 site inspection reports

71 254 Event accreditation assessments

1440 **Published reports** on terrorism, espionage, foreign interference and border security issues

245 Assessments on **foreign investment** proposals

3262 Government and industry subscribers to our **Business and Government Liaison Unit** website

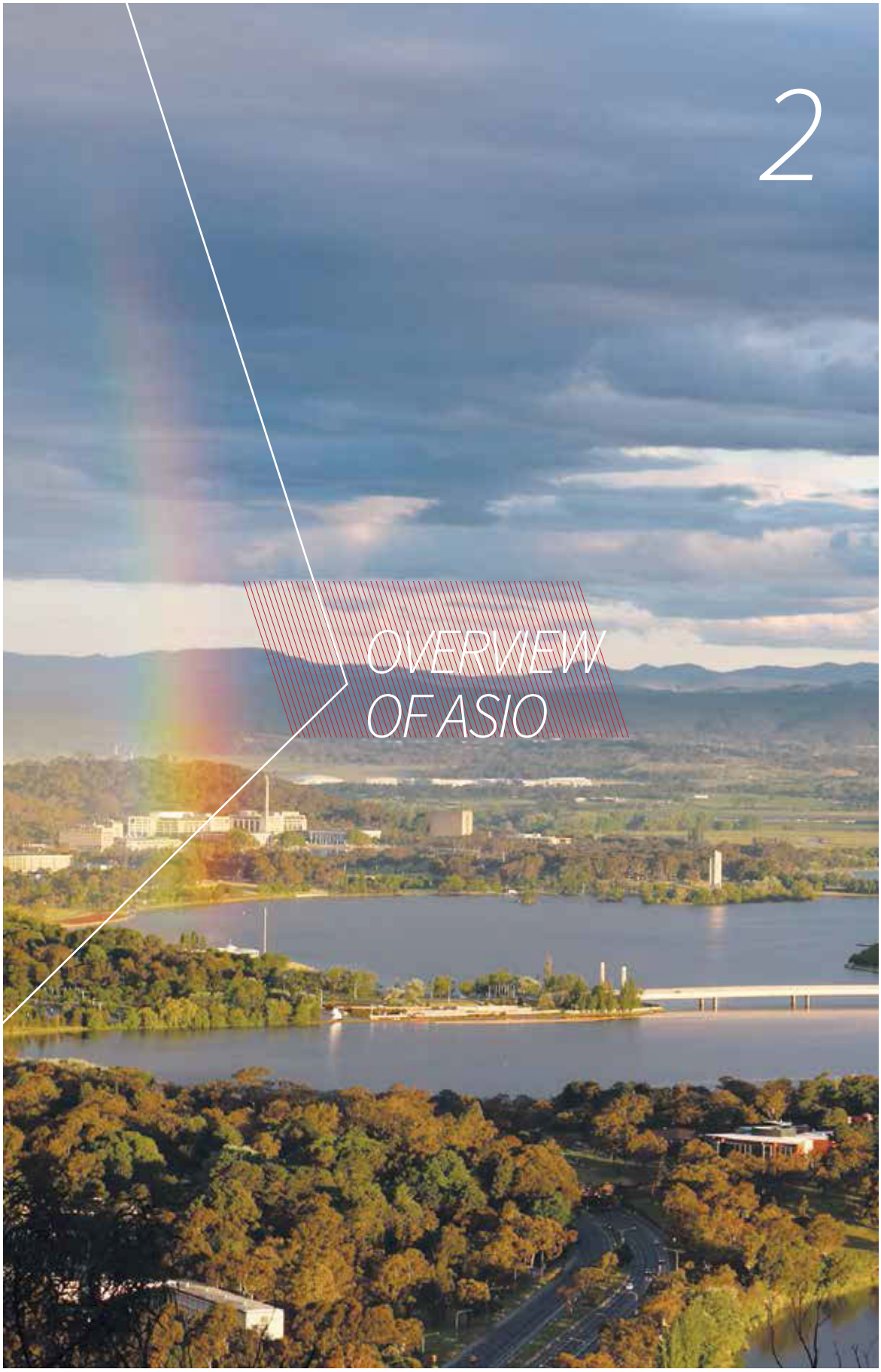
144 629 **Security assessments** for access to sensitive sites or materials

Budget and people

$533.449m budget

91% staff high job satisfaction (staff survey)

1980 employees



2

OVERVIEW OF ASIO

Overview of ASIO

ASIO's purpose is to protect Australia, 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 industry.[1] Our functions are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act).

In 2017–18 we pursued our purpose through four key activities:

1. counter terrorism;
2. counter espionage, foreign interference and malicious insiders;
3. counter serious threats to Australia's border integrity; and
4. provide protective security advice to government and industry.

[1] This purpose statement is included in ASIO's corporate plan 2017–18 and reflects our outcome in the ASIO Portfolio Budget Statement 2017–18. This outcome is supported by Program 1.1: security intelligence.

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

What we do

- counter terrorism
- counter espionage, foreign interference and malicious insiders
- counter serious threats to Australia's border integrity
- provide protective security advice to government and industry

How we do it

1 Harness our unique intelligence capabilities, partnerships and partner information

2 Apply rigorous data-driven analysis contextualised with our deep subject matter expertise

3 Anticipate threats and produce trusted and actionable advice to protect Australia

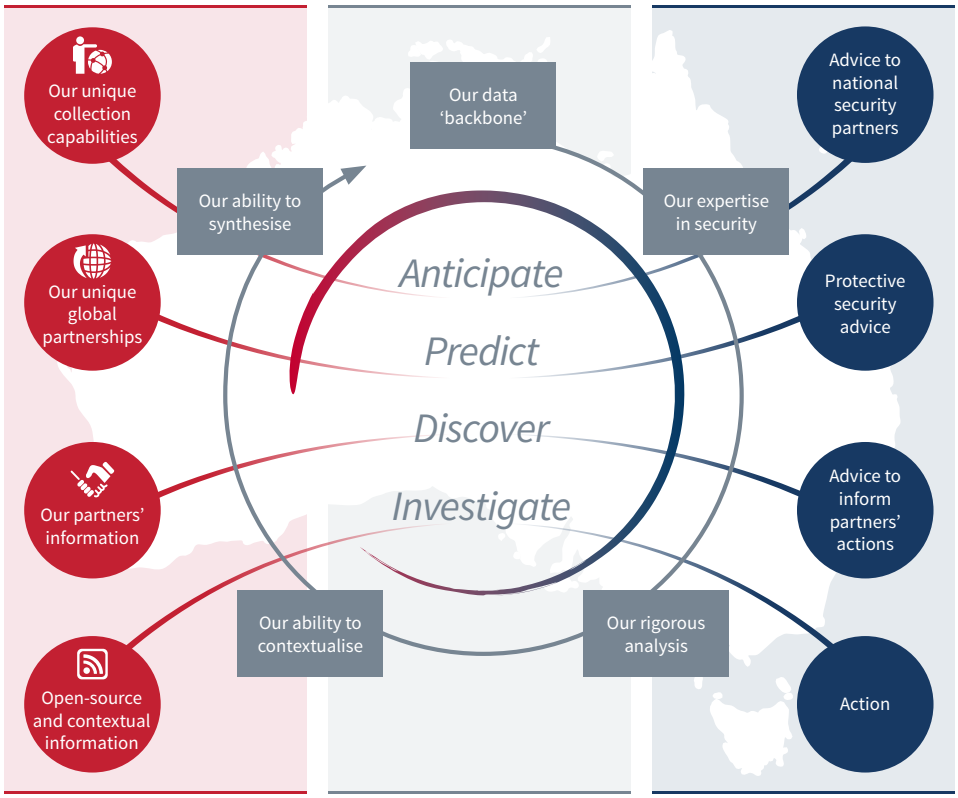


Figure 1: ASIO—what we do and how we do it

A commitment to legality and propriety

In working to meet our purpose, we must operate in a manner that is consistent with our values of excellence, integrity, respect, cooperation and accountability. These five values incorporate our firm commitment to operate lawfully, in proportion to threats we are investigating, and in line with the standards and expectations of the Australian community. A comprehensive oversight and accountability framework comprising legislation and ministerial, parliamentary and independent oversight provides assurance that we will continue to meet our commitment.

Organisational structure

An overview of ASIO's organisational structure is provided in Figure 2.

Organisational structure

as at 30 June 2018

Duncan Lewis

DIRECTOR-GENERAL OF SECURITY

- Chief Transformation Officer
- Chief Digital Advisor

Deputy Director-General
STRATEGIC ENTERPRISE MANAGEMENT GROUP

- New policy implementation

Deputy Director-General
OPERATIONAL SUPPORT AND CAPABILITIES GROUP

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

- Assurance
- Internal Security
- Assessments, Corporate Law and Capability Protection
- Data and Technical Analysis
- Strategic Partnerships and Production
- Financial Management
- Operations Law
- Telecommunication Operations
- Organisational Strategy, Policy and Reform
- Human Resources
- Litigation
- Computer Operations
- State Manager Qld
- Territory Manager NT
- Territory Manager ACT
- Ministerial, Media and Communication
- State Manager SA
- State Manager WA
- State Manager Tas.
- Property
- People Strategy
- Close Access Operations
- Strategy and Performance

Figure 2: ASIO's organisational structure at 30 June 2018

Deputy Director-General
OPERATIONS AND ASSESSMENTS GROUP

Operations and Assessments Capability and Strategy

Operational Capabilities	Information	Counter-Espionage and Interference	Counter-Terrorism	Security Advice and Assessments	Centre for Counter-Terrorism Coordination
Physical Surveillance	IT Infrastructure Services	Counter-Espionage and Interference A	Counter-Terrorism Coordination	National Threat Assessment Centre	Centre for Counter-Terrorism Coordination
Operations Services	Business Information Systems	Counter-Espionage and Interference B	Counter-Terrorism Investigations 1	Border Investigations and Assessments	
Training	Information Services	Counter-Espionage and Interference C	Counter-Terrorism Investigations 2	Intelligence Discovery, Investigations and Assessments	
		Counter-Espionage and Interference D			
		Counter-Espionage and Interference E			

3

AUSTRALIA'S SECURITY ENVIRONMENT AND OUTLOOK

Australia's security environment and outlook

Australia's national terrorism threat level remains at **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 14 major disruption operations of imminent attack planning and six terrorist attacks targeting people in Australia. The primary terrorist threat in Australia comes from a small number of Islamist extremists who are committed to violence as part of their ideology.

- All but one of the attacks and disruptions have been related to Islamist extremism. Of the six successful terror attacks Australia has experienced, three involved the use of knives and three involved firearms.

The most likely form of terrorism in Australia remains an attack by an individual or small group using simple attack methodologies, though the possibility of more complex attacks cannot be ruled out.

- While the threat of terrorist attacks conducted by lone actors continues, these threats are not isolated to Islamist extremists. Individuals motivated by other ideologies—such as an extreme left- or right-wing ideology—may consider conducting an act of terrorism.

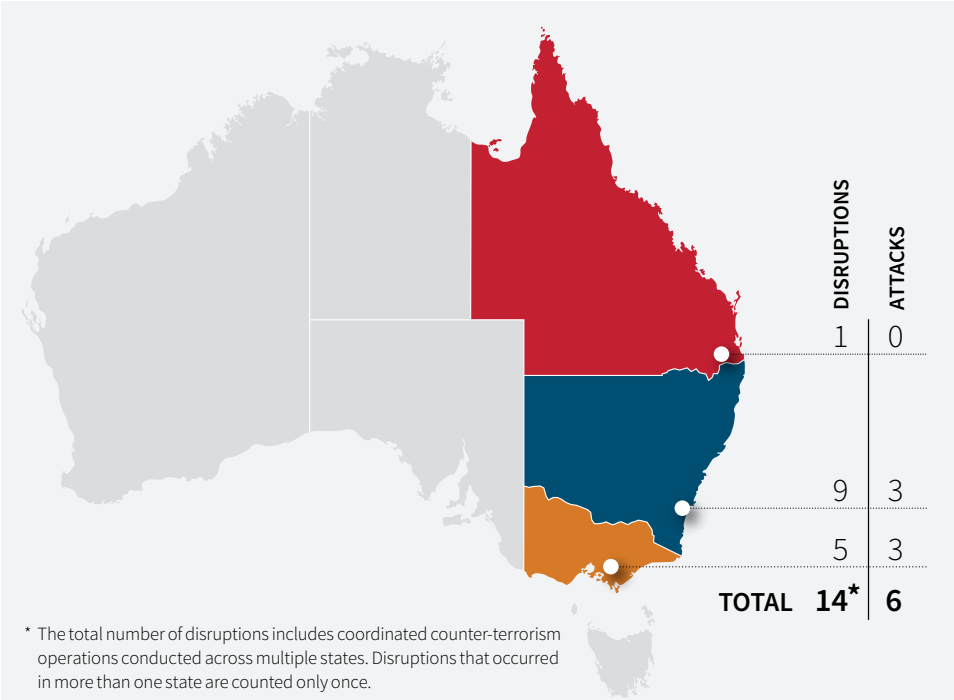
Any terrorist attack in Australia over the next 12 months would probably involve weapons and tactics that are low-cost and relatively simple, including basic weapons, explosives and/or firearms. Basic weapons are readily available, as everyday objects that do not require specialist skills. Globally, terrorists have used basic weapons such as knives or vehicles to conduct lethal attacks, though explosives remain a favoured terrorist weapon.

Terrorist attacks that occurred in the West in 2017 have demonstrated the trend towards targeting people at crowded places such as bridges, stadiums, public transport facilities and restaurant areas—locations that feature a large number of people and relatively low levels of security. Attacks at crowded places can achieve terrorist objectives by causing fear, death and injury, as well as significant international media coverage. The 2017 attacks on the London and Westminster bridges in the United Kingdom showed the use of a mixed-mode attack, with the assailants using a vehicle in the first stage of the attack before continuing the attack with knives.

- A range of online literature, including propaganda, provides weapons and tactics advice on how to conduct and improve the lethality of an attack. This literature includes simple instructions, which do not require specialist skills, on how to use readily available materials to make weapons, such as homemade explosives. Publicity about terrorist incidents is likely to provide further guidance and inspiration to terrorists.

While propaganda is still being produced by Islamist extremist groups overseas, there has been an overall decline in propaganda from groups such as the Islamic State of Iraq and the Levant (ISIL). This propaganda still calls for attacks in Western countries, and we continue to expect that, for years to come, this propaganda will remain accessible and justify the use of violence.

Onshore terrorist attacks and counter-terrorism disruptions since September 2014



* The total number of disruptions includes coordinated counter-terrorism operations conducted across multiple states. Disruptions that occurred in more than one state are counted only once.

2014

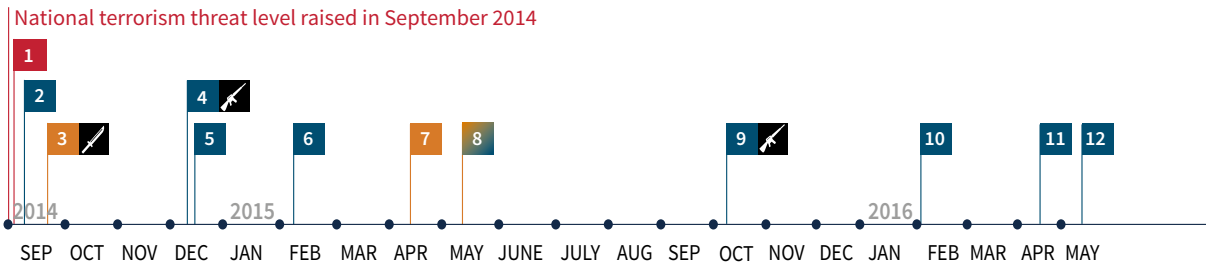
1 **OP BOLTON** *10 SEP* Preparation for an onshore attack disrupted.

2 **OP APPLEBY** *18 SEP* Preparation for an onshore attack disrupted.

3 **OP GOODRICH** *23 SEP* Two police officers attacked. Assailant killed.

4 **OP ARRABELLA** *15 DEC* Martin Place siege. Three killed including assailant.

5 **OP APPLEBY** *18 DEC* Possible plot against government buildings disrupted.



2015

6 **OP CASTRUM** *10 FEB* Possible plot to target members of the public disrupted.

7 **OP RISING** *18 APR* Possible plot against Anzac Day services or police disrupted.

8 **OP AMBERD KASTEEL** *8 MAY* Coordinated raids disrupt possible onshore attack planning.

9 **OP SF FELLOWS** *2 OCT* NSW Police Force civilian employee killed. Assailant killed.

2016

10 **OP CHILLON** *JAN/FEB* Possible plot disrupted.

11 **OP VIANDEN** *24 APR* Possible plot against Anzac Day services disrupted.

12 **OP SANANDRES** *17 MAY* Possible plot disrupted.

13 **OP FORTALEZA** *6 AUG* Alleged preparation for plot by an extreme right-wing individual disrupted.

14 **OP TRESSIDER** *10 SEP* Stabbing attack against a member of the public. Assailant arrested.

15 **OP RESTORMEL** *12 OCT* Possible plot disrupted. Two individuals carrying knives arrested.

16 **OP KASTELHOLM** *22 DEC* Possible plot disrupted. Four individuals charged with acts done in preparation for a terrorist act.

2017

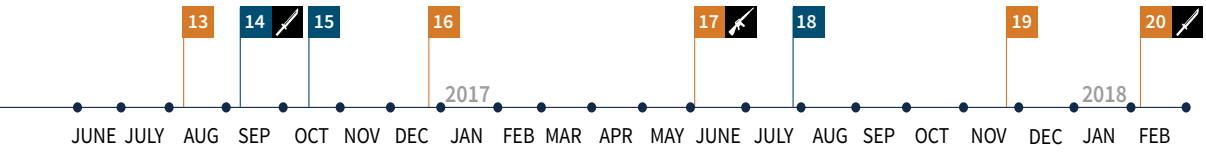
17 **OP TEMATIN** *5 JUN* Member of the public killed and three police officers injured during siege/hostage attack. Assailant killed.

18 **OP SILVES** *29 JUL* Alleged plot against aviation disrupted. Two individuals charged with terrorism offences.

19 **OP SAN JOSE** *27 NOV* Alleged New Year's Eve plot disrupted. One individual charged with terrorism offences.

