Australian Government
Australian Security Intelligence Organisation

ASIO 70TH 1949 2019

ASIO Annual Report 2018–19

ISSN 0815–4562 (print)
ISSN 2204–4213 (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

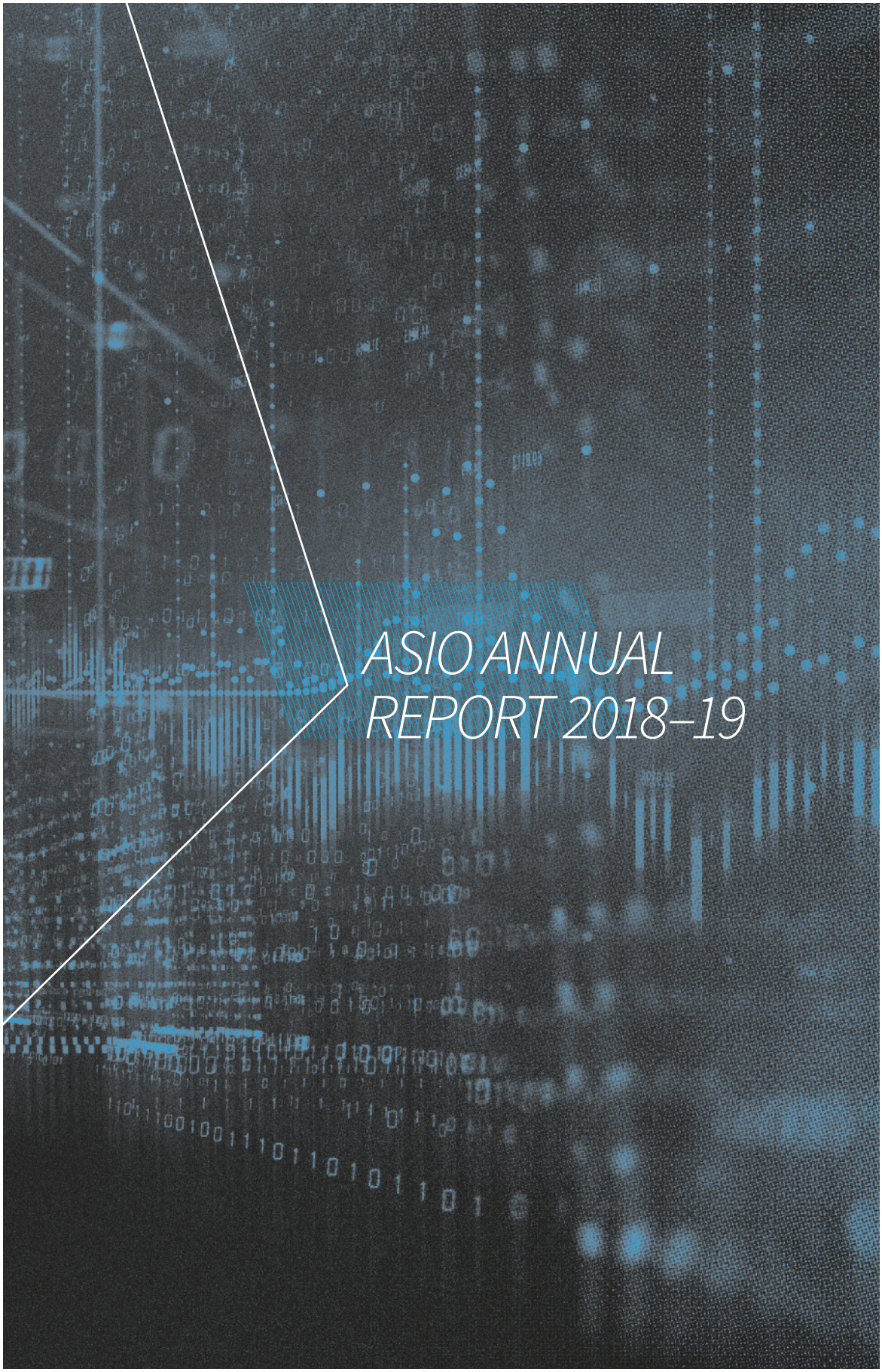
Website: www.asio.gov.au
Location of this annual report: www.asio.gov.au/asio-report-parliament

Acknowledgement of Country and Traditional Custodians

ASIO would like to acknowledge the Traditional Custodians of this land. We pay our respects to the Elders of this land, both past and present and those emerging.

Photographs

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 2018–19

ASIO Annual Report 2018–19

Australian Government

Australian Security Intelligence Organisation

Director-General of Security

14 September 2019
Ref: A16950593

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

Dear Minister,

ASIO Annual Report 2018-19

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 2018–19.

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 of the ASIO Act relating to special intelligence operations, telecommunications data access authorisations and technical assistance requests, technical assistance notices and technical capability notices 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.