2018

20 **OP VECCHIO** *9 FEB* Knife attack against a member of the public in their home. Assailant was arrested and charged with a terrorism offence.



Dispersal of foreign fighters

Although significant uncertainty exists about the future shape of ISIL and the foreign fighters who joined it, we expect the legacy of ISIL and the networks it has built, in person or online, will continue to adversely affect both the global and Australian security environments for years to come. These will also endure long past the current manifestation of ISIL in Syria and Iraq.

The collapse of ISIL's caliphate and its loss of territory in Syria and Iraq resulted in the dispersal of many foreign fighters who had travelled to Syria and Iraq to support ISIL. It is likely some ISIL fighters and their families have tried to depart Syria, and thousands have been detained in Syria and Iraq. Others may travel to alternative conflict zones, but this will depend on each individual's contacts, language skills, cultural affinity and associated networks. However, we remain concerned about a significant, but unknown, number of foreign fighters who cannot be accounted for.

Australian returnees

Of the Australians who travelled to fight with or support Islamist extremist groups in Syria or Iraq, we expect a very small number may return to Australia voluntarily or through deportation. Whether these individuals will present an ongoing terrorist threat to Australia depends on their ideology and willingness to engage in violence onshore in support of that ideology. Beyond planning attacks they may also hold a position of greater standing among Australia-based Islamist extremists, which they could use to influence, radicalise and recruit others.

- Those foreign fighters who have remained longer in the conflict zone are likely to have demonstrated more resolve and commitment to the ISIL cause and narrative, endured hardship and poor living conditions, and participated in multiple battles. Many may have developed international connections, been exposed to sophisticated military planning or become part of ISIL's terrorist support networks that move money, people and materials across international borders.
- This cohort is likely to return with increased security awareness, which will limit our understanding of their experiences, their networks—both in Australia and overseas—and, more importantly, of the potential threat they may pose now and in the future.

Communal violence and violent protest

Most Australian protests, while occasionally employing disruptive tactics, comply with regulations and conclude without significant incident. However, hostility between extreme left- and right-wing proponents at protests occasionally results in confrontational behaviour. Protests on other issues—such as government policy and the environment—are mostly peaceful, and counter-protests are rare. Occasionally, disruptive tactics are employed and incidental acts of violence may occur.

Minimal violence was observed at protests between left- and right-wing proponents during 2017–18. This may be due to a number of factors, including the police response at these protests, which effectively kept groups separate.

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.

Terrorism—the international security environment

South-East Asia

ISIL propaganda and calls for attacks continue to shape the security environment in South-East Asia, influencing extremist networks, small groups and lone actors to undertake acts of violence. In May 2018 an Indonesian pro-ISIL network conducted the deadliest terrorism campaign in Indonesia in over a decade, carrying out coordinated suicide-bombing attacks against police and churches in Indonesia's second largest city, Surabaya. In the Philippines, the May–October 2017 ISIL-backed seizure of territory in the southern Philippines city of Marawi was the first time ISIL had held territory outside the Middle East and Africa. Elsewhere in South-East Asia, counter-terrorism operations in Malaysia have disrupted several pro-ISIL attack plots over the course of the 2017–18 reporting period. Under ISIL's influence, disparate groups have coalesced, expanding cooperation and traditional areas of operation. Since the start of the conflict in Syria and Iraq, hundreds of individuals from South-East Asia have travelled to Syria and Iraq to fight with or give support to militant groups, including ISIL. The potential return of individuals with a hardened ideology, technical expertise or combat experience poses an ongoing risk to the South-East Asian security environment, where these individuals, or other foreign fighters travelling to South-East Asia, provide capability to networks in the region.

Middle East

The conflict in Syria and Iraq continues to dominate the Middle East security environment, which remains highly complex. Across the region, numerous threat actors continue to pose a significant security threat and retain the intent and capability to conduct attacks of varying complexity in several countries. ISIL has reverted to insurgency tactics in Syria and Iraq following large-scale territorial losses, and continues to conduct highly lethal attacks, including with explosive devices. The threat from al-Qa'ida has also not diminished—al-Qa'ida-aligned groups in Syria are well placed to benefit from ISIL's losses in the region. While al-Qa'ida's presence in Syria continues to evolve, and al-Qa'ida-aligned groups in Syria appear focused on local issues, they collectively represent an enduring threat to Australian interests.

Outside Syria and Iraq, ISIL-affiliated or -aligned groups and individuals have attacked a range of targets, aiming to exacerbate political and sectarian divisions. Despite a reduction in successful terrorist attacks, Turkey remains a high-threat environment. While authorities have disrupted several plots, both ISIL and Kurdish groups retain the intent and capability to conduct attacks, including in metropolitan centres. Yemen's security environment remains highly unstable and complex—factors which both al-Qa'ida in the Arabian Peninsula and ISIL-Yemen continue to exploit.

Europe

Islamist extremists continue to view Europe as a legitimate target for terrorist attack, and a number of attacks occurred there in 2017–18, including in France, Belgium, the United Kingdom, Russia and Spain. There were also a number of disruptions across Europe, including the disruption of a biological attack plot in Germany. Individuals and small groups inspired by Islamist extremist propaganda, or encouraged by groups such as ISIL, will continue to plan and conduct attacks in Europe. These attacks will most likely use basic weapons (such as knives and vehicles), firearms and explosives, and are likely to continue to target crowded places and police and military targets.

South Asia

The security environment in South Asia continues to decline. Afghanistan faces an enduring threat from the Taliban and Haqqani Network. Islamic State—Khorasan Province remains aggressive and has been reinforced by Central Asian ISIL fighters fleeing Iraq and Syria. Insurgent groups will continue to plan attacks against the semi-secure zone in Kabul, where the Australian Embassy and other embassies are located. Notwithstanding Pakistan's continuing offensive against insurgent forces, extremist groups in Pakistan will continue to conduct attacks against government targets and religious and ethnic minorities.

India continues to face threats from domestic militants including Hindu extremists, Sikh separatists and north-east separatists, as well as India-based Islamist extremists inspired by al-Qa'ida and ISIL. External threats from al-Qa'ida, ISIL and Lashkar-e-Tayyiba are ongoing.

ISIL and al-Qa'ida in the Indian Subcontinent continue to influence groups in Bangladesh, and maintain the intent and capability to conduct attacks against both domestic and foreign targets there.

Africa

In Africa, al-Qa'ida- and ISIL-aligned groups pose a significant and ongoing security threat. Al-Qa'ida affiliates in Africa continue to expand their areas of operation while ISIL-aligned groups pursue their own agendas and activities. Their terrorist campaigns seek to destabilise regional governments and undermine multinational efforts to improve the security environment, and they maintain their intent and capability to attack Western interests. Despite ongoing international and regional counter-terrorism operations, global jihadist ideology continues to resonate in the region and has resulted in the emergence of new areas of extremist activity, particularly in East Africa.

Espionage and foreign interference

Australia continues to be a target of espionage and foreign interference. Australia's position as a major commodity supplier, scientific and technological innovator, and potential joint venture partner makes it a target of foreign states seeking to gain an advantage. Australia's military modernisation program (including niche research and development capabilities) is also of interest to a wide range of foreign intelligence services seeking to obtain or compromise sensitive technologies.

We have identified foreign powers clandestinely seeking to shape the opinions of members of the Australian public, media organisations and government officials to advance their country's own political objectives. Ethnic and religious communities in Australia have also been the subject of interference operations designed to diminish their criticism of foreign governments. A range of countries target Australia, some of which we have strong and enduring relationships with, which doesn't appear to curtail their willingness to target Australia.

We are focused on activities that accord with the *Australian Security Intelligence Organisation Act 1979* definition of 'acts of foreign interference'—that is, activities related to Australia conducted by or on behalf of a foreign power that are clandestine, deceptive and/or threatening, or otherwise detrimental to Australia's national interests, in Australia and internationally. These activities—undertaken covertly—represent a threat to our sovereignty, the integrity of our national institutions and the exercise of our residents' rights.

We fully support the need to ensure Australia remains attractive to foreign investment by balancing national security against trade imperatives. However, the threat to critical infrastructure is changing and remains an ongoing challenge. While foreign investment can provide a measure of access and control over organisations and assets in Australia which may not otherwise be attainable, the threat is no longer only about access to critical infrastructure and associated data. For example, foreign intelligence services could use the ownership and the access provided through foreign investment to influence key decision-makers in the Australian Government and/or manipulate suppliers and customers during business decisions.

We regularly observe cyber espionage activity targeting Australia. Foreign state-sponsored adversaries target the networks of the Australian Government, industry and individuals to gain access to information and progress other intelligence objectives.

- The number of countries pursuing cyber espionage programs is expected to increase, as these programs can offer significant intelligence returns with relatively low cost and plausible deniability.

As technology evolves, the sophistication and complexity of cyber actors and their targeting methods will increase. Our understanding of the cyber threat has also evolved. The blurring of traditional lines between the cyber activities of state and non-state actors means that attributing the source of cyber intrusions can be a difficult and lengthy process. It is therefore vital that we continue to develop our capabilities to ensure we can assist government to respond quickly and proportionally to any cyber intrusions.

The transition from influence to interference

The who

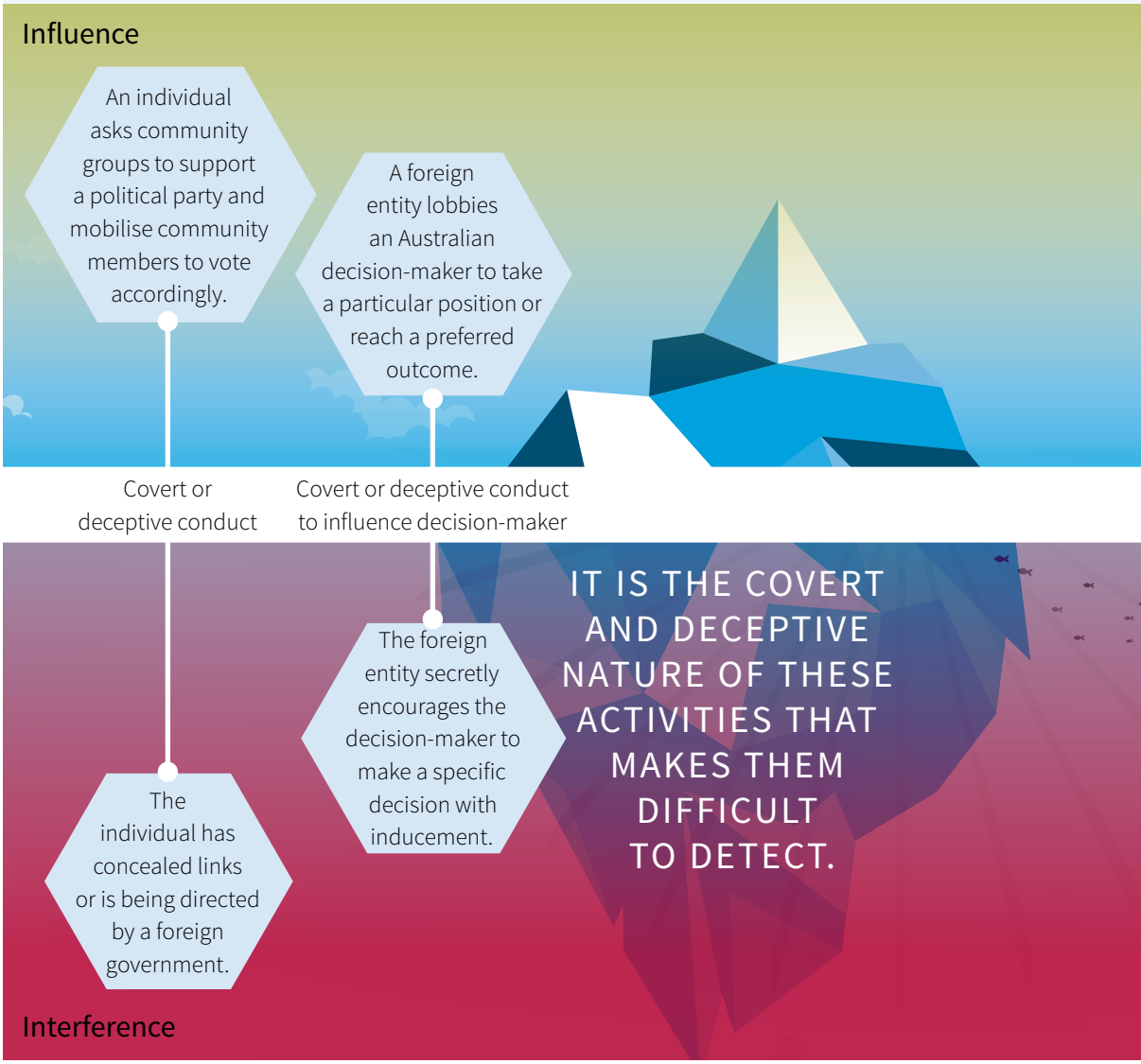
A person who acts:

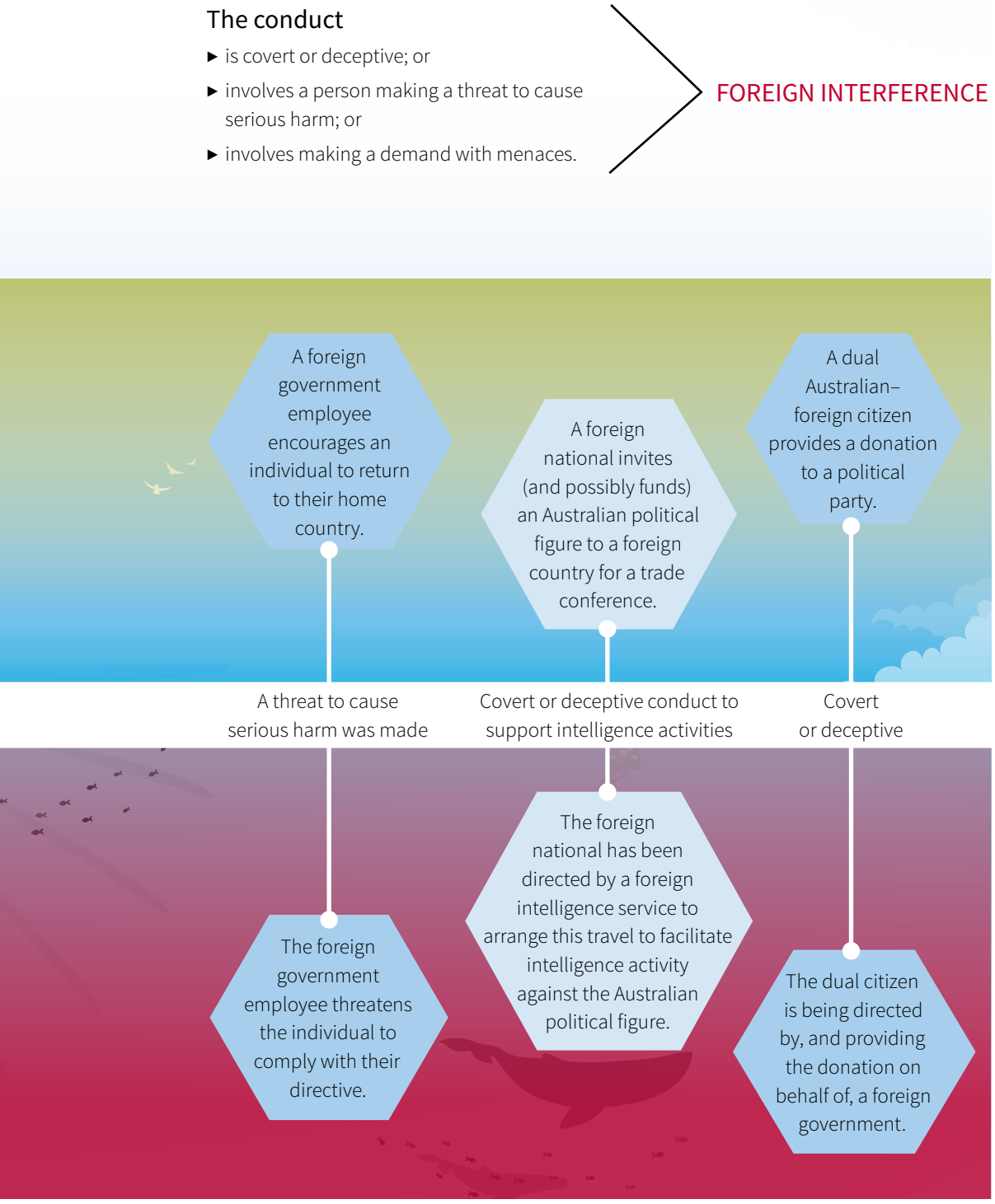
- on behalf of, or in collaboration with, a foreign principal; or
- is directed, funded or supervised by a foreign principal; and

The purpose

The purpose is to:

- influence the exercise of an Australian democratic right or duty; or
- support the intelligence activities of a foreign principal; or
- prejudice Australia's national security; and




The conduct
► is covert or deceptive; or
► involves a person making a threat to cause serious harm; or
► involves making a demand with menaces.
FOREIGN INTERFERENCE
A foreign government employee encourages an individual to return to their home country.
A foreign national invites (and possibly funds) an Australian political figure to a foreign country for a trade conference.
A dual Australian–foreign citizen provides a donation to a political party.
A threat to cause serious harm was made
Covert or deceptive conduct to support intelligence activities
Covert or deceptive
The foreign government employee threatens the individual to comply with their directive.
The foreign national has been directed by a foreign intelligence service to arrange this travel to facilitate intelligence activity against the Australian political figure.
The dual citizen is being directed by, and providing the donation on behalf of, a foreign government.

Espionage and foreign interference are insidious threats—activities that may appear relatively harmless today can have significant future consequences. The harm may not manifest until many years, even decades, after the activity has occurred. Hostile intelligence activity can undermine Australia's national security and sovereignty; damage Australia's reputation and relationships; degrade Australia's diplomatic and trade relations; inflict substantial economic damage; degrade or compromise nationally vital assets, defence capabilities and critical infrastructure; and threaten the safety of Australian nationals or others who serve Australian interests. Aggregate cost is difficult to quantify, particularly in dollar terms, but the harm poses a real and potentially existential threat to Australian security and sovereignty.