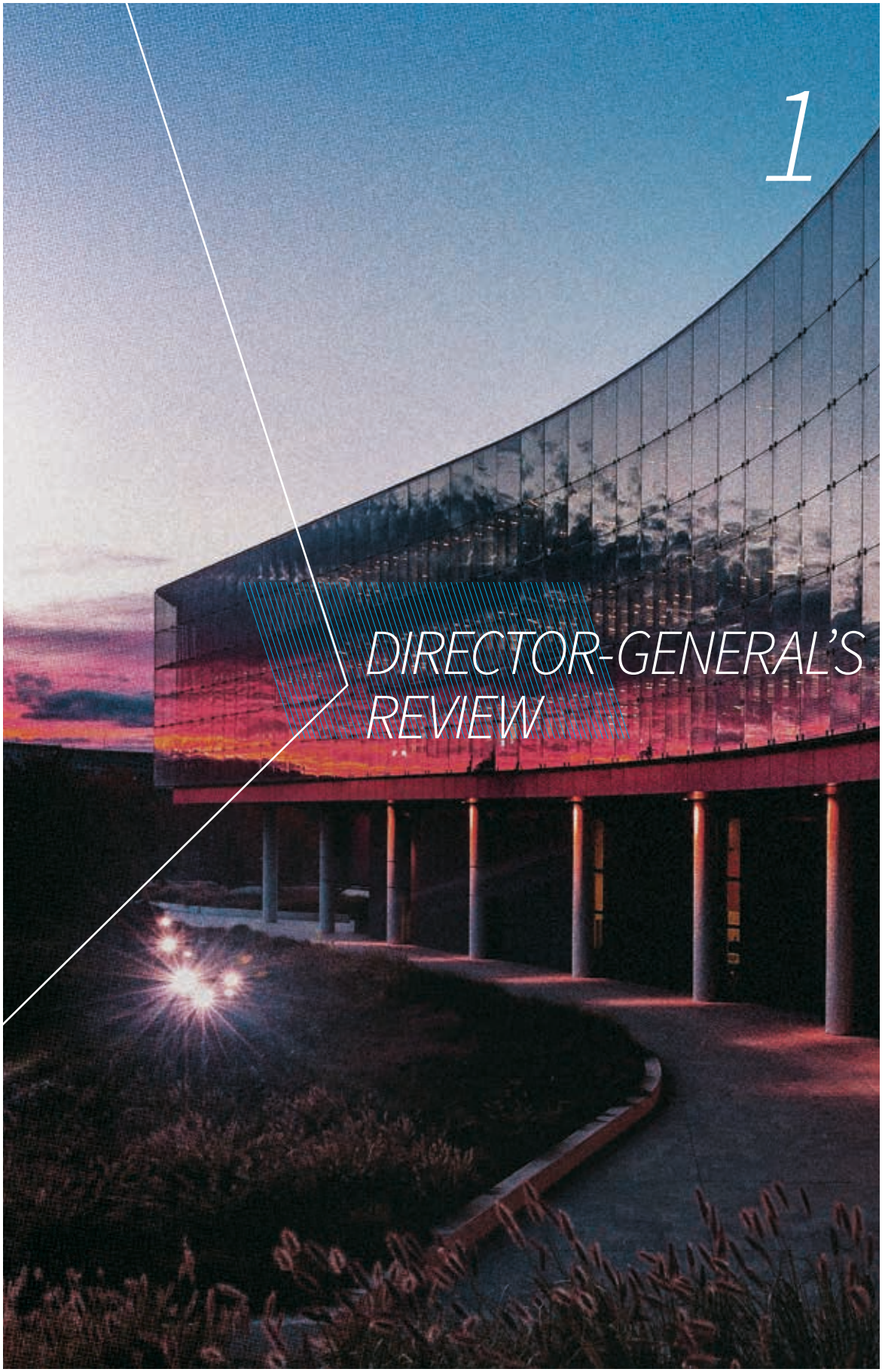
As required by subsection 17AG(2) of the PGPA Rule, I certify that fraud risk assessments and control plans have been prepared for ASIO, that we have appropriate mechanisms in place for preventing, investigating, detecting and reporting incidents of fraud, and that all reasonable measures have been taken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

Director-General's review

This year marks ASIO's 70th anniversary. Seven decades have passed since Prime Minister Ben Chifley established the Australian Security Intelligence Organisation during the earliest days of the Cold War. On 16 March 1949, ASIO commenced its work with just two employees, one being the inaugural Director-General of Security, Justice Sir Geoffrey Reed. Fast forwarding to 2019, and 13 Directors-General of Security later, ASIO has evolved into a workforce of nearly 2000 people, with officers located across Australia and the world.

The intervening years have been busy for ASIO, with each decade presenting its own unique challenges and defining moments. The Petrov Affair, the imagery and implications of which persist to the present day, was one such defining moment. Terrorist attacks such as the 1978 Sydney Hilton hotel bombing, the 9/11 attacks in the United States, and the Bali bombings were further defining moments where operational priorities dramatically changed. More recently, the challenges of international terrorism, the Islamic State of Iraq and the Levant (ISIL) and Australian foreign fighters, together with the rise in levels of espionage and foreign interference, have tested ASIO's capacity. Regardless of the decade, these events reveal the very high stakes involved in ASIO's work.

The one constant over the past 70 years has been ASIO's resolute focus on protecting Australia from those who wish us harm. This year has been no different—another year of high operational tempo, another year where ASIO has again been at the forefront of confronting Australia's national security challenges.

Security challenges

To say that we have had good operational success this year is not to say the job is done. The world in which we live is becoming ever more complex, more uncertain and, as a result of globalisation, more 'connected' than at any other time in history. The threats of terrorism, espionage and foreign interference recognise no borders. They are persistent,

and their enduring nature means we cannot afford to rest on our successes. ASIO works every day to meet these security threats while preparing for the security challenges of the future.

Terrorism

Shifts in the world order continue to unleash forces of change that will be with us for generations. One result is the terrorist threat to Australia has become real and dangerous. This is why our national threat level remains elevated. Readily available weaponry, fueled by malicious intent and inspired, encouraged or directed by like-minded networks overseas, means that Australia-based extremists retain the intent and capability to conduct attacks on Australian soil.