While there are now more vectors than ever through which espionage and foreign interference can be carried out, the passage of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill and Foreign Influence Transparency Scheme Bill will provide valuable new tools to help combat this threat, offer a significant public deterrent, and make it more difficult for our adversaries to do business here. In our view, the new espionage and foreign influence offences and foreign influence transparency scheme regime will impose appropriate restrictions on foreign and Australian entities seeking to act contrary to Australia's sovereignty, security and prosperity, while including important protections for our democratic rights and institutions.

4

REPORT ON PERFORMANCE

ASIO annual performance statement 2017–18

Introductory statement

I, as Director-General of Security and the accountable authority of ASIO, present the 2017–18 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.

Duncan Lewis
Director-General of Security

25 September 2018

ASIO's purpose

ASIO's purpose is to protect Australia, 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 industry. In 2017–18 we pursued this purpose through four key activities:

- **Key activity 1:** counter terrorism;
- **Key activity 2:** counter espionage, foreign interference and malicious insiders;
- **Key activity 3:** counter serious threats to Australia's border integrity; and
- **Key activity 4:** provide protective security advice to government and industry.

Results for 2017–18

ASIO's corporate plan 2017–18 outlines measures we use to assess our performance in achieving our purpose. The following statements describe our results against the performance measures for each key activity.

In developing these statements we have drawn on internal performance reporting and an independent survey of 74 of our senior government and industry stakeholders conducted between April and June 2018.

The results address the performance criterion contained in ASIO's Portfolio Budget Statement (PBS): effective advice, reporting and services that assist the Australian Government and ASIO's partners to manage security risks and disrupt activities that threaten Australia's security.

Key activity 1: counter terrorism

Performance measure

ACHIEVED

Our advice influences the Australian Government's policy development and responses to terrorism

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Support for Australian Government counter-terrorism policies and strategies

In 2017–18 we provided relevant and timely advice that informed Australian Government policies and strategies in response to terrorism. This included contributions to the development of:

- responses to the July 2017 disruption of a plot to use an improvised explosive device against an Etihad flight departing Sydney and a potential plot to use toxic gas in a terrorist attack (Operation Silves);
- policy advice on returning foreign fighters;
- Australia's strategy for protecting crowded places from terrorism; and
- strategies to counter violent extremism.

We contributed to the development of legislative responses to terrorism, including by providing assessments leading to the proscription of Islamic State—East Asia, Jemaah Anshorut Daulah (JAD), and Jama'at Mujahideen Bangladesh (JMB) as well as the relisting of multiple terrorist organisations under the Criminal Code. Our advice supported the relisting of Mosul as a declared area and the revocation of al-Raqqa's designation as a declared area.

Our counter-terrorism assessments provided the basis for the Minister for Foreign Affairs to temporarily suspend, cancel or refuse passports for extremists who would otherwise have travelled to the conflict zone in Syria and Iraq.

We also continued to provide the Department of Foreign Affairs and Trade with timely National Threat Assessment Centre (NTAC) assessments of the evolving terrorist threat environment, which resulted in a significant number of updates to the Australian Government's Smartraveller travel advice during the reporting period.

Outreach and assessments to strengthen policymakers' understanding of terrorism threats

Our advice and assessments informed policymakers' understanding of local and international terrorist threats. We produced 1154 intelligence and security reports and provided a significant number of briefings to stakeholders on a range of terrorism-related topics, including threats to aviation and mass passenger transportation, and pathways to radicalisation. The NTAC also provided 31 briefing sessions for federal and state government agencies on terrorism indicators, and extended these briefings to a range of foreign security and intelligence partners.

Stakeholder evaluation

Stakeholders in our annual stakeholder survey said our advice informing counter-terrorism policy and responses was well considered, balanced, practical and of high quality. Our advice to federal and state governments, law enforcement agencies and the aviation sector after the July 2017 Operation Silves disruption was acknowledged as having played a pivotal role in shaping policy responses, including on aviation, air cargo and international mail security.

Our assessments and NTAC threat reporting were also seen by policy and security agencies as being influential in informing both policy development and responses to terrorism. Our analysis of terrorism motivations, influences and trends in Australia was highly regarded, as were our biannual threat assessments of terrorism and violent protest and reports on right- and left-wing extremism. Stakeholders particularly mentioned the value of our international liaison arrangements and our capacity to draw on our partners' threat warnings and assessments.

Key activity 1: counter terrorism

Performance measure

ACHIEVED

National security partner agencies use our advice to disrupt and defend against terrorism

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Counter-terrorism disruptions

We continued to work closely with law enforcement and security agencies to protect Australians and Australia's interests from terrorism.

In 2017–18 we resolved or investigated 14 227 incoming leads. A number of these we referred within ASIO for further investigation, and some resulted in a joint investigation with law enforcement partners. Advice that we provided to federal and state law enforcement agencies contributed directly to the disruption of two planned terrorist attacks, including a major disruption in July 2017 of a terrorist attack plan against Australian aviation (Operation Silves). We also worked with international partners to support their disruption of terrorism-related threats, including by sharing advice and threat assessments informed by Operation Silves investigations.

ASIO intelligence contributed to the prosecution of individuals in New South Wales, Victoria, South Australia and Queensland on terrorism offences. Our support included the initial identification of activities of concern, the provision of unique insights and assessments, and the use of intelligence as evidence. Working with our law enforcement partners and prosecuting authorities, our evidentiary contribution included telecommunications intercepts, physical surveillance, and listening and tracking devices. Sensitive capabilities were protected from disclosure through legal mechanisms such as public immunity claims and suppression orders.

We supported security arrangements for special events, including the Gold Coast 2018 Commonwealth Games (GC18), through the provision of security planning and accreditation-related advice to partners (see also performance measure 3b).

We continued to play a leading role within the National Intelligence Community in intelligence prioritisation and evaluation. This included the:

- production of broad national-level counter-terrorism intelligence priorities;
- development of information requirements and priorities in relation to terrorism in South-East Asia;

- provision of advice to law enforcement agencies on high-priority terrorism investigation targets; and
- management of a collaborative counter-terrorism intelligence evaluation process.

In addition to providing counter-terrorism advice, we coordinated intelligence advice to support the Australian Government's responses to the kidnapping of Australians overseas.

Stakeholder evaluation

Stakeholders in federal and state governments and law enforcement regarded our counter-terrorism advice as timely, of high quality and very influential in informing their efforts to disrupt and defend against terrorism. Many pointed to Operation Silves as a demonstration of our effective collaboration with partners and provision of actionable operational intelligence. The federal and state Joint Counter Terrorism Teams (JCTT) valued our partnership highly and saw ASIO as an engaged and innovative partner continuously striving for improvements.

Stakeholders said we had worked effectively with security and law enforcement agencies to ensure the success of protective security aspects of GC18, and viewed the GC18 effort as being characterised by close cooperation and unprecedented information-sharing. Security and law enforcement partners also cited our contribution to pre-GC18 training and exercises as being highly valuable.

Government and industry stakeholders said our reporting and assessments disseminated by the Business and Government Liaison Unit (BGLU) and sectoral briefing days were valuable, influential and essential in informing the measures they implement to defend against terrorism.

Case study: proscribing Islamic State—East Asia

In December 2015, Islamic State—East Asia (IS-EA) publicly pledged its *bay'ah* (allegiance) to proscribed terrorist organisation the Islamic State of Iraq and the Levant, and in May 2017 it conducted a large-scale attack and held parts of Marawi City, Philippines, for five months. IS-EA's primary objective is to establish an Islamic state under sharia law in the Philippines. To achieve its objectives, IS-EA continues to conduct terrorist attacks against military and civilian targets in the Philippines. While Australia has not been explicitly named as a target, attacks by IS-EA may include Australian interests in the Philippines. IS-EA's attacks and propaganda could inspire or attract Australians to conduct activities of security concern.

Proscribing IS-EA as a terrorist organisation signals publicly that the Australian Government considers the group a terrorist organisation, and that Australians supporting IS-EA may be subject to criminal charges. One of our functions is to provide threat advice to inform government responses. Accordingly, the proscription of IS-EA was based on advice from ASIO, in consultation with other Australian Government departments including the Attorney-General's Department and the Department of Foreign Affairs and Trade.

On 8 September 2017, IS-EA was listed as a proscribed terrorist organisation under the *Criminal Code Act 1995*. The proscription of IS-EA criminalises a range of activities that provide support to the group, and enables the prosecution of Australians undertaking activities on behalf, or in support, of the organisation. Under division 102 of the Criminal Code, it is an offence to do things such as direct the activities of, be a member of, recruit for, provide training to, receive training from or participate in training with, provide funds to or receive funds from, or provide support to a terrorist organisation. It is also an offence to associate with a member of a listed terrorist organisation in certain circumstances where such an association intentionally provides support to that organisation.

Proscription assists with whole-of-government responses to Islamist extremist groups in South-East Asia, including the travel of foreign fighters to the region, encompassing those who are leaving Iraq and Syria.

Case study: counter-terrorism Operation Silves

Politically motivated violence remains a threat to Australia. Since September 2014 there have been 14 major disruption operations against imminent attack planning and six terrorist attacks targeting people in Australia. The primary terrorist threat in Australia comes from a small number of Islamist extremists who are committed to violence as part of their ideology. Although significant uncertainty exists about the future shape of the Islamic State of Iraq and the Levant (ISIL) and the future of the foreign fighters who joined it, we expect the legacy of ISIL and the networks they have built, in person or online, will continue to adversely affect both the global and Australian security environment for years to come.

On 26 July 2017, ASIO received lead information on a possible threat to Australian aviation. We assessed the information to be both serious and credible and commenced a security intelligence investigation. In response to the threat, we provided the lead intelligence to law enforcement partners, as well as results of an initial ASIO investigation that identified a key individual involved in the plot. This information enabled the commencement of a criminal investigation (Operation Silves) that paralleled the continued intelligence investigation. We continued to provide unique intelligence and investigative insights to law enforcement agencies in the lead-up to, and following, police activity to disrupt the plot.

Additionally, our security intelligence investigations informed advice produced by ASIO's National Threat Assessment Centre (NTAC). The NTAC produced threat assessments to provide threat advice to senior Australian Government and state and territory stakeholders as the investigation developed, and communicated the assessments through appropriate distribution channels and systems. These threat assessments aimed to address the needs of the policy and regulatory community and to help inform the responses of national security partners—including regulators, policymakers and industry, such as airport operators.

In response to our advice to regulatory bodies, stakeholders increased protective security measures including enhanced airport check-in and screening procedures for passengers, baggage and cargo. Operation Silves resulted in law enforcement–led disruption of Australia-based individuals inspired and directed by ISIL to attack aviation, and potentially other forms of mass transit in Australia, by both improvised explosive device and chemical dispersal weapon. On 29 July 2017, law enforcement action resulted in the arrest and subsequent charging of individuals for a range of offences, including acts in preparation for, or planning of, a terrorist act (section 101.6, *Criminal Code Act 1995*). Our assessment and advice played a pivotal role in shaping policy responses, including on aviation, air cargo and international mail security.

Key activity 2: counter espionage, foreign interference and malicious insiders

Performance measure

ACHIEVED

Our advice influences the Australian Government's policy development and responses to espionage, foreign interference and malicious insiders

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Support for Australian Government counter-espionage and foreign interference policies and strategies

In 2017–18 we provided the Australian Government and its policy agencies with extensive operational briefings, advice and assessments on the espionage and foreign interference threat to Australia. We published 286 intelligence and security products on counter-espionage and foreign interference to inform policymakers' decisions. Key analytical products released during this period include assessments of the harm from espionage and a strategic overview of foreign interference.

A focus for us during this reporting period was supporting the development of a suite of policy and legislative measures to counter the espionage and foreign interference threat to Australia. We provided advice and assessments that:

- highlighted potential weaknesses in the Criminal Code which were limiting law enforcement agencies' ability to charge and prosecute espionage and foreign interference–related activities under the current code;
- assisted the Attorney-General's Department to develop proposed legislation to respond to the threat; and
- informed the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the proposed legislative amendments.

We also provided advice to support the Department of Home Affairs' (Home Affairs) response to the foreign interference threat, including the establishment of the National Counter Foreign Interference Coordinator (NCFIC). We continue to provide advice, assessments, practical support and staff to support the NCFIC's work.

In June 2018 the Australian Parliament passed the National Security Legislation Amendment (Espionage and Foreign Interference) and Foreign Influence Transparency Scheme Bills. This was a significant development that criminalised acts of foreign interference for the first time in Australia.

During this reporting period, our advice also supported the Australian Government's response to the poisoning of former Russian military intelligence officer Sergei Skripal and his daughter Yulia Skripal, and the associated decision to expel two undeclared Russian intelligence officers from Australia.

Support for Australian Government foreign investment and critical infrastructure protection policies

Our foreign investment assessment advice to the Foreign Investment Review Board (FIRB) and government agencies such as the Treasury continued to raise Australian Government awareness of security risks associated with specific foreign investment proposals, as well as awareness of other issues of wider policy concern such as foreign powers' use of investment as a vector for espionage, foreign interference or sabotage; aggregated risks across investment sectors; and data centre protection.

- During 2017–18 we completed 245 foreign investment assessments, which provided advice on the potential for a foreign power to conduct espionage, foreign interference or sabotage through its involvement in specific investments.
- Our advice on the lack of ownership diversity within certain infrastructure sectors supported the Australian Government's announcement in February 2018 that ownership diversity should be considered a key requirement for future sales, and the introduction of new foreign investment conditions for the electricity sector.
- We identified security concerns about the implementation of the Business Exemption Certificate regime, in particular that applications did not include adequate details on the asset or company to be purchased and/or the location of the investment. We worked with Treasury to ensure that national security concerns would be appropriately addressed under the exemption certification process.
- We also provided advice to the Australian Government on the national security implications of amendments to the Credit Reporting Scheme, highlighting discrepancies between the credit reporting bureaus and the banking sector in their regulation, oversight and security practices. Our advice contributed to legislative changes to require higher levels of data security assurance under the scheme.

Stakeholder evaluation

Stakeholders said that our advice informing policy development and responses to espionage, foreign interference and malicious insiders was trusted and respected. They noted, in particular, that our advice had been influential in informing the Australian Government's response to the Skripal poisoning.

Stakeholders also commented favourably on our reports and assessments, noting the increasing quality and range of reports. FIRB representatives noted the high quality and continuing improvement of our advice and briefings on the foreign investment threat.

Key activity 2: counter espionage, foreign interference and malicious insiders

Performance measure

SUBSTANTIALLY ACHIEVED[2]

National security partner agencies use our advice to disrupt and defend against harmful espionage, foreign interference and malicious insiders

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Defence industry security assurance

A major focus for us continued to be working in partnership with the Department of Defence to implement the recommendations of the Australian Defence Industry Security Assurance Review. During this reporting period, we:

- augmented our counter-espionage and countering foreign interference resourcing and, jointly with Defence, began implementing a program to increase security assurance for the significant government investment in defence capability;
- provided high-level advice in support of Defence security policy and acquisition programs; provided intelligence on potential threats; and engaged regularly with the Department of Defence and the Australian Defence Force on high-priority capability projects, including the Future Submarines, Off-Shore Patrol Vessels and F-35 projects; and
- together with the Department of Defence and the Royal Australian Navy, engaged with French services to plan and prioritise security responses to the building of Future Submarines and to share threat reporting.

We continue to develop analytic and investigative effort focused on threats to defence industry and acquisition programs to prevent harm and maintain Australia's military advantage.

Raising awareness of the espionage, foreign interference and malicious insider threat

We continued our program of briefings and outreach to improve understanding, among federal and state governments and industry, of techniques employed by foreign intelligence services, manifestations of espionage and foreign interference, and the associated risks of this interference, to protect our national institutions of government from foreign influence.

[2] See 'Analysis of performance' for discussion of this result.

We provided 28 foreign intelligence service threat briefings for federal and state parliamentarians, ministerial staff and high-office holders travelling overseas, which included advice on mitigation strategies to minimise possible threats. Our outreach team provided frequent security briefings (5–10 per week) to raise government agencies' awareness of espionage, foreign interference and malicious insider threats. These briefings also offered the opportunity to reiterate security clearance holder obligations, including responsibilities under the Contact Reporting Scheme (CRS). The CRS continued to be a valuable tool in defending against harm from espionage, foreign interference and malicious insiders. Approximately 15 per cent of CRS reports produced security intelligence leads that would not otherwise have been identified.

Preserving the integrity of government business: personnel security assessments

ASIO provides security assessments to Australian Government agencies on an individual's suitability for access to national security–classified information and/or areas. This process is critical to protecting the national interest from espionage and foreign interference. We also contribute to whole-of-government development and reform of personnel security policy.

In 2017–18 we completed 32 153 personnel security assessments—an increase of more than 18 per cent from the previous financial year. We continued responding to requests for Negative Vetting 1 and 2 personnel security clearances in line with agreed time frames with the Australian Government Security Vetting Agency (AGSVA). However, we did not meet agreed time frames for Top Secret Positive Vetting (TS(PV)) clearances, as a result of the continuing significant growth in assessment demand for PV clearances. We received more than 3000 requests for PV clearances during 2017–18—an increase of 43 per cent from the previous financial year.

We continue to work closely with AGSVA to improve the efficiency of the security assessment process while maintaining an appropriate level of assurance for vetting candidates. The Independent Intelligence Review of June 2017 identified significant delays in processing times for TS(PV) security clearances. The review noted that, although it is vital to shorten vetting time frames, the clearance process must also remain robust. In line with the review recommendations, ASIO has seconded staff to AGSVA to build on existing cooperation between our two agencies and to better integrate ASIO's security expertise in the vetting work stream.

Stakeholder evaluation

Stakeholders said the quality of our briefings for politicians, senior office holders and officials was of a very high standard. Our tailored briefings on foreign states of concern and the management of electronic devices during travel were particularly sought after and highly regarded by those about to travel. While acknowledging that our personnel security assessments are only one part of the vetting process, many stakeholders reiterated their concerns about the time taken to issue them.

Key activity 2: counter espionage, foreign interference and malicious insiders

Performance measure

PARTIALLY ACHIEVED[3]

We collect foreign intelligence in Australia that advances Australia's national security interests

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Under the *ASIO Act 1979*, we are responsible for collecting foreign intelligence in Australia on matters relating to Australia's national security, foreign relations or economic wellbeing. The specific details of outcomes achieved in this area are classified.