ISIL's 'caliphate' has been crushed and it has lost its safe havens and organised military capability. Remnants of ISIL, however, remain dangerous and will require ongoing attention. Our domestic terrorist threat environment has not significantly improved following the collapse of ISIL. In fact, the threat from home-grown terrorism, coupled with the anticipated attempts by some terrorist fighters to return to Australia, remains a matter of the gravest security concern.

We must now consider those who have travelled to overseas conflict zones and wish to return to Australia. They may take months or even years to return. Those who do will present a longer-term threat, as travellers to the Soviet Afghan war did in decades past.

The recent tragic events in Christchurch, New Zealand, earlier this year have brought the right-wing extremist threat back into focus. This threat is not something new, but current extreme right-wing networks are better organised and more sophisticated than those of the past. Regardless of the different vectors and threats, ASIO's role in countering terrorism is far from over. At the time of publication, ASIO together with our law enforcement partners have thwarted 16 attacks in the past five years. To date, 93 people have been convicted of terrorism by Australian courts.

Countering espionage and foreign interference

While ASIO's adversaries may have changed over the past 70 years, the challenges they pose have not. Australia remains a target for acts of espionage and interference by foreign states, who continue to target the government, academia and industry for access to sensitive and valuable information. These acts, which occur on a daily basis, are of unprecedented scale and sophistication. The threat to Australia from foreign states seeking to obtain strategic advantage at our expense cannot be understated.

Ironically, the very technologies that have enabled rapid globalisation are the same technologies that facilitate foreign espionage and interference. Modern, instantaneous broadband communication provides a great vector for cyber intrusions and attacks and facilitates foreign interference in ways not possible in the past.

Partnerships

We live in an increasingly uncertain world, challenged by complex security issues that no agency can manage in isolation. We draw great benefit from working with our long-term partners, who are also grappling with the threat posed by terrorists and foreign powers. Building on these partnerships, we have prevented the flow of foreign fighters into conflict zones, strengthened intelligence-sharing relationships, and increased collaboration on the challenges of foreign interference.

Home Affairs portfolio

After 70 years in the Attorney-General's portfolio, ASIO moved into the Home Affairs portfolio on 11 May 2018. Such significant administrative and corporate changes naturally create challenges but also opportunities, and ASIO has been fully engaged in the implementation process. The changes have not affected our functions or statutory independence, and have delivered the expected strengthened levels of cross-agency cooperation. We have worked diligently to integrate ourselves and others into our new portfolio and deliver the efficiencies, coordination and results-driven change the Australian Government expects.

Meeting our challenges

Technological breakthroughs—and the use of these advances by those intent on causing harm to Australia—continue at an extraordinary pace and are being increasingly disruptive to our operating environment. ASIO is moving with this wave of technological change to harness new capabilities and develop protections against capabilities that are used against us. Through a major enterprise transformation project, we are positioning ourselves to be at the forefront of agencies utilising artificial intelligence and machine-learning to do business at machine speed in an age of 'big data'.

Legislative change

The passage of the *Telecommunications and Other Legislation Amendment Act 2018* by parliament on 6 December 2018 represented an important response to these technological challenges. The Act is designed to allow agencies to lawfully access communications and data through a range of measures, including enhanced obligations for industry to assist agencies in prescribed circumstances. The amendments recognise that ASIO and our partners must pursue smarter, more sustainable strategies to counter our adversaries, and that we must take the long view of the challenges confronting us.

Enterprise transformation

In 2018 ASIO commenced a significant Enterprise Transformation Program to implement the recommendations of David Thodey AO's 2017 report *A digital transformation of the Australian Security Intelligence Organisation*. This program positions ASIO to take advantage of modern data and technology platforms and equip us with the tools to better respond to changes in our complex security and technology environments.

During the reporting period, ASIO has taken critical steps in the foundational stages of our enterprise transformation. For example, ASIO has approached the open market for the first time to engage with new technology partners, ensuring

we are on the cutting edge of digital and technological innovation. We have also established a portfolio management capability to optimise allocation of our resources and investments across the enterprise, and have developed a new operating model to ensure our functions continue to work seamlessly together to deliver security intelligence outcomes. We are embedding an innovation ecosystem in our operating model and portfolio management, and introducing contemporary ways of working to support ASIO's future as an agile, digitally enabled Organisation.

The roadmap for our enterprise transformation is the ASIO Strategy 2018–23. Launched in October 2018, the strategy sets the direction to realise our vision of delivering trusted intelligence to secure Australia. It works to leverage our unique expertise and capabilities to shape Australia's security environment and foster institutional resilience to current and future threats.

Performance

We achieved six of the eight performance objectives outlined in our 2018–19 corporate plan. This assessment was confirmed by the findings of our 2019 Stakeholder Survey, which indicate ASIO performed effectively during this reporting period in challenging circumstances. The survey was conducted by an independent reviewer, who sought views on our performance from 74 key interlocutors across government and industry. The survey found ASIO was achieving its purpose, and our advice continues to be highly regarded and in high demand. Importantly, stakeholders commented positively on our willingness to collaborate and to engage with a wider range of stakeholders within government and industry.

Nevertheless, our challenges are significant and we cannot assume they will take care of themselves. Our stakeholders say we need to continue to experiment with bold new ideas, and to be even more agile, pragmatic in our advice and open to experimentation and collaboration.

We partially achieved two of the eight strategic performance objectives set out in our corporate plan for 2018–19. These both fall within our countering espionage, foreign interference, sabotage and malicious insiders key activity. While our work in these areas is well regarded, the higher level of espionage and foreign interference threat—combined with greater awareness among our stakeholders of that threat—has increased demand for our advice and support, which is stretching current resources. With the terrorist threat showing no signs of significantly decreasing, ASIO has limited scope to redirect internal resources to address the increasing gap between demand for our counter–espionage and foreign interference advice and our ability to furnish this assistance.

Our annual performance statement, contained in Part 4 of this report, provides further information on our performance during 2018–19 and the continued value of our work to our national security partners. In relation to our financial performance, the operating environment in 2018–19 continued to be challenging, resulting in ongoing pressure on our resources and sustainability. We continue to review the sustainability of our current operations in light of anticipated future pressures on our operating environment and departmental capital budgets.

Outlook

The forecast for Australia's security environment is for only more complex challenges and more uncertainty. We expect this will fuel further demand for our advice among our expanding government and private sector stakeholder cohort, while our core business of investigating security threats continues on its own trajectory. ASIO will need to build new capability and capacity to meet current and future demand for our trusted advice and expertise.

In the coming years, as Australia's security environment presents new challenges, we will necessarily prioritise our finite resources—across our counter-terrorism, counter–espionage and foreign interference, border integrity and protective security advice programs—towards addressing activities of the greatest potential harm to Australians and Australian interests.

Continuing the journey commenced by our predecessors, ASIO's people will keep on doing their remarkable work, with integrity and propriety.

As the Australian Government determined 70 years ago, ASIO's ultimate duty remains to secure the nation and keep its people safe. There is no higher priority.