ASIO always operates in a resource-constrained environment, and we manage priorities within that constraint. During this reporting period we provided limited support to partners. Where we did plan and execute foreign intelligence collection operations with partners, our foreign intelligence partners said we were effective. Joint operations were considered to have been successful and to have provided valuable, and in some cases unique, foreign intelligence.

4

Case study: Skripal expulsions

In March 2018, former Russian military intelligence (GRU) officer Sergei Skripal, his daughter Yulia Skripal, and a responding police officer became critically ill as a result of exposure to a military-grade nerve agent on British soil. United Kingdom authorities assessed it was highly likely that the Russian Federation was responsible for this attack. A hostile act like this, carried out on the soil of a close ally, carries implications for Australian interests.

As part of our role to advise the Australian Government on policy development and responses to espionage, foreign interference and malicious insiders, we provided advice to the government on Russian intelligence activity in Australia. The Australian Government took a decision consistent with many international partners, and as part of a global response to the Russian state's offensive use of a chemical weapon, to remove the diplomatic accreditation of two Russians based at the Embassy of the Russian Federation in Canberra.

Our advice on matters of espionage, foreign interference and malicious insiders is critical to the government's ability to protect Australia, Australians and Australian interests, including on matters affecting close allies and partners.

[3] See 'Analysis of performance' for discussion of this result.

Case study: qualified NV1 security assessment

On 2 March 2018, we furnished a qualified security assessment to an Australian Government department on their sponsorship of an application for a Negative Vetting 1 (NV1) security clearance for an Australian citizen working overseas as a locally engaged staff member for the department.

Our assessment found the staff member was at serious threat of attempts by foreign intelligence services in his country of residence to exploit his access to information that would enable espionage, acts of foreign interference or other actions contrary to security requirements. This was due to the nature of the staff member's access to privileged information; the likelihood that the relevant foreign intelligence services would be aware of his access; and his vulnerability to attempts to exploit his access due to his significant ongoing links to the country, including having a foreign spouse and family resident in-country, and his reliance on the foreign government for visa-related issues.

We did not recommend against the staff member being granted an NV1 security clearance but recommended a personal security strategy that would allow the individual and the department to better understand and manage the risk of exploitation by foreign intelligence services. The personal security strategy required the department to provide additional protective security briefings and a designated point of contact for the staff member to discuss any personal security issues on a more frequent basis.

Key activity 3: counter serious threats to Australia's border integrity

Performance measure

ACHIEVED

Our advice influences the Australian Government's policy development and responses to serious threats to Australia's border integrity

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Our advice and assessments for Operation Silves, and its implications for Australia's aviation and border security arrangements, directly informed the Australian Government's protective security responses to the disrupted plot. The Office of Transport Security, now the Aviation and Maritime Security Division within Home Affairs, drew on our assessments to help implement heightened security measures across the Australian aviation sector.

4 Stakeholder evaluation

Home Affairs said our contribution to border security policy development during the year—as well as our security assessments and intelligence assessments on people-smuggling and our advice on emerging potential threats—had been influential. They said our extensive reporting and assessments on aviation security threats, in particular, had made an important contribution to their development of new measures to further strengthen security at Australia's ports of entry. Our ability to draw on our extensive range of international liaison partners, who often provide unique perspectives on border security issues, was also considered valuable.

Key activity 3: counter serious threats to Australia's border integrity

Performance measure

ACHIEVED

National security partner agencies use our advice to disrupt and defend against serious threats to Australia's border integrity

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Supporting visa, citizenship and security access decision-making

We continued to produce security assessments to assist Home Affairs and other agencies to manage security risks relating to visas and citizenship applications; access to security controlled places, such as sensitive air or maritime port areas; special events accreditation; and access to security-sensitive chemicals, biological agents and nuclear sites.

In 2017–18 we completed 5454[4] visa security assessments. We met all service-level agreements with Home Affairs on visa security assessments.

Table 1: Visa security assessments, 2017–18

Type of entry	2017–18
Temporary visas	1746
Permanent residence and citizenship	294
Onshore protection (air)	66
Offshore refugee/humanitarian	919
Illegal maritime arrivals	95
Other referred caseloads	2334
TOTAL	**5454***

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

We also completed 144 629 access security assessments for border security, most of which involved providing advice to AusCheck within the Attorney-General's Department on applications for Aviation Security Identity Cards or Maritime Security Identity Cards; and completed a further 9963 access assessments on security-sensitive chemicals, biological agents or nuclear sites.

[4] In 2016–17 we finalised 14 358 visa security assessments. The decrease in the number of finalisations this financial year is due to changes to the security assessment referral criteria, which resulted in a decrease in Home Affairs referrals to ASIO for assessment.

Providing accreditation-related advice to partners in support of security arrangements for major events was a significant focus during this reporting period. We completed 71 254 events accreditation assessments in support of the Association of Southeast Asian Nations (ASEAN) and Australia Special Summit and the 2018 Commonwealth Games (GC18).

Other support for Home Affairs

Alongside our security assessment work, we continued to collaborate with Home Affairs and other national security partner agencies on Operation Sovereign Borders' disruption-related work and, where appropriate, provided intelligence to assist in the multi-agency taskforce's efforts to disrupt people-smuggling ventures.

We provided advice on security indicators to help Home Affairs identify foreign fighters returning from Syria and Iraq. We also worked with Home Affairs on process improvements and proposed system changes, to ensure that visa decision-making is underpinned by the best available information. This included providing training to Home Affairs visa processing officers.

Stakeholder evaluation

Stakeholders said our work had directly contributed to disrupting serious threats to Australia's border security. Home Affairs said our work in identifying and assessing border security–related threats was highly regarded, noting in particular the valuable contribution our foreign fighter profiles had made to border security arrangements as well as our effective collaboration with the department on adverse and qualified visa security assessments. Stakeholders also said that our contribution to planning and implementing GC18, including our support for accreditation, had been valuable and effective.

Case study: border security

Australia remains an attractive target for terrorist groups, and Australia's border integrity and security form a critical part of Australia's defences against the terrorist threat. The collapse of ISIL's caliphate has created an increased movement of potential terrorists across the globe.

In 2017–18, ASIO continued to mitigate these threats to Australia's security by ensuring individuals posing a security risk were denied entry to Australia. An example occurred in early 2018, when for a second time ASIO took action against an offshore foreign national. In 2016–17, ASIO investigated the foreign national, who at that time held an Australian visa. ASIO assessed the individual displayed support for a violent, extremist ideology and potentially planned to travel on to Syria to engage in politically motivated violence. ASIO assessed the individual presented an avoidable risk to Australia's security, and issued an adverse security assessment in early 2017 resulting in the cancellation of the visa. In 2018 this individual sought further travel to Australia, which was refused on the basis of a further ASIO security assessment.

This individual's travel was prevented on two occasions, thereby enabling ASIO to help keep Australia safe and to assist the global effort in identifying individuals with an intent to commit politically motivated violence.

Key activity 4: provide protective security advice to government and industry

Performance measure

ACHIEVED

Our protective security advice and services assist national security partner agencies to manage security risks

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

Performance measure

ACHIEVED

Our engagement with at-risk industry sectors assists them to manage national security risks effectively

Source: *ASIO Corporate Plan 2017–18*; addresses ASIO PBS 2017–18

In 2017–18 we provided protective security advice and services to federal, state and territory governments and industry to enhance their understanding and responses to security threats.

Our Business and Government Liaison Unit (BGLU) continued to facilitate contact between ASIO and our government and industry stakeholders.

- In 2017–18, BGLU facilitated 10 industry briefings, including three interstate briefings to increase our visibility to stakeholders in more states and territories. The diverse topics covered included defence industry, the energy and resources sector, and the terrorist threat to crowded places. Feedback surveys were conducted after eight of the 10 briefing days, and 92 per cent of survey respondents said the briefing sessions met their expectations.
- The BGLU secure website also continued to provide a valued repository of information for industry and government stakeholders. In 2017–18 the website hosted 55 ASIO reports, and subscribers grew by nearly 60 per cent—from 2046 to 3262—during this reporting period.

During this reporting period, we began an academic outreach program. We established engagement with 18 universities, three key university committees, and several other research institutes and university internet connectivity suppliers. Our briefings provided advice on threats to university students, staff, intellectual property, IT networks and reputations; and supported university efforts to protect and commercialise innovative research.

We also contributed briefings to the Centre for Defence Industry Capability roadshow for small and medium enterprises engaged in defence supply chain programs, and engaged with defence industry 'primes' such as BAE, Northrop Grumman, and Thales.

Physical protective security advice and services

Throughout 2017–18, ASIO's T4 Protective Security Directorate (ASIO-T4) continued to provide expert protective security advice and services to the Australian Government and other entities, including state and territory governments, commercial companies, and owners and operators of critical infrastructure.

Table 2: ASIO-T4 advice and services, 2017–18

Advice	Performance 2017–18
Physical security certification program	**Zone 5 facilities** ▸ 89 site inspections and reports completed ▸ 60 certifications issued **Lead agency gateway facilities** ▸ 1 site inspection and report completed ▸ 3 certifications issued **Courier services** ▸ 1 site inspection and report completed ▸ 0 endorsements issued
Security services and equipment evaluation	▸ 71 security products evaluated
Protective security review reports	▸ 1 protective security risk review completed
Communications	**Publications** ▸ 6 protective security circulars posted on Govdex, for government ▸ 10 security managers guides posted on the BGLU website, for industry and government ▸ 4 security equipment guides posted on Govdex, for government **Training** ▸ 4 protective security training courses delivered ▸ 2 safe maintenance courses delivered ▸ 1 Security Construction and Equipment Committee (SCEC)–approved locksmith briefing delivered **Other** ▸ ASIO-T4 developed and delivered the 'Introduction to counter-terrorism protective security' training course for government security practitioners.

Alongside these services, ASIO-T4 continued a capacity-building program to help stakeholders self-manage security risks.

- In 2017–18, ASIO-T4 produced practical guidance material to support industry and government, including those considered 'at risk'. These documents distilled ASIO-T4 expertise into practical 'how to' guidance material which security practitioners can apply to their own facilities. The publications were distributed to stakeholders, including 10 ASIO-T4 reports published on the BGLU website.
- ASIO-T4 also partnered with federal, state and territory government security practitioners to develop and deliver protective security training courses and tailored advice.

Stakeholder evaluation

Stakeholders said that our protective security advice and services had helped them manage security risks. Briefings by senior ASIO officers were highly sought after; and partners reported that our presentations were generally viewed as being balanced, informative and influential. Government and industry stakeholders said that sectoral briefings continued to be valuable, and assessed the quality of presentations as generally of a high standard.

Stakeholders said ASIO-T4's expertise and contribution to national protective security arrangements during this reporting period was highly regarded. They noted the ASIO-T4 series of security manager and critical infrastructure guides as an impressive body of work. Stakeholders also noted ASIO-T4's increasing focus on building partners' protective security capabilities, and particularly highlighted its protective security and 'train the trainer' courses.

While stakeholders in defence industry and academia valued their engagement with ASIO, stakeholders recognised that considerably more work needs to be done to establish broader, more strategic partnerships in light of the assessed level of threat to Australia's defence capabilities, and research and development. This will be a major focus for ASIO in the years ahead as we rebuild our counter-espionage capabilities and expand our outreach to industry and academia.

ASIO-T4 case study: enhanced information-sharing network

Australia's state and territory law enforcement agencies share similar protective security challenges. Terrorist attacks in Australia, as elsewhere in the West, would probably involve weapons and tactics that are low-cost and relatively simple, including basic weapons such as everyday objects that do not require specialist skills.

To support the efforts of law enforcement agencies in providing protective security advice, ASIO-T4 established an information-sharing network with the protective security units in all state and territory policing agencies. Initially, ASIO-T4 engaged with individual jurisdictions—gauging requirements, current capabilities and challenges. We then gathered the entities together to co-develop the network. The network provides a platform for the agencies to share experience, capabilities, knowledge and information. It also provides direct access to ASIO-T4 expertise and, through ASIO-T4, reach into international partners. Through this collaborative partnership, ASIO-T4 and the national policing agencies can now deliver a more nationally consistent approach to protective security and specific technical protective security advice to stakeholders, including on crowded places.

ASIO-T4 case study: crowded places

The threat of terrorist attacks on crowded places has featured prominently in the public sphere over recent years, with the occurrence of a number of attacks on public crowded places, including in Nice, Berlin and London. Through the Australia–New Zealand Counter Terrorism Committee (ANZCTC), significant work has been done to address such threats.

In 2017–18, ASIO-T4 worked collaboratively with the protective security information-sharing network to develop a protective security training course focused on mitigating the risk of attack by hostile armed offenders, including the use of hostile vehicles, blasts and ballistics. ASIO-T4 engaged directly with law enforcement and Australian Government protective security professionals to develop the course outline and content. The course aims to provide a consistent level of understanding to support government security practitioners in meeting the current threat from hostile armed offenders. Personnel supporting the ANZCTC Crowded Places Advisory Group, within state and territory police and the Australian Federal Police, have been given priority attendance on the courses. Feedback from attendees has been overwhelmingly positive, with participants agreeing the course increased capability. We will deliver several additional training courses over the next 12 months.

Analysis of performance

In 2017–18, ASIO continued to protect Australia, its people and interests from threats to security by identifying and investigating threats; and providing advice to assist federal and state governments, law enforcement agencies, industry and academia to manage security risks and disrupt harmful activities. We achieved or substantially achieved all but one of the performance objectives set out in our 2017–18 corporate plan. This assessment of our performance was confirmed by stakeholder responses in our 2018 annual stakeholder survey, which was conducted by an independent senior reviewer with extensive national security experience. The senior reviewer conducted interviews with 74 senior stakeholders from 66 federal, state and territory government bodies; industry; and academia. He found that ASIO:

- continues to be highly regarded as an effective partner offering high-quality and largely unique services; and
- is viewed by its stakeholders as being a very credible organisation, with officers that are seen as customer-focused, well trained and professional.

The preceding performance statements provide further detail from the survey on our performance against each specific key activity.

We achieved these results in a challenging security and operating environment. Terrorism remains a persistent and serious threat, and foreign actors continue to conduct activities that undermine Australia's sovereignty. These threats are occurring within a context of rapidly changing and diversifying technology, which provides additional challenges.

Factors that contributed positively to our performance in responding to these challenges during this reporting period included:

- continuing close and effective working relationships with our national and international law enforcement, security and intelligence partners;
- expanding relationships and engagement with business, industry and academia;
- use and refinement of risk-led prioritisation frameworks that helped to focus our efforts on areas of highest potential harm, and areas that represented the most effective use of resources;
- a strong organisational focus on innovation and the development of new and improved security intelligence capabilities; and
- the Australian Government's investment in ASIO capabilities.

The scale and seriousness of the terrorism, espionage and foreign interference threats facing Australia have, however, continued to put significant pressure on our work programs. The heightened espionage and insider threat has increased demand for assurance about staff with access to Australia's most sensitive information and capabilities. This is reflected in the significant increase in demand for ASIO security assessments for PV clearance holders. Our assessment that we have *substantially* achieved our performance objectives for measure 2(b)—'National security partner agencies use our advice to disrupt and defend against harmful espionage, foreign interference and malicious insiders'—

acknowledges that, while we have performed well in most of the activities that contribute to this measure, including in completing security assessments for non-PV clearances, there is more work to be done to meet agreed time frames for PV clearances.

Security intelligence demands have also limited the availability of resources to collect foreign intelligence in Australia—refer to performance measure 2(c). We assessed our performance against this measure as *partially* achieved to recognise that, while our stakeholders valued our contributions in this area, we could not meet all of their requests to collect foreign intelligence.

As part of our response to the challenges of the security and operation environment, in 2018 we commenced a major transformation project to ensure the Organisation remains fit for purpose. This will include a change to our business model to capitalise on the benefits of augmented decision-making and data science. The successful transformation of ASIO into an organisation with world-class digital capability will contribute significantly to our ability to achieve our future performance objectives.

Report on financial performance

In 2017–18 we managed our expenditure effectively in a challenging operating environment; with continued high levels of security threat, demanding investigative workloads and stakeholder requirements, and increasing business costs placing considerable pressure on ASIO's resources and financial sustainability.

We achieved a small surplus of $0.972 million (excluding depreciation), which represents 0.2 per cent of the budget.

The 2017–18 financial year was the final year of the new policy proposal 'Enhancing security intelligence capabilities to counter the Islamist terrorism threat'. For this measure, we received $52.0 million in operating funding and an equity injection of $13.5 million for capital activities. Additionally, during this reporting period, we received operating funding of $19.4 million and capital funding of $1.4 million relating to additional estimates measures.