Duncan Lewis AO DSC CSC
Director-General of Security

ASIO at a glance 2018–19

12 478
Counter-terrorism (CT) leads resolved or investigated

11 669
Visa security assessments

32 887
Personnel security assessments

97%
Business and Government Liaison Unit (BGLU) briefing day satisfaction rate

3
Disruptions of planned terrorist attacks

81
Zone 5 site inspections and reports

983
Published CT intelligence and security reports

269
Published counter–espionage and foreign interference intelligence and security products

275
Foreign Investment Review Board assessments

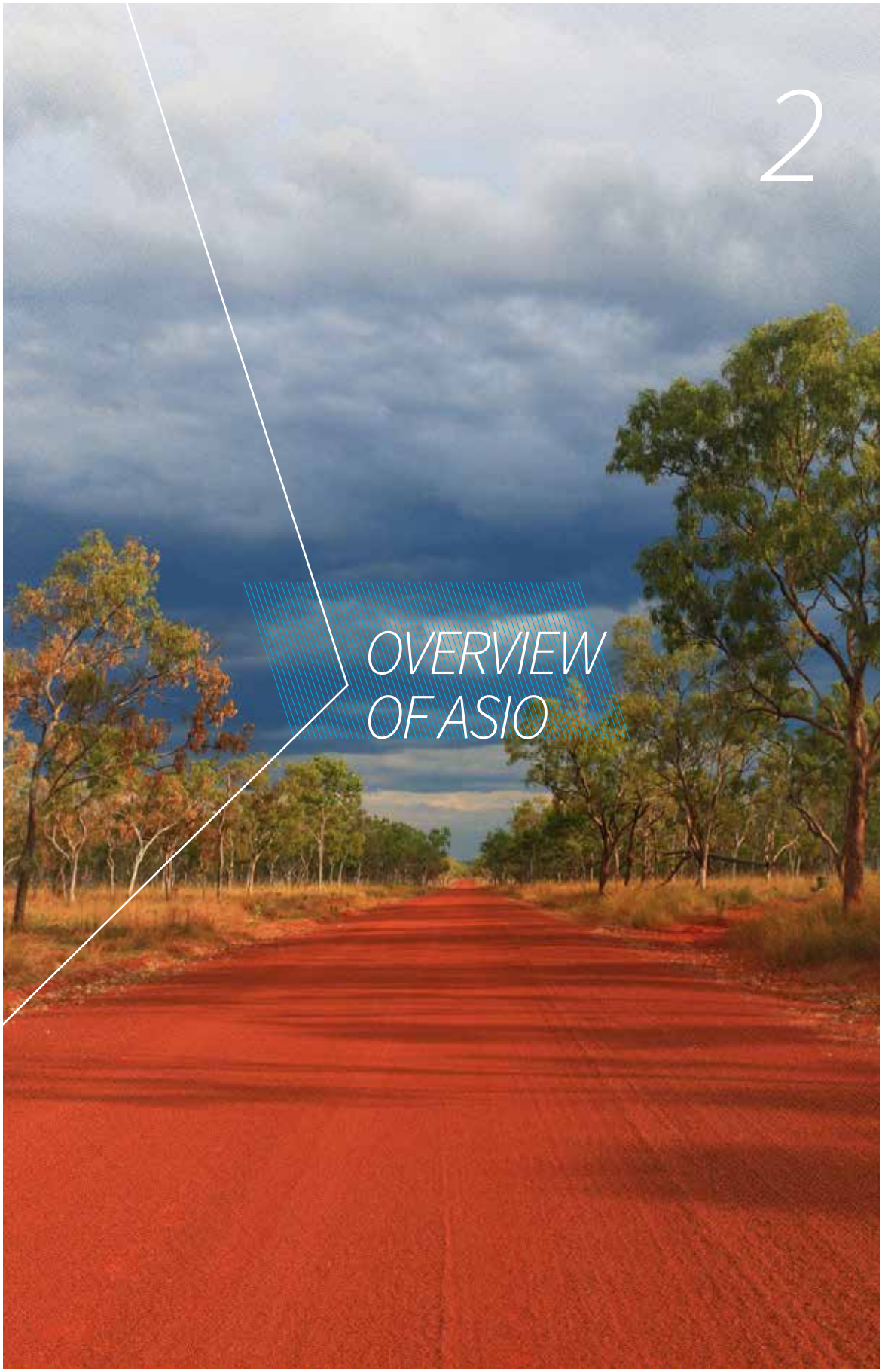
4480
Subscribers to the BGLU website

87
Security products evaluated

145 114
Security assessments for access to sensitive sites and materials

$547.418m
Budget

1961
Total employees



2

OVERVIEW OF ASIO

2

Overview of ASIO

ASIO's purpose is to protect Australia, its people and its interests from threats to security.[1] Our functions are set out in section 17 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), which states:

1. The functions of the Organisation are:

   a. to obtain, correlate and evaluate intelligence relevant to security;

   b. for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;

   c. to advise Ministers and authorities of the Commonwealth in respect of matters relating to security, in so far as those matters are relevant to their functions and responsibilities;

   ca. to furnish security assessments to a State or an authority of a State in accordance with paragraph 40(1) b);

   d. to advise Ministers, authorities of the Commonwealth and such other persons as the Minister, by notice in writing given to the Director-General, determines on matters relating to protective security; and

   e. to obtain within Australia foreign intelligence pursuant to section 27A or 27B of this Act or section 11A, 11B or 11C of the *Telecommunications (Interception and Access) Act 1979*, and to communicate any such intelligence in accordance with this Act or the *Telecommunications (Interception and Access) Act 1979*; and

   f. to co-operate with and assist bodies referred to in section 19A [of the ASIO Act] in accordance with that section.

In 2018–19 we pursued our purpose through four key activities:

- countering terrorism;
- countering espionage, foreign interference, sabotage and malicious insiders;
- countering serious threats to Australia's border integrity; and
- providing protective security advice to government and industry.

The annual performance statements in Part 4 of this annual report summarise our performance in relation to these key activities during 2018–19.

[1] This purpose statement reflects our outcome in the ASIO Portfolio Budget Statement 2018–19: 'To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to Government'. This outcome is supported by Program 1.1: security intelligence. ASIO's *Corporate Plan 2019–20* adopts a revised purpose statement for the Organisation: 'As the nation's security service, ASIO protects Australia from violent, clandestine and deceptive efforts to harm its people and undermine its sovereignty'. This annual report addresses the purpose statement contained in ASIO's *Corporate Plan 2018–19.*

Potts Point, Sydney (1949–51)

Queens Road, South Melbourne (1951–68)

469 St Kilda Rd, Melbourne (1968–86)

Russell Offices, Canberra (1986–2014)

Commitment to legality and propriety

In working to meet our purpose, ASIO must 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.

ASIO's accountable authority

Mr Duncan Lewis AO DSC CSC, Director-General of Security was ASIO's accountable authority during the 2018–19 reporting period. Mr Lewis commenced as Director-General of Security in September 2014. Mr Lewis concluded his term as Director-General on 14 September 2019. Mr Michael Burgess commenced as Director-General of Security on 15 September 2019.

Organisational structure

An overview of ASIO's organisational structure during 2018–19 is provided in Figure 1.

Organisational structure

as at 30 June 2019

Duncan Lewis

DIRECTOR-GENERAL OF SECURITY

- Chief Transformation Officer
- Chief Digital Advisor

Deputy Director-General
STRATEGIC ENTERPRISE MANAGEMENT GROUP

First Assistant Director-General

- Enterprise Transformation
- State Manager NSW North
- Enterprise Strategy and Governance
- State Manager Vic. South
- Corporate and Security
- Office of Legal Counsel

Assistant Director-General

- Enterprise Transformation
- North
- Enterprise Risk and Assurance
- South
- Internal Security
- Assessments, Corporate Law and Capability Protection
- Digital Advice
- Strategic Engagement
- Financial Management
- Operations Law
- Enterprise Transformation 1
- Enterprise Strategy and Management
- Human Resources
- Litigation
- Ministerial, Media and Communication
- Property Management
- People Strategy

Deputy Director-General
OPERATIONAL SUPPORT AND CAPABILITIES GROUP

- Technical Capabilities

Assistant Director-General

- Data and Technical Analysis
- Telecommunication Operations
- Computer Operations
- Close Access Operations
- Strategy and Performance

Figure 1: ASIO's organisational structure at 30 June 2019

Deputy Director-General
OPERATIONS AND ASSESSMENTS GROUP

Operational Capabilities	Information	Data	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 Mission	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			
			Counter-Espionage and Interference F			

3

AUSTRALIA'S SECURITY ENVIRONMENT AND OUTLOOK

Australia's security environment and outlook

Terrorist threat—onshore and offshore

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.

The threat of terrorism in Australia remains elevated—with some Australia-based extremists maintaining the intent and capability to conduct attacks onshore. Since September 2014, when the national terrorism threat level was raised, there have been seven attacks targeting people and 16 major counter-terrorism disruption operations in response to attack planning in Australia. While the frequency of attacks and disruptions has decreased since a peak in 2016, terrorism-related incidents continue to regularly occur in Australia.

The principal source of the terrorist threat remains Sunni Islamist extremism and emanates primarily from small groups and individuals inspired, directed or encouraged by extremist groups overseas. Overseas groups continue to espouse a violent ideology which resonates with some Australia-based extremists. Repeated calls for attacks in the West will continue to adversely shape Australia's security environment. Other forms of extremism are currently less likely to manifest in violence over the next 12 months.

The targeting preferences of onshore extremists are likely to continue to be directed towards 'soft' targets, such as crowds of people in public places, over targets such as infrastructure, where greater physical security measures exist. While the symbolic appeal of an attack against a government or authority—such as the military, police and security agencies—remains, easily accessible targets can reduce the capability required to undertake a successful terrorist attack. Terrorist targeting of crowded places, in particular, has featured in recent terrorist attacks both onshore and globally. A low-capability attack targeting people fulfils a number of key terrorist objectives, including casualties, public fear and anxiety, and media attention.

- Any terrorist attack in Australia for at least the next 12 months is more likely to be low cost, locally financed, and use readily acquired weapons and relatively simple tactics. However, terrorists are creative and could use new and innovative weapons and tactics.

The influence of offshore terrorist groups

The Islamic State of Iraq and the Levant (ISIL) has lost all of its former territory. While ISIL's ability to direct external attack planning from the conflict zone may have been diminished because of sustained losses, the group continues to inspire attacks globally—including against the West. ISIL's violent Islamist extremist ideology retains its appeal with extremists, many of whom continue to draw inspiration from developments in the Syria and Iraq conflict zone to justify extremist narratives. Calls by ISIL for attacks in the West are likely to continue.

Islamist extremist groups and supporters will continue to disseminate propaganda designed to radicalise, recruit and inspire terrorist attacks in the West, including in Australia.

- While a single piece of propaganda in isolation is unlikely to be the sole catalyst for an onshore attack, we remain concerned that the reinforcement through propaganda of a particular weapon or tactic may increase the likelihood of it being used in onshore terrorist attacks.

Australian travellers to the conflict zone

Australian foreign fighters may take months or even years to return to Australia. Some Australians have returned already, and further returnees, including women and children, are likely. Whether these individuals present an ongoing threat will depend on their ideology and willingness to participate in violence onshore.

A small number of Australians continue to hold an intention to travel to the Syria and Iraq conflict zone. Prevented or aspirational travellers may maintain their extremist ideology. It is feasible these individuals could shift from seeking to travel to planning to undertake an attack onshore.

Extreme right-wing terrorism in Australia

The threat from the extreme right wing in Australia has increased in recent years. Extreme right-wing groups in Australia are more cohesive and organised than they have been over previous years, and will remain an enduring threat. Any future extreme right-wing-inspired attack in Australia would most likely be low capability and conducted by a lone actor or small group, although a sophisticated weapons attack is possible.

Communal violence and violent protest

Australia continues to enjoy a high level of community cohesion, and communal violence is infrequent. Previous acts of communal violence in Australia have primarily occurred because of local or international events that resonated with expatriate communities. The most likely form of expression of communal tensions will be through public events and demonstrations aimed at drawing the attention of the broader Australian community towards specific issues.

Violent protest in Australia continues to be rare, and the vast majority of protest activity concludes peacefully. Where violence has occurred, it has generally been opportunistic rather

than pre-planned. Over the next 12 months, acts of opportunistic violence or civil disobedience at protests are possible, particularly those attended by counter-protesters.

Terrorism—the international security environment

Terrorism has maintained a stubborn momentum into 2019 and will continue to evolve, representing a potent threat with global dimensions and reach. Terrorists inspired by violent Islamist extremist and right-wing extremist ideologies reinforce their respective narratives by fomenting hatred and inciting violence to realise their ideological objectives. Terrorist attacks globally, whether directed or inspired, are now an indelible feature of the security environment.

The international security environment is shaped by extremists subscribing to a broad spectrum of violent ideologies. ISIL and the networks it has spawned, in person and virtually, have endured beyond the collapse of its so-called caliphate and continue to present a transnational threat. Al-Qa'ida continues, through its affiliates, to embed itself in local conflicts, exploiting parts of the globe where governance is weak and security conditions are advantageous; but it has not relinquished its longstanding anti-Western ethos. The right-wing extremist attacks in Christchurch on 15 March 2019 demonstrate that it takes only a single individual to embrace and act on a violent extremist ideology to have a global impact.

Online propaganda remains an indispensable tool for extremists. Social media, file-sharing platforms and encrypted messaging applications remain vehicles for the global dissemination of easy-to-digest narratives aimed at attracting supporters and inciting violence. ISIL's approach to propaganda has set the standard among Islamist extremists, but right-wing extremists will also continue to produce internet-savvy, sophisticated messaging.

Europe

Europe remains a target for attack by individuals affiliated with, or inspired by, Islamist extremist groups such as ISIL and al-Qa'ida. The most likely source of attack is an individual or small group inspired by Islamist extremist ideology, using basic weapons (such as knives and vehicles), firearms or explosives to target crowded places. During 2018–19, Islamist extremist attacks occurred in several European countries, including the United Kingdom, Spain, the Netherlands and France. Disruptions also continue to occur regularly throughout Europe, further demonstrating the ongoing intent and capability of extremists to conduct attacks. The potential return of foreign fighters to Europe, with experience and hardened ideologies, is likely to exacerbate the terrorist threat.