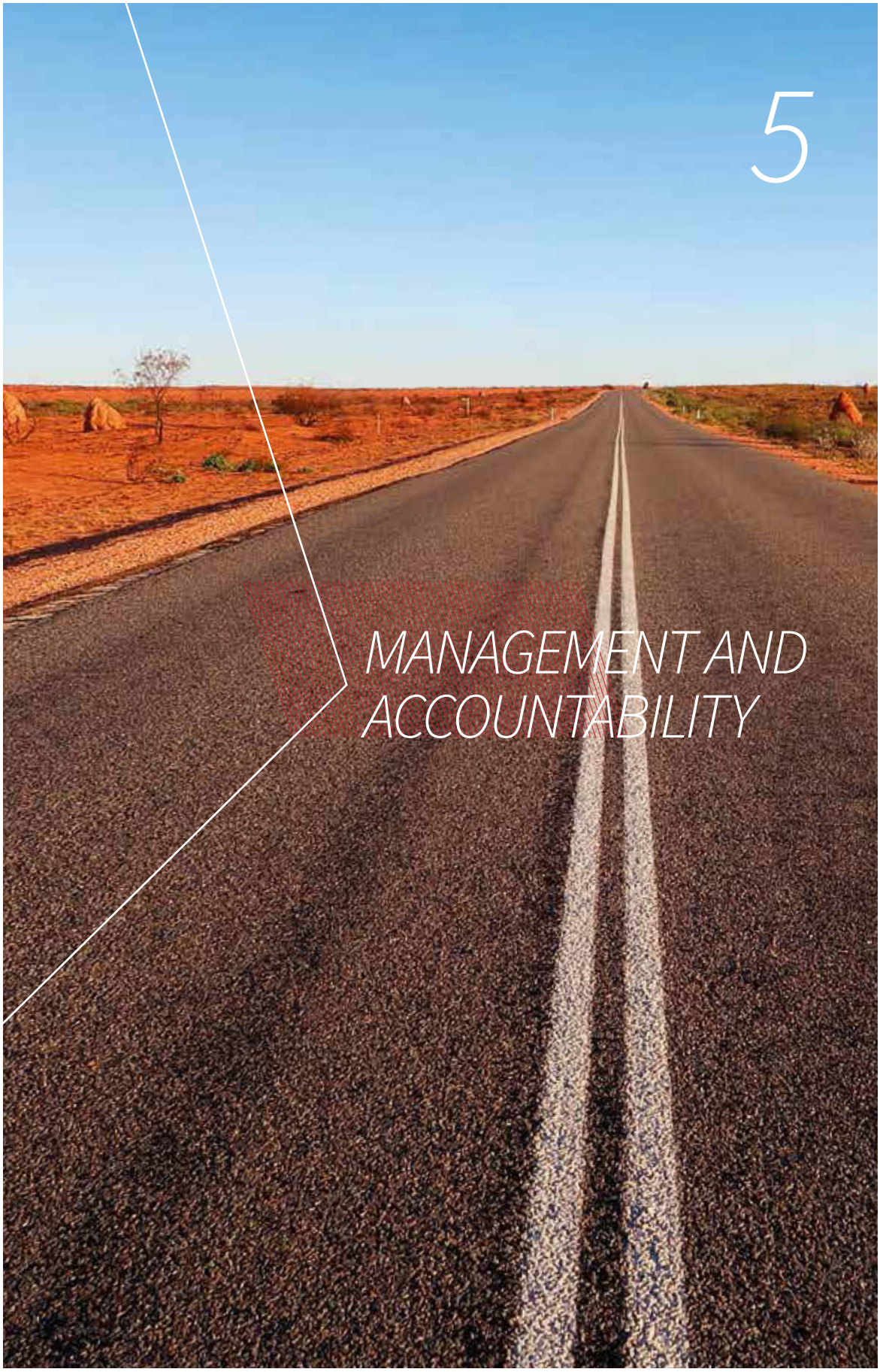
There are significant resourcing pressures in other areas of our work (refer 'Annual performance statements').

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), on our 2018–19 operating budget, and across the forward estimates.

Our DCB will remain under 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 a capital expenditure increase in 2017–18, a trend that we expect to continue over the forward estimates. While our DCB will increase from $68.6 million in 2017–18 to $85.6 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 2018–19 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 2017–18 is provided at Appendix A. Our total payments for this reporting period are at Appendix B.



5

MANAGEMENT AND ACCOUNTABILITY

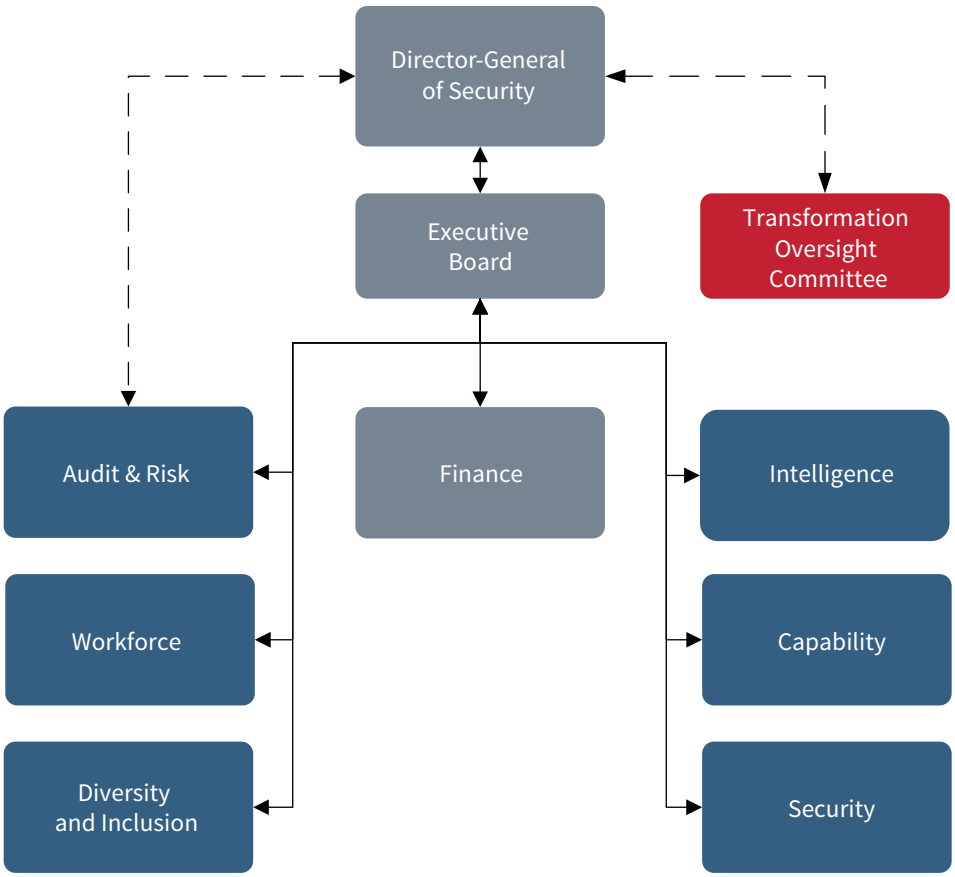
Corporate governance

The Director-General of Security is the accountable authority for ASIO under the Public Governance, Performance and Accountability (PGPA) Act. Our Executive Board and corporate governance committees support the Director-General to fulfil his responsibilities under the PGPA Act. Their roles are to provide strategic direction, manage risk, coordinate effort and evaluate performance in support of ASIO's mission.

New governance arrangements were implemented during this reporting period to strengthen our oversight of performance and risk management. In addition to our corporate committees which report regularly to the Executive Board on matters such as developments in the security environment, our budget, capability development, risk management and progress toward our ASIO2020 and diversity and inclusion goals, the Executive Board established three new standing committees and commenced a new performance- and risk-reporting regime.

We also commissioned a review of ASIO's future data and technology needs during this reporting period, resulting in a report titled *A digital transformation of the Australian Security Intelligence Organisation*. One of the report's recommendations was the introduction of governance arrangements to support the transformation in the form of additional committees. One of the three new committees included the Transformation Oversight Committee, which was established in February 2018 to provide oversight, leadership and governance—to ensure momentum is maintained and ASIO's Enterprise Transformation delivers value.

Governance framework standing committees 2017–18



All of the corporate governance committees report to the Executive Board on ASIO's performance and risk against our four key activities defined in ASIO's corporate plan 2017–18.

ASIO Executive Board

The Executive Board is ASIO's peak advisory committee, which assists the Director-General to govern ASIO. Its membership comprises the Director-General, the Deputy Directors-General and an external member.

The board met every two months during this reporting period, setting ASIO's overall strategic direction and overseeing the management of its resources. The board received regular reporting from our corporate committees on matters such as developments in the security environment, our budget, capability development, performance and risk management, as well as reporting on progress toward our Enterprise Transformation, ASIO2020, and diversity and inclusion goals.

Intelligence Committee

The Intelligence Committee makes decisions relating to ASIO's security intelligence program. The committee met fortnightly during this reporting period and conducted triannual reviews of performance and risk.

Workforce Committee

The Workforce Committee makes decisions relating to ASIO's workforce program. The committee met monthly during this reporting period and conducted triannual reviews of performance and risk.

Security Committee

The Security Committee makes decisions relating to ASIO's internal security program. The committee met bimonthly during this reporting period and conducted triannual reviews of performance and risk.

Finance Committee

The Finance Committee makes decisions relating to ASIO's financial management program. The committee met monthly during this reporting period and conducted triannual reviews of performance and risk.

ASIO Diversity and Inclusion Committee

The ASIO Diversity and Inclusion Committee makes decisions relating to ASIO's diversity and inclusion program. The committee met monthly during this reporting period and conducted triannual reviews of performance and risk.

Capability Committee

The Capability Committee makes decisions relating to ASIO's capability program. The committee met bimonthly during this reporting period and conducted triannual reviews of performance and risk.

Transformation Oversight Committee

The Transformation Oversight Committee was established to provide oversight and leadership to ensure momentum is maintained and that ASIO's Enterprise Transformation delivers value. The committee is accountable for realising the Enterprise Transformation vision, delivery and performance.

Audit and Risk Committee

The Audit and Risk Committee was established to meet the requirements of section 45 of the PGPA Act. 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.

Fraud is managed in line with the Commonwealth Fraud Control Framework. ASIO's Fraud Risk Assessment and Fraud Control Framework 2016–18 remain current and will be updated in the next reporting period. All staff must complete mandatory e-Learning on ethics and accountability, which contains modules on fraud, every three years.

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.

External scrutiny

Ministerial accountability

ASIO's ministerial accountability changed during this reporting period. In May 2018 our ministerial accountability moved from the Attorney-General to the Minister for Home Affairs, the Hon. Peter Dutton MP. The Minister for Home Affairs exercises all the powers and functions under the ASIO Act except those that remain explicitly with the Attorney-General. These reflect the Attorney-General's role as first law officer with responsibility for integrity and oversight, including being consulted on ministerial guidelines, issuing ASIO warrants and authorising special intelligence operations.

We keep the Minister for Home Affairs informed of significant national security developments, as well as other important issues affecting ASIO. During this reporting period, we provided advice to our minister on a range of investigative, operational and administrative issues, which were communicated primarily through more than 230 formal submissions. The Director-General also briefed other ministers on security issues and matters relevant to their portfolios, when required.

We conduct our security intelligence activities in accordance with ministerial guidelines, which are available online at www.asio.gov.au/attorney-generals-guidelines.html. The guidelines stipulate that we must conduct our activities in a lawful, timely and efficient manner, while 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 following a recommendation by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), and we contributed to that review during this reporting period.

The Attorney-General issues all warrants for ASIO to employ its special powers, except for questioning warrants, and questioning and detention warrants, which are issued by a 'prescribed 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 the Attorney-General's Department 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 helped us carry out our functions.

5

Engagement with parliament

Leader of the Opposition

The Director-General of Security is a statutory position, with a responsibility to ensure the provision of 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 annual report. Throughout 2017–18, 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 policies, governance and expenditure. ASIO appeared before the PJCIS in closed and public hearings for its Review of Administration and Expenditure no. 16 (2016–17), providing both oral and written submissions.

The PJCIS also reviews the listing of terrorist organisations under the *Criminal Code Act 1995* and key national security legislation. During 2017–18, ASIO appeared at a number of hearings about the relisting of terrorist organisations.

The PJCIS also conducts inquiries into other matters relating to the intelligence agencies, as referred by the government or the parliament. During this reporting period, ASIO appeared before a number of public and closed PJCIS hearings, including the Review of the Foreign Influence Transparency Scheme Bill 2017, the Review of the Home Affairs and Integrity Agencies Legislation Amendment Bill 2017, the Review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, and the Review of the Security of Critical Infrastructure Bill 2017. ASIO also continued to contribute to the PJCIS review of ASIO's statutory questioning and detention powers.

The PJCIS's recommendations from its inquiries are reported to each House of the parliament and to the responsible minister. ASIO's submissions 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 24 October 2017, 27 February 2018 and 24 May 2018. Our evidence to the committee can be found in the estimates *Hansard* for those days (refer to www.aph.gov.au/Parliamentary_Business/Senate_Estimates and navigate to the relevant hearing).

Independent oversight

Inspector-General of Intelligence and Security

The role of the Inspector-General of Intelligence and Security (IGIS) is to review the activities of the National Intelligence Community 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 retains statutory powers similar to a standing royal commission.

The Australian community's trust and confidence in how ASIO fulfils its legislative requirements and embodies ethical standards is critical to ASIO's reputation and ongoing effectiveness as Australia's security intelligence organisation. Every ASIO officer is responsible for complying with ASIO's legislative requirements as well as internal policies and procedures. This includes acting with propriety and meeting the ethical standards expected by the Australian community.

During 2017–18 the IGIS regularly inspected activities across our operational functions, and investigated complaints received by her office. Details can be found in the IGIS annual report, available online from www.igis.gov.au.

In February 2018, the IGIS commenced an inquiry into an ASIO matter under section 8(2) of the IGIS Act. The inquiry is continuing at the time of writing this report.

Consistent with our commitment to acting with legality and propriety, we are taking steps to address areas identified by the IGIS during this reporting period as requiring improvement and further attention.

During this reporting period, we continued to work closely with the IGIS to support our independent mandate. This included providing a range of information briefings to IGIS staff on operational matters, which covered a wide range of topics including new operational capabilities and initiatives.

Independent National Security Legislation Monitor

The Independent National Security Legislation Monitor's (INSLM) role is to review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation, and to report regularly to the Prime Minister and the parliament.

During this reporting period, the INSLM commenced a review of the prosecution and sentencing of children for Commonwealth terrorist offences. We are contributing to the review, which is still underway at the time of reporting. Our unclassified submission to the INSLM and evidence provided 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 Department of Home Affairs 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 conducts subsequent reviews every 12 months for the duration of the adverse assessment.

We also undertake 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 that ASIO has relied on to make its assessment and any information ASIO has obtained since the adverse security assessment was completed or provided to the Independent Reviewer, including information from 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.

Significant legal matters affecting ASIO's business

Our involvement in legal proceedings in courts, tribunals and other forums continued at a high tempo. Matters included terrorism and other prosecutions, judicial and merits review of security assessments, and civil lawsuits. We provided information for use as evidence, with appropriate protections, to prosecutions, and responded to subpoenas and disclosure requests.

The Administrative Appeals Tribunal (AAT) reviewed a number of security assessments, primarily concerning the cancellation of passports held by people who had travelled, or intended to travel, overseas to engage in politically motivated violence.

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

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

Tribunal reviews—security assessments

Over this reporting period, we managed 15 adverse security assessment reviews before the Administrative Appeals Tribunal, including those relating to cancelled passports, visas and security clearances.

Of these:

- one application was filed but not continued;
- four matters were pending at the end of this reporting period;

- two assessments were remitted to ASIO by consent for new assessments to be prepared, which resulted in two non-prejudicial assessments being issued in this reporting period;
- three applications were dismissed;
- four matters were heard, with three adverse security assessments being affirmed or affirmed with minor variations and one decision remaining 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 and the High Court of Australia during this reporting period.

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 the Islamic State of Iraq and the Levant (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 he was given the opportunity to answer questions as comprehensively as he wished.
On 25 May 2017, the Full Federal Court heard an appeal by the applicant. On 11 July 2017, the court delivered its judgement which accepted the appeal by BSX15 and set aside the assessment. The court found that ASIO should have questioned BSX15 further about his other names; in particular, its assessment that he was identical with 'Muthana Najim Abdullah'. The court found that BSX15 was not afforded sufficient procedural fairness, set aside the assessment and awarded BSX15's costs.

ASIO has carefully considered this judgement.

Plaintiffs S111A-H/2018 v. Minister for Home Affairs, Director-General of Security, and Ors (No. S111 of 2018)

In April 2018 the plaintiffs commenced High Court proceedings seeking damages against the Commonwealth, release from immigration detention, and the setting aside of the security assessment on the alleged grounds that it was beyond power, used for an improper purpose, made in bad faith, contrary to the principles of procedural fairness, and/or unreasonable.

The case is still before the High Court.

Management of human resources

The Thodey Review emphasised the importance of cultural and people management reform in achieving enterprise transformation. In particular it identified the need for the Organisation to:

- escalate the adoption of more agile models of recruiting, managing, developing and deploying professional staff and skills; and
- raise digital literacy across the workforce.

As a result, during the latter half of the reporting period, we initiated a review of our human resource operating model and strategies, with a view to implementing enterprise-wide changes from mid-2018 to 2019. Meanwhile, we continued to advance several human resources (HR) initiatives, laying solid foundations for the reforms ahead.

Recruitment

In 2017–18 we achieved a net growth of 49 ongoing staff. As at 30 June 2018, we employed 1814.9 full-time equivalent staff (refer Appendix C). Our separation rate at that time was 5.05 per cent.

The attraction of high-quality candidates to meet our people capability needs and ongoing growth requirements is one of the Organisation's highest corporate priorities. At the same time, it presents one of the greatest challenges due to the highly competitive external market for specialised skills and the need for candidates to meet stringent security clearance requirements.

A more strategic and nuanced approach to candidate sourcing was adopted during the year, particularly for intelligence and information technology roles that have traditionally been more difficult to fill. The aim of this approach is to generate more informed and motivated candidates, who both possess the required capabilities and are more able to transition to ASIO employment after a long recruitment lead time. We have continued to shape and refine our selection approach for assessing candidates to ensure the capability requirements of the Organisation are being met.

Over the reporting period, our recruitment for all graduate programs continued successfully, including for the Future Technologist (formerly Technical Graduate), Intelligence Officer and Intelligence Analyst streams. Further, we established a new legal graduate program to complement our other graduate initiatives. Delivering effective junior lawyers upon successful completion, the program provides the opportunity to undertake supervised legal work across all areas of law practised in ASIO's Office of Legal Counsel, combined with targeted training opportunities, to develop the necessary legal competencies. This new program attracted a strong field of high-quality candidates.

We also recommenced the Information Management and Information Technology Traineeship. The aims of the traineeship are to establish a dedicated career pathway for school leavers and develop critical skills to support the technology capability of the Organisation.

One of the future objectives, reinforced by the Thodey Review, is to invest in the continuous improvement of HR and recruitment systems and processes. Our aim is to make recruitment practices more agile

and responsive to both organisational needs and the competitive demands of current labour markets. In May, an end-to-end review of these practices was conducted which is expected to result in further changes to the way we approach and manage recruitment in coming years.

Training

We continued to provide an extensive range of personal and professional development opportunities to effectively meet the diverse needs of our staff during the 2017–18 reporting period, with a focus on positioning all staff to meet ASIO's Enterprise Transformation program objectives. This included providing training opportunities to support our enhanced career development and management programs and pathways. Notably, all members of our Senior Executive Service commenced a tailored 360-degree feedback and executive coaching program during this period, which included tailored adaptive leadership and change management support.

In 2017–18:

- we approved or conducted 135 training courses, including 4057 face-to-face training activities attended by 1367 staff;
- our staff completed 2554 mandatory and 784 non-mandatory e-Learning courses across seven mandatory and 31 non-mandatory online programs;
- we allocated $316 413 to 137 staff attending over 90 ASIO-supported study programs;
- we allocated $159 050 to 13 domestic and two international development opportunities attended by 15 members of our Senior Executive Service;
- we allocated $212 982 to 49 members of our Senior Executive Service for the 360-degree survey and feedback executive coaching program; and
- we allocated $180 000 to 40 employees under the Language Skills Development Program.