South-East Asia

Terrorism is resurgent in South-East Asia, where ISIL's propaganda, resources and direction have reinvigorated Islamist extremism and increased the current threat of terrorist attacks in our near region. Undeterred by ISIL's loss of territory in the Middle East, pro-ISIL groups and individuals in Indonesia, Malaysia and the Philippines have continued their campaigns of plots and attacks in support of ISIL and local extremist agendas. While ISIL continues to dominate the regional threat environment with low-capability but often deadly attacks conducted primarily against local security forces and sectarian targets, al-Qa'ida groups continue to exist in South-East Asia and are undertaking recruitment and training in preparation for possible future acts of violence.

Reinvigoration of cross-border extremist connections within the region, and extending to foreign conflict zones, has increased the risk of inter-group cooperation, sharing of skillsets, and transfer of attack methodologies and ideology. Under ISIL's influence, attack methodologies in the region are evolving; for example, suicide bombings have emerged in 2018–19 as a new and repeated tactic in terrorist attacks in the southern Philippines.

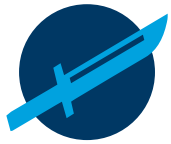
South-East Asians travelled in large numbers to the Syria and Iraq conflict, and extremists from South-East Asia continue to seek access to new conflict zones to fight with or give support to global jihadist organisations, including ISIL and al-Qa'ida. The potential return of South-East Asian foreign fighters from foreign conflict zones poses an ongoing risk to the regional security environment.

South and Central Asia

The terrorist threat across South Asia remains high. Islamist extremist groups continue to operate in the ungoverned areas of Afghanistan and Pakistan, where they can train, operate, recruit and fundraise with relative freedom. Afghan and Pakistani government interests, as well as religious and ethnic minorities, are frequently attacked, and Western interests continue to be highly desired targets. The Easter Sunday bombings in Sri Lanka—which killed over 250 people—demonstrate the ongoing influence of transnational terrorist groups such as ISIL throughout the region. ISIL also announced a new affiliate in India, likely as part of its efforts to demonstrate its reach and strength following its territorial losses in Syria and Iraq. ISIL and al-Qa'ida in the Indian Subcontinent continue to influence Islamist extremists in Bangladesh, who aspire to attack foreign and domestic targets there.

Middle East

The Middle East security environment remains highly complex and dynamic, with numerous threat actors. Despite the fall of ISIL's caliphate and complete loss of territory, the group remains an enduring threat in Syria and Iraq. ISIL is conducting an insurgency in both countries, mounting attacks of varying complexity and lethality, including with explosive devices. Al-Qa'ida-affiliated or -aligned groups in the Middle East continue to thrive in areas of instability, sectarian tension and civil strife, particularly north-west Syria and Yemen. While they appear focused on local issues, these groups represent an enduring threat to Western interests.



Basic weapons

Basic weapons are defined as readily available, everyday objects that do not require specific skills or training to use as weapons. These weapons include knives and vehicles. Four of the seven terrorist attacks in Australia since September 2014 have used basic weapons.

Explosives

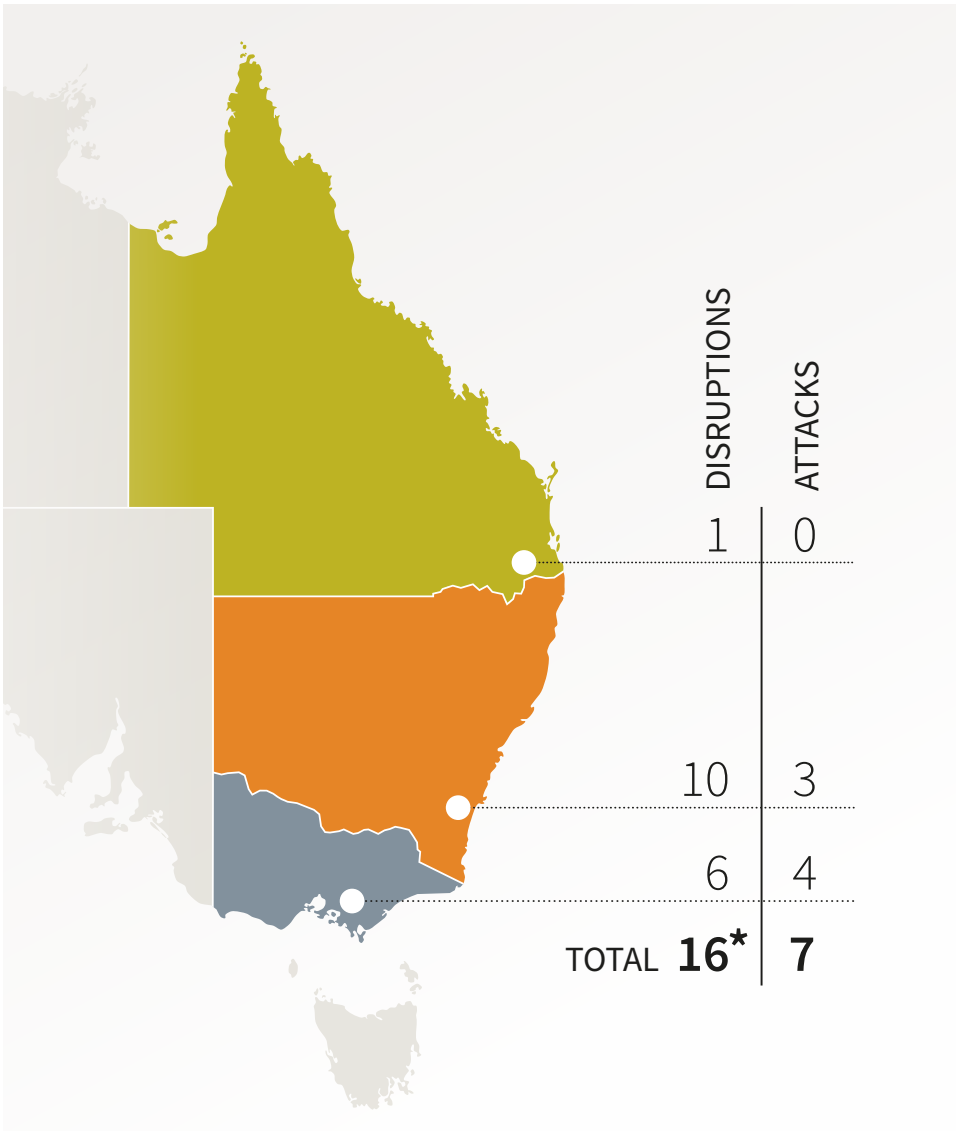
Explosives remain a popular tactic due to their accessibility and proven effectiveness in causing mass casualties and economic disruption. Australia-based extremists may consider the use of homemade, commercial or military explosives for a domestic terrorist attack. One terrorist attack has involved the use of a flammable gas cylinder in an attempt to create an explosion in Australia.