By adopting the 70-20-10 learning model, we equip our employees with the foundational, core job role and advanced competencies required to successfully operate in the workplace across a diverse range of generic and specialist skillsets—these include management and leadership, personal safety, collection and analysis, language, and surveillance capability development programs. We undertake training-needs analysis to understand training requirements, followed by reviews and evaluation to update the programs for continuous improvement and alignment of training with ASIO's objectives. We deliver our training programs through a mix of in-house learning and development, training by subject matter experts and external training providers. We provide a tailored ASIO-specific training course to in-house trainers to ensure the best learning outcomes—this has resulted in consistently positive feedback from both course participants and line managers, indicating that ASIO has continued to deliver the capability development requirements to support its employees' diverse roles.

Strategic workforce and performance management

Recognising the critical role of leadership in promoting a high-performance, innovative and inclusive culture, we developed a Leadership Charter during the reporting period. Centred on four overarching principles—mission focused, inclusive, committed to building people, and enterprise minded—the charter articulates the behaviours expected of all leaders in ASIO, regardless of level.

We concluded a review of the skills and capabilities required in our intelligence, executive, technological and corporate roles and developed a new agency-specific and systemised job family model to embed these requirements within future workforce planning and practices. The model came into effect on 1 July 2018.

This work also fed directly into improvements to career management practices which during 2017–18 focused on providing enhanced information and tools to better inform staff about potential career options, and enable them, with increased knowledge and confidence, to identify and engage in relevant professional development. Further, work continues to develop a new integrated learning management system to support the recording and use of performance information, identification and provision of training, development of talent, and career planning.

Performance management

Performance management policy and processes continued to be refined during the year. Building on 2015–16 and 2016–17 reforms, we achieved 100 per cent rate of compliance for employee participation in the performance cycle.

To further strengthen our high performance culture, we are now focusing on strengthening the quality of employee and line manager discussions supported by a training and coaching framework and early intervention strategies to enhance performance. New technologies will also be employed to support two-way exchanges, aid alignment of individual objectives with organisational priorities and goals and help identify current and future development requirements.

Diversity and inclusion

We are committed to creating a diverse and inclusive environment where differences are valued, and staff are respected and supported to be highly capable, innovative and adaptive. Creating this workforce and culture will ensure we are best placed to achieve our purpose.

In 2017–18 we undertook a range of initiatives in support of this vision, including:

- releasing ASIO's Diversity and Inclusion Strategy 2018–20, which articulates our diversity and inclusion goals, and paves the way for us to broaden our staffing profile and harness the diversity of our existing workforce;

- strengthening our employee engagement program for staff on long-term leave and establishing family room facilities to provide support for staff members with caring responsibilities;
- rolling out the ASIO-wide 'if not, why not' approach to flexible working arrangements;
- establishing staff-initiated and -led diversity networks that form an essential part of creating a diverse and inclusive culture where all staff feel valued, respected, included and safe;
- creating a community of support for Aboriginal and Torres Strait Islander employees;
- delivering a number of cultural awareness initiatives, including a cross-cultural communication week and training packages; and
- continuing our commitment to the Male Champions of Change program, including the establishment of a dedicated EL1 position to support this program; and our commitment to reviewing our current targets, actions and transparency in relation to gender equality, particularly for shortlisting and promotion at the EL1 level and above.

In 2017–18 we also gave staff opportunities to broaden their awareness and understanding of diversity and inclusion issues by offering active membership of groups including the Diversity Council of Australia and Pride in Diversity; offering participation in a range of presentations and workshops such as the Global Summit of Women and LGBTI 'train the trainer' courses; and hosting keynote speakers including the Hon. Michael Kirby AC, Professor Brian Schmidt AC FRS FAA and leading Science, Technology, Engineering, and Mathematics (STEM) innovators and advocates Dr Catherine Ball and Dr Cathy Foley.

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

We are committed to creating a diverse and inclusive environment where all staff are valued and respected in order to build a highly capable, innovative and adaptive workforce to achieve our purpose.

DRIVER
ASIO senior leadership

LEAD BY EXAMPLE
ASIO middle management

RESPONSIBILITY
All staff

FOUNDATION
Diversity and Inclusion Strategy 2018–20
and ASIO Diversity and Inclusion Committee

DIVERSITY
In ASIO, we believe that our people are our best asset and that our differences and individual perspectives bring value.

INCLUSION
In ASIO, our differences are valued rather than tolerated and we are able to bring our whole self to work.

Diversity and inclusion is everyone's right and responsibility.

Workplace agreement

We continued to operate under our 10th Workplace Agreement, which was agreed in 2016 and expires in 2019. The agreement meets our requirement under the ASIO Act to adopt the employment principles of the Australian Public Service, when they are consistent with the effective performance of the Organisation. The consultation and negotiation for our 11th Workplace Agreement will be undertaken in the 2018–19 reporting period.

Work health and safety

ASIO is committed to providing a safe working environment and ensuring the health, safety and welfare of our staff.

Work continued on implementing recommendations arising from ASIO's strategic review of its work health and safety programs and performance. Work health and safety governance and performance monitoring structures have been strengthened, and we continue to integrate health and safety considerations across the spectrum of our day-to-day work activities. In 2017–18 a review of ASIO's Health and Safety Representative (HSR) network resulted in improved HSR representation on the Work Health and Safety Committee. The network continues to engage with work teams and inform them about the importance of maintaining a safe workplace. ASIO's first aid officers provided a critical first-response function when safety incidents occurred.

Pivotal to health and safety in ASIO is a mental health and wellbeing strategy, which is being developed to complement programs that support the physical health and safety of ASIO staff. A notable event in the health and wellbeing calendar over this period was a presentation to staff by Wayne Schwass, former AFL player and mental health advocate, about his experience with depression and the importance of maintaining good mental health.

We maintained our active early intervention and preventative approach to compensation and rehabilitation. No areas of non-compliance were identified in 2017–18, and ASIO continued to enhance processes and maintain a positive relationship with Comcare in both work health and safety, and rehabilitation.

- In line with legislated notification obligations, we reported two incidents to Comcare in 2017–18.
- 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*.

Disability reporting

Since 1994, non-corporate Australian Government entities have reported on their performance as policy advisers, purchasers, employers, regulators and providers 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. Since 2010–11, entities have not been required to report on these functions.

The Commonwealth Disability Strategy has been replaced by the National Disability Strategy 2010–20, which sets out a 10-year national policy framework to improve the lives of people with a 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 show 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 on people with a disability.

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 the ASIO Staff Association representatives to discuss the health of the workplace.

The ASIO Ombudsman provided valuable support and advice to employees and line managers during this reporting year, including:

- providing advice and guidance in response to three informal contacts from staff;
- undertaking two preliminary reviews of investigative matters;
- responding to three policy matter queries;
- undertaking two health checks of business areas;
- carrying out two investigations relating to the Code of Conduct.

The ASIO Ombudsman also gave valuable advice on the development and formulation of our human resources policy. The ASIO Ombudsman met weekly with the Assistant Director-General of Human Resources; every fortnight with the First Assistant Director-General of Corporate Services; and every two months with the Deputy Director-General of the Strategic Enterprise Management Group. In addition, senior ASIO managers drew on the ASIO Ombudsman's unique skills and experience to inform their decision-making on the application of policy.

In 2017–18 the ASIO Ombudsman did not participate in any work related to public interest disclosures.

Property and procurement

The Ben Chifley Building continued to support the business and capability needs of ASIO and its partners. Our facilities, including Australia's largest security-accredited auditorium, hosted a broad range of events in 2017–18. The corporate suites, including the security-accredited auditorium, were booked on 1692 occasions. In addition, the data centre provided capability for National Intelligence Community partners.

We continued to work closely with the Australian Federal Police to deliver on a range of joint accommodation projects.

Environmental performance

We continued our commitment to reducing our carbon footprint and improving our environmental performance. In 2017–18 we participated in the 11th consecutive Earth Hour event, and achieved the following:

- reduced our total energy consumption by 253 110 kilowatt hours through the use of solar panels, saving approximately $36 000 and 232 tonnes of carbon emissions;
- increased efficiencies in our data centres by adjusting temperatures and installing monitoring equipment to reduce energy consumption and decrease maintenance costs;
- reduced our use of water for cooling towers and the air-conditioning plant by fine-tuning processes, and monitoring and repairing water leaks;
- used 1791 kilolitres of bore water for irrigation and toilet flushing, reducing reliance on potable water and saving approximately $9200 worth of potable water;

- used 19 240 kilolitres of captured stormwater for irrigation and toilet flushing, reducing reliance on potable and bore water and saving approximately $103 300 worth of potable water; and
- recycled 23 612 kilograms of waste, including paper products, toner cartridges, batteries, scrap metal and fluorescent tubes.

Procurement

Throughout 2017–18 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.

We support 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 to support small- and medium-sized enterprises include:

- standardising contracts and approach-to-market templates, which use clear and simple language;
- ensuring information is easily accessible through the 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 payments to small business are available on the Treasury's website, www.treasury.gov.au.

Consultants

We entered into 35 new consultancy contracts involving total actual expenditure of $10.6 million (goods and services tax (GST)-inclusive). In addition, nine ongoing consultancy contracts were active during the period, involving total actual expenditure of $0.24 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 we used appropriate methods for engaging and contracting consultants. We engaged consultants when we needed 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, and information on the value of contracts and consultancies is available on the AusTender website. However, 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 to the PJCIS, which oversees 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 the Auditor-General with access to the contractor's premises.

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 to the PJCIS.

Advertising and market research spends

We spent $676 741 on advertising in 2017–18, 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

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY 81

INDEPENDENT AUDITOR'S REPORT 83

STATEMENT OF COMPREHENSIVE INCOME 86

STATEMENT OF FINANCIAL POSITION 87

STATEMENT OF CHANGES IN EQUITY 88

STATEMENT OF CASH FLOWS 89

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS 90

Overview 90

1. Financial Performance 91

1.1 EXPENSES 91

1.2 OWN-SOURCE REVENUE AND GAINS 92

2. Financial Position 93

2.1 FINANCIAL ASSETS 93

2.2 NON-FINANCIAL ASSETS 94

2.3 PAYABLES 96

2.4 PROVISIONS 96

3. Funding 98

3.1 APPROPRIATIONS 98

4. Managing uncertainties 99

4.1 CONTINGENT ASSETS AND LIABILITIES 99

4.2 FINANCIAL INSTRUMENTS 100

5. Other information 101

5.1 KEY MANAGEMENT PERSONNEL REMUNERATION 101

5.2 RELATED PARTY DISCLOSURES 101

5.3 MAJOR BUDGET VARIANCES 101

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 2018 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

15 August 2018

Australian National Audit Office

INDEPENDENT AUDITOR'S REPORT

To the Minister for Home Affairs

Opinion

In my opinion, the financial statements of the Australian Security Intelligence Organisation for the year ended 30 June 2018:

(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 2018 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 2018 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; and
- Notes to and forming part of the financial statements.

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* (the Code) to the extent that they are not in conflict with the *Auditor-General Act 1997*. 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. The Director-General of Security is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the assessment indicates that it is not appropriate.

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

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 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 Director-General of Security.
- conclude on the appropriateness of the Director-General of Security'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

Kristian Gage

Executive Director

Delegate of the Auditor-General

Canberra

15 August 2018

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2018

	Notes	2018 $'000	Original Budget 2018 $'000	2017 $'000
EXPENSES				
Employee benefits	1.1.A	248 944	244 075	239 924
Suppliers	1.1.B	199 453	196 294	181 969
Depreciation and amortisation	2.2.A	89 365	84 708	88 335
Other	1.1.C	566	-	1291
TOTAL EXPENSES		**538 328**	**525 077**	**511 519**
OWN-SOURCE INCOME				
Revenue				
Sale of goods and services	1.2.A	16 494	19 218	15 008
Other revenue	1.2.B	11 531	3196	5115
Gains	1.2.C	143	140	2553
TOTAL OWN-SOURCE INCOME		**28 168**	**22 554**	**22 676**
NET COST OF SERVICES		**(510 160)**	**(502 523)**	**(488 843)**
REVENUE FROM GOVERNMENT	3.1	**421 767**	**417 815**	**402 998**
DEFICIT ON CONTINUING OPERATIONS		**(88 393)**	**(84 708)**	**(85 845)**
OTHER COMPREHENSIVE INCOME				
Changes in asset revaluation surplus		36 811	-	-
TOTAL COMPREHENSIVE LOSS		**(51 582)**	**(84 708)**	**(85 845)**

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

STATEMENT OF FINANCIAL POSITION as at 30 June 2018

	Notes	2018 $'000	Original Budget 2018 $'000	2017 $'000
ASSETS				
Financial assets				
Cash and cash equivalents	2.1.A	23 552	10 809	17 338
Trade and other receivables	2.1.B	70 807	71 402	76 702
Accrued revenue		753	916	1644
Total financial assets		***95 112***	***83 127***	**95 684**
Non-financial assets				
Prepayments		26 919	19 252	25 911
Land and buildings	2.2.A	161 127	144 514	153 938
Property, plant and equipment	2.2.A	146 458	151 615	130 341
Computer software	2.2.A	59 274	51 662	50 616
Total non-financial assets		***393 778***	***367 043***	**360 806**
TOTAL ASSETS		**488 890**	**450 170**	**456 490**
LIABILITIES				
Payables				
Suppliers	2.3.A	8829	18 085	11 865
Other payables	2.3.B	24 704	6680	25 911
Total payables		***33 533***	***24 765***	**37 776**
Provisions				
Employee provisions	2.4.A	78 834	77 198	75 256
Restoration obligations	2.4.B	6072	3700	4938
Total provisions		***84 906***	***80 898***	**80 194**
TOTAL LIABILITIES		**118 439**	**105 663**	**117 970**
NET ASSETS		**370 451**	**344 507**	**338 520**
EQUITY				
Parent equity interest				
Contributed equity		752 158	750 760	668 644
Reserves		69 858	33 046	33 047
Accumulated deficit		(451 565)	(439 299)	(363 171)
TOTAL EQUITY		**370 451**	**344 507**	**338 520**

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

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2018

	2018	Original Budget 2018	2017
	$'000	$'000	$'000
RETAINED EARNINGS			
Opening balance	(363 172)	(354 591)	(277 326)
Comprehensive income			
Deficit for the period	(88 393)	(84 708)	(85 845)
Closing balance	***(451 565)***	***(439 299)***	**(363 171)**
ASSET REVALUATION RESERVE			
Opening balance	33 047	33 046	33 047
Other comprehensive income			
Changes in asset revaluation surplus	36 811	-	-
Closing balance	***69 858***	***33 046***	**33 047**
CONTRIBUTED EQUITY			
Opening balance	668 644	668 644	626 449
Transactions with owners			
Contributions by owners			
Equity injection—appropriation	14 939	13 541	14 103
Departmental capital budget	68 575	68 575	28 092
Closing balance	***752 158***	***750 760***	**668 644**
CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT	**370 451**	**344 507**	**338 520**

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 2018

	Notes	2018 $'000	Original Budget 2018 $'000	2017 $'000
OPERATING ACTIVITIES				
Cash received				
Appropriations		477 892	417 716	421 916
Sales of goods and services		10 498	22 225	13 977
Net GST received		22 083	16 286	19 794
Other		11 381	1556	2808
Total cash received		***521 854***	***457 783***	**458 495**
Cash used				
Employees		245 562	243 574	234 556
Suppliers		220 169	198 324	195 772
Section 74 receipts		30 176	19 191	26 493
Total cash used		***495 907***	***461 089***	**456 821**
NET CASH FROM OPERATING ACTIVITIES		**25 947**	**(3306)**	**1674**
INVESTING ACTIVITIES				
Cash received				
Proceeds from sales of property, plant and equipment		948	-	760
Total cash received		***948***	***-***	**760**
Cash used				
Purchase of property, plant and equipment		55 244	78 852	51 850
Purchase of computer software		32 553	-	24 414
Total cash used		***87 797***	***78 852***	**76 264**
NET CASH USED BY INVESTING ACTIVITIES		**(86 849)**	**(78 852)**	**(75 504)**
FINANCING ACTIVITIES				
Cash received				
Contributed equity		67 116	82 116	68 732
Total cash received		***67 116***	***82 116***	**68 732**
NET CASH FROM FINANCING ACTIVITIES		**67 116**	**82 116**	**68 732**
Net increase (decrease) in cash held		6214	(42)	(5095)
Cash and cash equivalents at the beginning of the reporting period	2.1.A	17 338	10 851	22 433
CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD		**23 551**	**10 809**	**17 338**

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

There were no new or revised accounting standards that were issued prior to the signing of the statement by the Director-General that are applicable to the current reporting period.

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

	2018 $'000	2017 $'000
1.1 EXPENSES		
1.1.A Employee benefits		
Wages and salaries	**195 219**	186 995
Superannuation		
▷ Defined contribution plans	**17 915**	16 569
▷ Defined benefit plans	**15 117**	15 330
Leave and other entitlements	**20 361**	20 263
Separation and redundancies	**332**	767
Total employee benefits	**248 944**	**239 924**
1.1.B Suppliers		
Goods supplied	**8702**	6211
Services supplied	**146 582**	136 925
Operating lease payments	**42 239**	37 202
Workers' compensation premiums	**1930**	1631
Total supplier expenses	**199 453**	**181 969**

Accounting policy

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

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	**53 793**	54 853
Between 1 to 5 years	**213 380**	216 636
More than 5 years	**312 641**	371 083
Total operating lease commitments	***579 814***	***642 572***
1.1.C Other expenses		
Finance costs: unwinding of discount—restoration obligations	**124**	238
Impairment of receivables	**7**	6
Write-down and impairment of property, plant and equipment	**419**	1039
Losses from asset sales	**16**	8
Total other expenses	**566**	**1291**

	2018	2017
	$'000	$'000

1.2 OWN-SOURCE REVENUE AND GAINS

1.2.A Sale of goods and services

Sale of goods	-	49
Sale of services	16 494	14 959
Total sale of goods and services	**16 494**	**15 008**

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

Sub-lease—rental income	10 297	3910
Resources received free of charge—remuneration of auditors	150	145
Royalties	8	18
Other	1076	1042
Total other revenue	**11 531**	**5115**

Sublease rental income commitments

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

Commitments for rental income are receivable:

Within 1 year	2722	5444
Between 1 to 5 years	9318	23 811
More than 5 years	9196	24 282
Total rental income commitments	***21 236***	***53 537***

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

Expiry of lease restoration obligation	-	2320
Other gains	143	233
Total gains	**143**	**2553**

Accounting policy

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

2. Financial Position

	2018 $'000	2017 $'000
2.1 FINANCIAL ASSETS		
2.1.A Cash and cash equivalents	**23 552**	**17 338**

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	**7615**	4753
Appropriation receivable	**57 449**	67 000
GST receivable	**5743**	4949
Total trade and other receivables	**70 807**	**76 702**

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

Credit terms for goods and services were within 30 days (2017: 30 days).

Financial assets were assessed for impairment at 30 June 2018. 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 collectability 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 2017					
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 1 July 2017	***4363***	***149 574***	***130 341***	***50 616***	***334 894***
Additions by purchase	98	3414	48 595	32 784	84 891
Revaluations	2192	20 768	14 861	-	37 821
Depreciation and amortisation expense	(244)	(19 039)	(46 064)	(24 018)	(89 365)
Disposals—other	-	-	(1275)	(108)	(1383)
Net book value 30 June 2018	**6410**	**154 717**	**146 458**	**59 274**	**366 859**
Gross book value	6472	159 194	154 860	152 562	473 088
Accumulated depreciation, amortisation and impairment	(62)	(4477)	(8402)	(93 288)	(106 229)
Net book value 30 June 2018	**6410**	**154 717**	**146 458**	**59 274**	**366 859**

Computer software

The carrying value of computer software included $23.844m (2017 $25.498m) purchased software and $35.430m (2017 $25.118m) internally generated software.

Impairment

Non-financial assets are assessed for impairment at the end of each reporting period. There are no indicators of impairment for property, plant, equipment and computer software. Any reduction in assets' carrying value due to impairment throughout the year have been accounted for in the Statement of Comprehensive Income.

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	-	-	2895	7816	10 711
Between 1 to 5 years	-	-	-	2734	2734
Total capital commitments	***-***	***-***	***2895***	***10 550***	***13 445***

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 $4000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

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-down 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:

	2018	2017
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 2018. 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 (2017: 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 professional external consultants to conduct a comprehensive valuation of carrying amounts for all non-financial assets (excluding software) at 30 April 2018. Comprehensive valuations are carried out at least once every three years. JLL 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 2018 are detailed above in Note 2.2.A.

	2018	2017
	$'000	$'000
2.3 PAYABLES		
2.3.A Suppliers		
Trade creditors and accruals	**8829**	11 865
Total suppliers	**8829**	**11 865**

Settlement is usually made within 30 days.

2.3.B Other payables		
Salaries	**1905**	1908
Superannuation	**263**	252
Unearned income	**2092**	6719
Amortisation of rent expense	**17 769**	13 198
Lease incentives	**556**	1512
Fringe benefits tax	**2119**	2322
Total other payables	**24 704**	**25 911**
2.4 PROVISIONS		
2.4.A Employee provisions		
Leave	**78 834**	75 256
Total employee provisions	**78 834**	**75 256**

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

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

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

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

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

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

	2018	2017
	$'000	$'000
2.4.B Restoration obligations	**6072**	**4938**
Carrying amount 1 July 2017	**4938**	7374
Additional provisions made	**-**	836
Provision utilised	**-**	(1000)
Lease expiry	**-**	(2510)
Unwinding of discount or change in discount rate	**124**	238
Revaluation as at 30 June	**1010**	-
Closing balance	***6072***	***4938***

ASIO has a number of agreements for the leasing of premises which contain provisions requiring restoration of the premises to original condition at the conclusion of the lease. ASIO has made a provision to reflect the present value of this obligation.

3. Funding

3.1 APPROPRIATIONS

3.1.A Annual Departmental appropriations

	Ordinary annual services	Capital budget	Equity injections
	$'000	$'000	$'000
2018			
Appropriation Act			
Annual appropriation	**421 767**	68 575	14 939
PGPA Act			
Section 74 transfers	**30 176**	-	-
Total appropriation	**451 943**	**68 575**	**14 939**
Appropriation applied (current and prior years)	**(471 678)**	(58 575)	(8541)
Variance	***(19 735)***	***10 000***	***6398***

Operating appropriation variances in 2017–18 are due to prior year appropriations applied in the current year. Capital appropriations remain unspent due to the timing of asset purchases.

The following entities spend money from the Consolidated Revenue Fund on behalf of ASIO:
Department of Foreign Affairs and Trade relating to services overseas: $8.014m (2017: $8.029m).

2017			
Appropriation Act			
Annual appropriation[1]	402 998	28 092	14 103
PGPA Act			
Section 74	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)***	***(3838)***

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

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

	2018	2017
	$'000	$'000
3.1.B Unspent departmental annual appropriations (recoverable GST exclusive)		
Appropriation Act (No. 1) 2016–17	22	84 338
Appropriation Act (No. 1) 2017–18	70 651	-
Appropriation Act (No. 2) 2017–18	5000	-
Appropriation Act (No. 3) 2017–18	3952	-
Appropriation Act (No. 4) 2017–18	1398	-
Total	**81 023**	**84 338**

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	**972**	**2490**
Depreciation and amortisation	(89 365)	(88 335)
Deficit as per statement of comprehensive income	(88 393)	(85 845)

4. Managing uncertainties

4.1 CONTINGENT ASSETS AND LIABILITIES

Quantifiable contingencies

ASIO's contingent liabilities relate to claims for damages or costs. The amount represents an estimate of ASIO's liability based on precedent in such cases. ASIO is defending the claims.

Contingent liabilities

Balance from previous period	-	150
New contingent liabilities recognised	60	-
Obligations expired	-	(150)
Total contingent liabilities	**60**	-

Unquantifiable contingencies

At 30 June 2018, 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.

	2018 $'000	2017 $'000
4.2 FINANCIAL INSTRUMENTS		
4.2.A Categories of financial instruments		
Financial assets		
Loans and receivables		
Cash	23 552	17 338
Trade receivables	7615	4753
Accrued revenue	753	1644
Total financial assets	**31 920**	**23 735**
Financial liabilities		
At amortised cost		
Trade creditors and accruals	8829	11 865
Total financial liabilities	**8829**	**11 865**

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.

The only net gain or loss from financial assets or liabilities through profit or loss for the period ending 30 June 2018 was the impairment of Trade Receivables.

6

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

	2018	2017
	$'000	$'000

5.1 KEY MANAGEMENT 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	**1593**	1606
Long-term employee benefits	**189**	189
Post-employment benefits	**276**	264
Total key management personnel remuneration expenses[1]	**2058**	**2059**

The number of key management positions is 5. (2017: 5)

Several key management positions were occupied by different officers for portions of the year.

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.

All related party transactions with Key Management Personnel during 2017–18 were in the ordinary course of business and do not require separate disclosure.

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 $22.09m in 2017–18.

5.3 MAJOR BUDGET VARIANCES

The nature and timing of the Commonwealth's budget process meant the original Budget in the 2017–18 Portfolio Budget Statements was published in May before the closing 2016–17 and opening 2017–18 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 2017–18 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 2017–18 consistent with the requirement under the Commonwealth budgeting framework. Variances between the 2017–18 operating result 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 $13.3m. The overall increase in expenses can be attributed to:

- Average Staffing Level for the year was higher than budgeted due to the late Full Time Equivalent growth in 2016–17, resulting in higher than the budgeted employee expenses. There were also unbudgeted redundancies totalling $0.3m.
- supplier expenses were higher than anticipated in the original Budget due to a review of ASIO's technology state and processes and subsequent business reform planning.
- measures approved through additional estimates also contributed to additional expenditure.
- the depreciation increase of $4.7m resulted from higher than anticipated capital purchases and the increase in asset fair value due to the revaluation.

Departmental revenue

The total increase in departmental revenue from the original Budget estimate is $9.6m and can be attributed to:

- own-source revenue increase of $5.6m relates to rental income for the Australian Cyber Security Centre (ACSC) not being included in the orginal Budget as the timing of their move from the Ben Chifley Building was uncertain. Revenue relating to the ACSC was recognised over a faster period than anticipated in the budget as the sub-lessee indicated they would be terminating the lease.
- revenue from Government increase of $4.0m relates to measures approved through additional estimates.
- revenue from sale of goods and services was $2.7m less than budget, this budget is difficult to predict as it is dependent on requests and activities undertaken by external parties.

Departmental assets

Total departmental assets are $38.7m higher than the original Budget position. The overall increase can be attributed to:

- the variance for financial assets is $12.0m above the Budget estimate mostly as a result of the inter-relationship with departmental expenses and revenue. More funds were also drawn in June than required. These funds will be available in 2018–19.
- non-financial assets are higher by $26.7m. ASIO undertook a revaluation in 2017–18 resulting in an overall increase in fair value, in particular movements in Land and Buildings (increase of $23.0m) and Property, Plant and Equipment (increase of $14.9m). These movements were not included in the budget due to the nature and uncertainty of the activity.
- software purchases were higher than anticipated and Property, Plant and Equipment purchases were lower than anticipated. These purchases were part of an asset replacement program in 2017–18 of which the detailed category split was not known at the time of estimating the budget.
- the timing and increase in the number of prepayments has contributed to the balance being above budget.
- measures approved through additional estimates have also contributed to the increase in asset balances from budget.

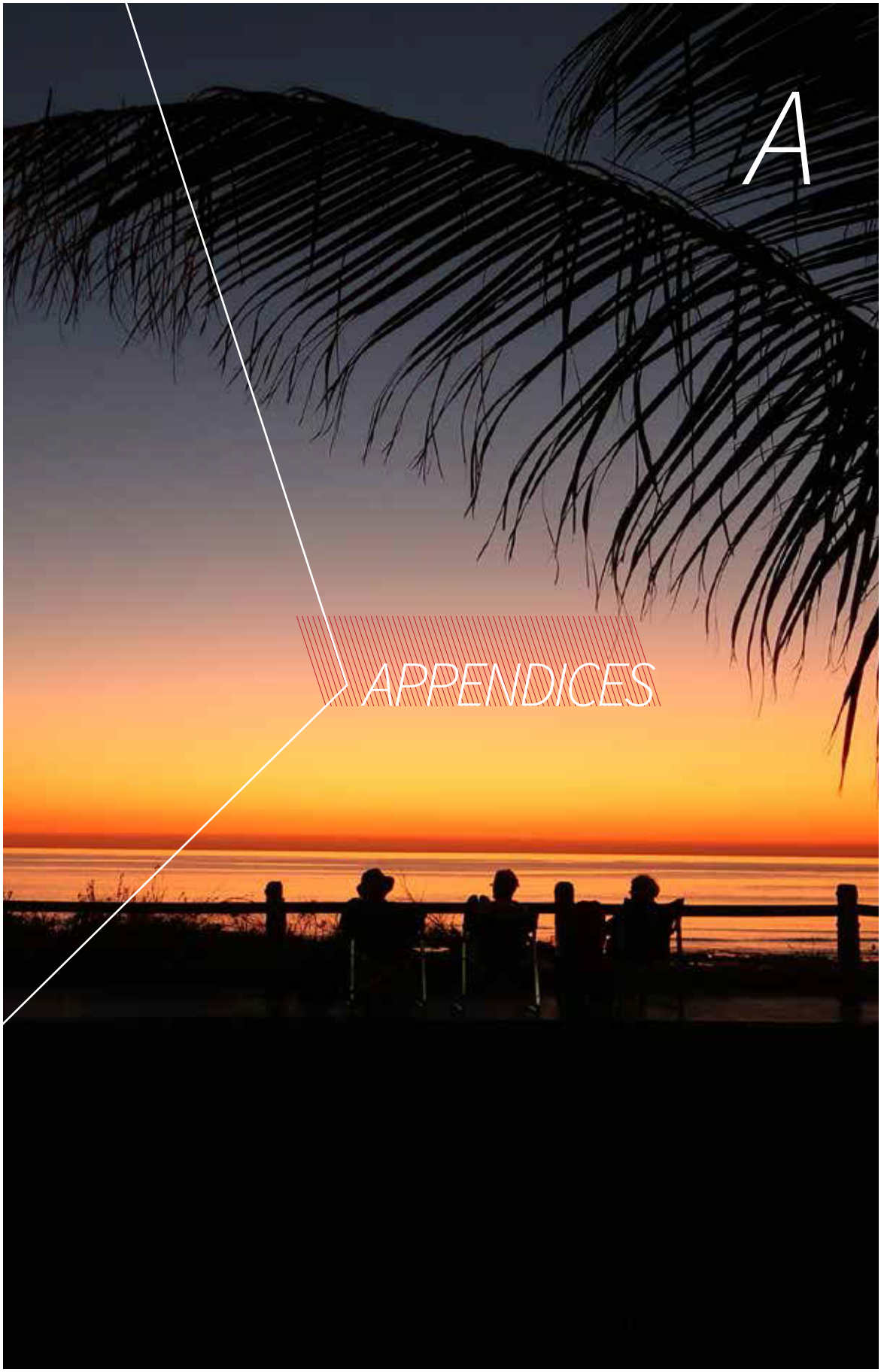
Departmental liabilities

Total departmental liabilities are $12.8m more than the original Budget position. Variances within the result include:

- higher employee provisions due to unanticipated growth of the employee base in late 2016–17.
- increase to provisions for rent amortisation due to stage of leases. Potential changes were not factored into the original Budget.
- increase to provision for restoration obligations due to the revaluation conducted in 2017–18.

Statement of Cash Flows and Statement of Changes in Equity

The amounts reported in the Statement of Cash Flows and the Statement of Changes in Equity are inter-related with figures disclosed in the Statement of Comprehensive Income and Statement of Financial Position. Consequently, variances in these Statements 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 2017–18 $'000	Payments made 2017–18 $'000	Balance remaining 2017–18 $'000
ORDINARY ANNUAL SERVICES[1]			
Departmental appropriation			
Prior year appropriation[2]	67 000	67 000	-
2017–18 appropriation	421 767*	390 000	31 767
Section 74 relevant agency receipts[3]	30 176	25 892	4284
2017–18 capital budget	68 575*	53 575	15 000
Cash on hand	17 338	(6214)	23 552
Total ordinary annual services	***604 856***	***530 253***	***74 603***
OTHER SERVICES			
Departmental non-operating[4]			
Equity injections	14 939*	8541	6398
Total other services	***14 939***	***8541***	***6398***
TOTAL NET RESOURCING AND PAYMENTS FOR ASIO	**619 795**	**538 794**	

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

[2] Includes an amount of $5.0m from 2016–17 for the Departmental Capital Budget. For accounting purposes this amount has been designated as 'contributions by owners'.

[3] $22.795m per Portfolio Budget Statement plus $7.381m underestimate at time of PBS.

[4] 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* 2017–18 $'000	Actual Expenses 2017–18 $'000	Variation 2017–18 $'000
Program 1.1: Security Intelligence			
Departmental expenses			
Appropriation[1]	421 767	421 767	(0)
Expenses not requiring appropriation in the Budget year	84 126	89 515	(5389)
Total for Program 1.1	***505 893***	***511 282***	***(5389)***
Total expenses for Outcome 1	**505 893**	**511 282**	**(5389)**

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

[1] Ordinary annual services (Appropriation Act Nos 1 and 3) including reductions under section 51 of the PGPA Act and Retained Revenue Receipts under section 74 of the PGPA Act 2013.

A

Appendix C: workforce statistics

Full-time equivalent actual

2016–17	**1794.3**
2017–18	**1814.9**

Head count of staff by load and employment status

	2016–17			2017–18		
	Ongoing	**Non-ongoing**	**Total**	**Ongoing**	**Non-ongoing**	**Total**
Full-time	1611	12	**1623**	1640	10	**1650**
Part-time	240	18	**258**	260	21	**281**
Casual	N/A	50	**50**	N/A	49	**49**
Total	**1851**	**80**	**1931**	**1900**	**80**	**1980**

Notes:
• 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

	2016–17				2017–18			
	Ongoing	**Non-ongoing**	**Casual**	**Total**	**Ongoing**	**Non-ongoing**	**Casual**	**Total**
Female	844	10	14	**868**	882	8	12	**902**
Male	1007	20	36	**1063**	1018	23	37	**1078**
Total	**1851**	**30**	**50**	**1931**	**1900**	**31**	**49**	**1980**

Notes:
• 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

		2016–17				2017–18			
		Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Senior Executive Service	Director-General	1	0	0	**1**	1	0	0	**1**
	SES Band 3	2	0	0	**2**	4	0	0	**4**
	SES Band 2	11	0	2	**13**	12	0	3	**15**
	SES Band 1	34	2	1	**37**	37	2	1	**40**
Senior officers	AEE2/3	175	3	1	**179**	187	5	1	**193**
	AEE1	365	3	3	**371**	407	5	3	**415**
Employees	AE1 to AE6 (including technical specialists)	1263	22	43	**1328**	1252	19	41	**1312**
Total		**1851**	**30**	**50**	**1931**	**1900**	**31**	**49**	**1980**

Notes:
• 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

	2016–17				2017–18			
	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Canberra-based	1320	18	37	**1375**	1358	23	36	**1417**
Other locations	531	12	13	**556**	542	8	13	**563**
Total	**1851**	**30**	**50**	**1931**	**1900**	**31**	**49**	**1980**

Notes:
• 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

	2016–17		2017–18	
Available data	1805	93.5%	1862	94.0%
Identify as Indigenous	12	0.7%	10	0.5%
People with a disability	19	1.1%	20	1.1%
Non-English-speaking background	324	18.0%	333	17.9%

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	$324 136 minimum point
SES Band 2	$252 195 minimum point
SES Band 1	$201 756 minimum point
Senior employees	
AEE3	$155 230
AEE2	$131 172–155 230
AEE1	$114 445–127 893
Employees	
AE6	$90 042–101 459
AE5	$81 464–87 451
AE4	$74 229–79 658
AE3	$65 650–71 746
AE2	$57 749–63 952
AE1	$49 837–55 352
Intelligence employees	
IE	$90 042–101 459
IE trainees	$81 464–95 912
Information technology employees	
SITEA	$155 230
SITEB	$131 172–155 230
SITEC	$114 445–127 893
ITE2	$90 042–101 459
ITE1	$78 421–86 215
Engineers	
SIE(E)5	$155 230
SIE(E)4	$131 172–155 230
SIE(E)3	$114 445–127 893
SIE(E)2	$90 042–101 459
SIE(E)1	$78 421–86 215

Notes: Figures at 30 June 2018. 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 Home Affairs on 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 ASIO material that ASIO relied on 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 their time in detention.

There were no matters falling within the Independent Reviewer's terms of reference on 1 July 2017, and no new matters were referred to the Independent Reviewer during the year.

The Independent Reviewer's appointment is due to expire on 1 September 2018. Go to www.ag.gov.au/asareview for more information.

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 warrants and question and detention warrants during this reporting period. The details are provided in the following table.

Subsection	Description	2016–17	2017–18
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 during this reporting period	0	0
94(1)(b)	The total number of warrants issued under that division during this reporting period	0	0
94(1)(c)	The total number of warrants issued under section 34E during this reporting period	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, during this reporting period	0	0
94(1)(e)	The total number of warrants issued under section 34G during this reporting period	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 during this reporting period	0	0
94(1)(f)(ii)	The number of hours each person spent in detention under such a warrant during this reporting period	0	0
94(1)(f)(iii)	The total of all those hours for all those persons during this reporting period	0	0
94(1)(g)	The number of times each prescribed authority had persons appear for questioning before them under warrants issued during this reporting period	0	0

List of annual report requirements under schedule 2 of the Public Governance, Performance and Accountability Rule

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

PGPA Rule reference	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 of 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 an 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

PGPA Rule reference	Description	Requirement	Part of this report
17AE(1)(b)	An outline of the structure of the portfolio of the entity.	Mandatory for portfolio departments	N/A
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 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	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 PGPA Act that relates to non-compliance with finance law and action taken to remedy non-compliance	If applicable, mandatory	N/A
	External scrutiny		
17AG(3)	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny	Mandatory	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 during the period	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
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

PGPA Rule reference	Description	Requirement	Part of this report
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
	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

PGPA Rule reference	Description	Requirement	Part of this report
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
	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	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
Statement on questioning warrants and questioning and detention warrants	Appendix F
Statement on special intelligence operations authorities	Appendix G
Statement on authorisations for telecommunications data	Appendix H

To comply with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance, Performance and Accountability Act 2013*, Appendices G and H have been deleted from the version of the annual report tabled in parliament to avoid prejudice to ASIO's activities.

Correction of errors in 2016–17 annual report

Our 2016–17 annual report stated that there were 1751 people with available EEO data and nine people with a disability in 2016–17. The correct figures are 1750 and 19 respectively.

A

Abbreviations and short forms

A

AASB—Australian Accounting Standards Board

AAT—Administrative Appeals Tribunal

ABF—Australian Border Force

ACSC—Australian Cyber Security Centre

AE—ASIO employee

AEE—ASIO executive employee

AGSVA—Australian Government Security Vetting Agency

AIC—Australian Intelligence Community

ANZCTC—Australia–New Zealand Counter-Terrorism Committee

ASEAN—Association of Southeast Asian Nations

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

CSS—Commonwealth Superannuation Scheme

D

DCB—Departmental Capital Budget

DIBP—Department of Immigration and Border Protection

E

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

F

FIRB—Foreign Investment Review Board

FOI Act—Freedom of Information Act

FRR—Public Governance, Performance and Accountability (Financial Reporting) Rule 2015

G

GC18—Gold Coast 2018 Commonwealth Games

GRU—former Russian military intelligence agency

GST—Goods and services tax

H

HSR—ASIO's Health and Safety Representative network

I

ICT—information and communications technology

IE—intelligence employees

IGIS—Inspector-General of Intelligence and Security

INSLM—Independent National Security Legislation Monitor

IS-EA—Islamic State—East Asia

ISIL—Islamic State of Iraq and the Levant

ITE—information technology employee

J

JAD—Jemaah Anshorut Daulah

JCTT—Joint Counter Terrorism Team

JMB—Jama'at Mujahideen Bangladesh

M

N

NCFIC—National Counter Foreign Interference Coordinator

NTAC—National Threat Assessment Centre

NV1—Negative Vetting 1 security clearance

NV2—Negative Vetting 2 security clearance

A

O

ONI—Office of National Intelligence

P

PBS—Portfolio Budget Statement

PGPA—Public Governance, Performance and Accountability

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

PJCIS—Parliamentary Joint Committee on Intelligence and Security

PSS—Public Sector Superannuation Scheme

PSSap—Public Sector Superannuation Scheme accumulation plan

PV—Top Secret 'positive vetting' security clearance

S

SCEC—Security Construction and Equipment Committee

SES—senior executive service

SIE(E)—specialist intelligence employee (engineer)

SITE—senior information technology employee

SME—small and medium enterprises

STEM—Science, Technology, Engineering and Mathematics

T

TS—Top Secret

TS(PV)—Top Secret 'positive vetting' security clearance

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 the refusal of a visa or cancellation of a passport.

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

Contact Reporting Scheme—The Contact Reporting Scheme is a whole-of-government counter-espionage strategy managed by ASIO as part of the Commonwealth Government Protective Security Policy Framework (PSPF), and is one of a number of mechanisms designed to protect privileged information. The scheme not only facilitates assessment of foreign intelligence collection interests, but also protects Australian Government staff when in contact with foreign nationals of potential security interest.

foreign interference—activities relating to Australia that are conducted 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 conducted for intelligence purposes;
- are conducted for the purpose of affecting political or governmental processes; or
- are otherwise detrimental to the interests of Australia.

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

extremism—any ideology or world view that is advanced through the use of violence and that is relevant to Australia's security.

extremist—an extremist is an individual who or group that is or has been involved in violent activities relevant to Australia's security.

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

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

ideology—the set of beliefs, ideas and ideals characteristic of a social group or individual, or forming the basis of an economic or political theory.

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.

Islamism—a political ideology that holds that Islam provides a complete and self-contained social, political, religious and legal system that should be implemented in existing Muslim societies.

Islamist—a person who believes in Islamism.

Islamist extremist—a person who uses violence or advocates the use of violence in the pursuit of extreme Islamist objectives.

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

lone actors—an individual 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 breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.

non-prejudicial assessment—an assessment where ASIO does not have security concerns about the proposed action.

Operation Silves—the July 2017 disruption of a plot to use an improvised explosive device against an Etihad flight departing Sydney and a potential plot to use toxic gas in a terrorist attack.

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 and that is relevant to Australia's security; violent extremism is unlawful.

violent extremist—an extremist who or group that is, or has been, involved in violent activities relevant to Australia's security.

Zone 5 facilities—Zone 5 areas are used for the storage, handling, processing or discussion of information classified TOP SECRET; codeword information; or large quantities of other information where the compromise, loss of integrity or unavailability of the aggregate of the information would have a catastrophic business impact. Some Zone 5 areas are also accredited by the Australian Signals Directorate as a Sensitive Compartmented Information Facility.

Index

2018 annual stakeholder survey 5, 51

A

Aboriginal and Torres Strait Islander employees 69

academic outreach program 47

access to security controlled places 45

access to security-sensitive chemicals, biological agents and nuclear sites 45

accountability 13, 55, 60, 61, 62, 116

accreditation 4, 35, 42, 45, 46

acts of foreign interference 25, 38, 43

A digital transformation of the Australian Security Intelligence Organisation 4, 57

Administrative Appeals Tribunal (AAT) 64

adverse security assessments 64, 65

advertising 75, 120

Afghanistan 24

Africa 4, 23, 24

al-Qa'ida 23

al-Qa'ida-aligned groups 23

al-Qa'ida in the Arabian Peninsula 23

al-Qa'ida in the Indian Subcontinent 24

annual report ii, iii, iv, v, 5, 62, 63, 64, 114, 115, 119, 120, 121, 122

ANZCTC Crowded Places Advisory Group 50

APS Statistical Bulletin 71

ASEAN–Australia Summit 4

ASIO2020 57, 59

ASIO Diversity and Inclusion Committee 59

ASIO employees 64, 111

ASIO Ombudsman 72

ASIO's corporate plan 5, 51

ASIO's Enterprise Transformation 57, 60, 67

ASIO's purpose 11, 32

ASIO's T4 Protective Security Directorate (ASIO-T4) 48, 49, 50

ASIO-T4 reports 49

Association of Southeast Asian Nations 4, 46

attacks on the London and Westminster bridges 19

Attorney-General 4, 38, 45, 61, 62

Attorney-General's Department 36

Attorney-General's Guidelines 61

Attorney-General's portfolio 4

Audit and Risk Committee 60, 74

AusTender 74, 119

Australia-based Islamist extremists 22

Australian Defence Force 40

Australian Defence Industry Security Assurance Review 40

Australian Embassy 24

Australia–New Zealand Counter Terrorism Committee (ANZCTC) 50

Australian Federal Police 50, 73

Australian Government 88, 97, 101, 119

Australian Government Security Vetting Agency 41

Australian Public Service 71, 117, 118

Australian Security Intelligence Organisation Act 1979 4, 11, 25, 42, 61, 62, 71, 114, 121

Australians who had been kidnapped overseas 36

Australia Special Summit 46

Australia's ports 44

Australia's security environment 17, 19

aviation 4, 21, 34, 35, 37, 44

Aviation Security Identity Cards 45

B

Bangladesh 24, 33

Belgium 24

Ben Chifley Building 73, 102

border integrity 11, 32, 44, 45, 46

border security 4, 44, 45, 46

budget 5, 53, 57, 59, 88, 98, 99, 101, 102, 107

Business and Government Liaison Unit (BGLU) 36, 47, 48, 49

C

Capability Committee 59

Centre for Defence Industry Capability 48

chemical dispersal weapon 37

citizenship applications 45

classified briefings 62

clearances 41, 52, 64

Code of Conduct 72

Comcare 64, 71

Commonwealth Disability Strategy 71

Commonwealth Fraud Control Framework 60

Commonwealth Procurement Rules 74, 75, 118

communal violence 22

compensation 71, 91

Comprehensive Review into the Legal Framework of the National Intelligence Community 5

consultancy contracts 74, 118

Contact Reporting Scheme 41

corporate governance 117

corporate governance committees 57, 58

counter espionage, foreign interference and malicious insiders 11, 32, 38, 40, 42

counter terrorism 11, 32, 33, 35

counter-terrorism assessments 33

counter-terrorism disruptions 35

Criminal Code 4, 33, 37, 38, 62

Criminal Code Act 1995 4, 37

critical infrastructure 25, 28, 39, 48, 49

cross-cultural communication 69

crowded places 19, 24, 33, 47, 50

cultural awareness 69

cyber actors 25

cyber espionage 25

cyber intrusions 25

D

declared area 33

defence 28, 40, 47, 48, 49

defence industry 40, 47, 48, 49

Departmental Capital Budget (DCB) 53

Department of Defence 40

Department of Finance 74, 97, 101, 119, 120

Department of Foreign Affairs and Trade 33, 36, 98

Department of Home Affairs 4, 5, 38, 44, 45, 46, 61, 62, 64, 65, 113

disability 71

disruption 4, 19, 24, 33, 34, 35, 37, 46

diversity and inclusion 57, 59, 68, 69

Diversity and Inclusion Strategy 2018–20 68

Diversity Council of Australia 69

diversity networks 69

E

East Africa 24

e-Learning 60, 67

Embassy of the Russian Federation in Canberra 42

employees 64, 67, 69, 72, 97, 109, 110, 111, 112, 117, 118

energy and resources sector 47

equity 87, 88, 89, 99

espionage 3, 5, 6, 11, 25, 28, 32, 38, 39, 40, 41, 42, 43, 49, 51

Europe 24

Executive Board 57, 58, 59, 60, 101

external scrutiny 117

extreme left- or right-wing ideology 19

F

federal and state governments 34, 36, 40, 51

Federal Court of Australia 65

financial statements 79, 81, 90, 97, 119

first aid officers 71

flexible working arrangements 69

foreign actors 3

foreign fighters 22, 23, 33, 37, 46

Foreign Influence Transparency Scheme 3, 28, 62

foreign intelligence collection 5, 42

foreign intelligence services 25, 40, 43

foreign interference 3, 4, 5, 6, 11, 25, 28, 32, 38, 39, 40, 41, 42, 43, 51

foreign investment 25, 39

Foreign Investment Review Board 39

foreign powers 25, 39

foreign security and intelligence partners 34

foreign states 25, 41

France 24

Fraud Risk Assessment and Fraud Control Framework 2016–18 60

G

gender equality 69

Germany 24

Global Summit of Woman 69

Gold Coast 2018 Commonwealth Games (GC18) 4, 35, 36, 46

governance 57, 58, 62, 71, 116, 117

graduate programs 66

H

Haqqani Network 24

High Court of Australia 65

Home Affairs portfolio 4

human rights 63

I

immigration detention 64, 65, 113

improvised explosive device 4, 33, 37

Independent National Security Legislation Monitor's (INSLM) 63

Independent Reviewer of Adverse Security Assessments 64, 113

India 24

Indigenous 111, 117

Indonesia 4, 23

industry 4, 5, 6, 11, 25, 32, 36, 37, 40, 47, 48, 49, 51

inquiries 62

inquiry 62, 63

Inspector-General of Intelligence and Security (IGIS) 63

intelligence and security reports 34

Intelligence Committee 59

intelligence priorities 35

international liaison arrangements 34

ISIL-affiliated or -aligned groups and individuals 23

ISIL's caliphate 22, 46

ISIL-Yemen 23

Islamic State—East Asia (IS-EA) 4, 33, 36, 37, 124

Islamic State—Khorasan Province 24

Islamic State of Iraq and the Levant (ISIL) 4, 19, 22, 23, 24, 37, 46, 65

Islamist extremists 19, 22, 24, 37

A

J

Jama'at Mujahideen Bangladesh 33

Jemaah Anshorut Daulah 33

Joint Counter Terrorism Teams 36

K

Kabul 24

key national security legislation 62

Kurdish groups 23

L

Language Skills Development Program 67

Lashkar-e-Tayyiba 24

law enforcement agencies 4, 34, 35, 36, 37, 38, 50

Leader of the Opposition 62

Leadership Charter 68

leads 35, 41

legal graduate program 66

Lewis AO, DSC, CSC, Mr Duncan 14, 31, 81

LGBTI 69

London 19, 50

M

Male Champions of Change program 69

Marawi 4, 23, 36

Maritime Security Identity Cards 45

mass passenger transportation 34

mental health and wellbeing strategy 71

Middle East 4, 23

Minister for Foreign Affairs 33

Minister for Home Affairs 61, 65

ministerial accountability 61

N

National Counter Foreign Interference Coordinator 38

National Disability Strategy 2010–20 71

National Intelligence Community 5, 35, 63

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 3

National Security Legislation Amendment (Espionage and Foreign Interference) Bill 28, 62

National security partner agencies 33, 35, 40, 45, 51

national terrorism threat level 19

National Threat Assessment Centre (NTAC) 33, 34, 37

Nice 50

O

Office of National Intelligence (ONI) 4

Office of Transport Security 44

Ombudsman 117

Operation Silves 4, 33, 34, 35, 36, 37, 44

organisational structure 13, 14, 115

oversight and accountability framework 13

P

Pakistan 24

Parliamentary Joint Committee on Intelligence and Security 38, 62, 74, 75

passports 33, 64

pathways to radicalisation 34

people-smuggling 44, 46

people with a disability 71, 72, 122

permanent protection visa 64, 113

personnel security assessments 41

Philippines 4, 23, 36

police and military targets 24

Portfolio Budget Statement 11, 32, 33, 35, 38, 40, 42, 44, 45, 47, 107, 116

pro-ISIL network 4, 23

propaganda 19, 23, 24, 36

proscription 4, 33, 36, 37

prosecution 3, 4, 35, 37, 63

protective security advice 11, 32, 47, 48, 49, 50

Public Governance, Performance and Accountability Act 2013 31, 57, 60, 81, 90, 98, 108, 116, 117, 121

public interest disclosures 72

PV clearances 41, 52

Q

qualified security assessment 43

questioning and detention warrants 62, 121

questioning warrants 62, 114, 121

R

right- and left-wing extremism 34

risk management 57, 59

Royal Australian Navy 40

Russian Federation 24, 42

Russian intelligence activity in Australia 42

Russian military intelligence 39, 42

S

salary classification structure 112

security briefings 41, 43

Security Construction and Equipment Committee (SCEC) 48

security environment 17, 19

security manager and critical infrastructure guides 49

security planning and accreditation for special events 4

Senate estimates 63

Senate Legal and Constitutional Affairs Committee 63

Senior Executive Service (SES) 67, 110, 112, 118

separation rate 66

Sergei Skripal 39, 42

shadow ministers 62

Sikh 24

small business 74, 119

Smartraveller 33

South Asia 24

South-East Asia 23, 37

Spain 24

special events accreditation 45

special intelligence operations 61, 121

special powers 62

stakeholder evaluation 34, 36, 39, 41, 44, 46, 49

state and non-state actors 25

statutory questioning and detention powers 62

Surabaya 23

surveillance 35, 67

Syria and Iraq 4, 22, 23, 33, 46

T

Taliban 24

taxation 90

terrorism 4, 5, 11, 15, 19, 20, 21, 23, 24, 32, 33, 34, 35, 36, 37, 48, 50, 51, 53, 63, 64

terrorism indicators 34

terrorism offences 21, 35

terrorist attack 4, 19, 24, 33, 35

terrorist organisation 36, 37

terrorist threat 4, 19, 22, 33, 37, 46, 47

the Hon. Peter Dutton MP 61

Thodey Review 66

Top Secret Positive Vetting 41

training 36, 37, 46, 48, 49, 50, 66, 67, 68, 69

transformation 4, 5, 52, 57, 66

Transformation Oversight Committee 57, 60

transformation program 5

Turkey 23

U

United Kingdom 19, 24, 42

universities 47

V

violent protest 22, 34

visas 45, 64

W

warrant request 62

warrants 61, 62, 114, 121

waste 74

weapons and tactics 19, 50

workforce 59, 66, 68, 69, 72, 109

Workforce Committee 59

work health and safety 71

workplace agreement 71

Y

Yemen 23

Z

Zone 5 facilities 48