Firearms

Australia-based extremists continue to show interest in firearms-based terrorist attacks. Three of the seven terrorist attacks in Australia since September 2014 have used firearms.

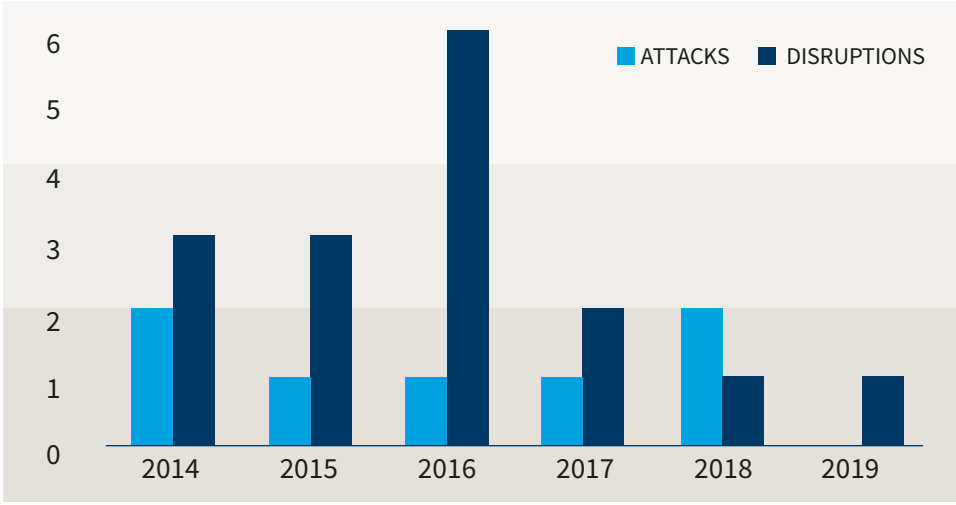
Onshore terrorist attacks and counter-terrorism disruption operations since September 2014

Locations of onshore terrorist attacks and major 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 have been counted only once.

Frequency of onshore terrorist attacks and major counter-terrorism disruptions since September 2014



Targeting preferences of onshore extremists who successfully conducted terrorist attacks or who were disrupted beforehand since September 2014*

17

Members of the public and crowded places

1

Unspecified/undecided

9

Police, military or government agencies

1

Infrastructure

* These numbers take into account groups and individuals who were considering multiple different target types before they were disrupted.

Outside Syria and Iraq, groups and individuals of varying affiliation or alignment have attacked a range of targets including in Egypt, Israel and the Palestinian Territories, Iran, Saudi Arabia and Yemen. Turkey also remains a high-threat environment despite the absence of recent significant attacks or plot disruptions, with both ISIL and Kurdish groups retaining the capability to conduct attacks, including in metropolitan centres. As a political solution to Yemen's civil war remains elusive, the country's security environment continues to be highly unstable and complex.

Espionage and foreign interference

Australia continues to be a target of espionage and foreign interference—activities that can harm Australia's interests by undermining its national security and sovereignty; damaging its reputation and relationships; degrading its diplomatic and trade relations; inflicting substantial economic damage; compromising nationally vital assets, defence capabilities and critical infrastructure; and threatening the safety of Australians.

Important legislative reform in 2018–19 has provided ASIO and our partners with a range of new tools to counter foreign interference. The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* and *Foreign Influence Transparency Scheme Act 2018* will strengthen Australia against acts detrimental to its security and provide the Australian public with a greater degree of transparency regarding those who represent the interests of foreign states. These tools will increase the cost and risk of conducting foreign interference in Australia and make it more difficult for Australia's adversaries to threaten its interests.

Australia's national security and economic growth are at risk from foreign states seeking to advance their strategic and economic interests at the nation's expense. Foreign intelligence services continue to seek access to privileged and classified information. Australia's research and development of innovative technologies and its military modernisation program are attractive targets for espionage by foreign states seeking to gain an advantage to the detriment of Australia's security and prosperity.

Australia's telecommunications sector is also an attractive target, as it underpins Australia's critical infrastructure and provides opportunities for our adversaries to conduct activities that pose a persistent threat to national security. The security and integrity of these networks and the communications and data they carry is of the upmost importance. The implementation of the *Telecommunications and Other Legislative Amendments Act 2017*—also referred to as the Telecommunications Sector Security Reforms—provides valuable new tools to help combat this threat.

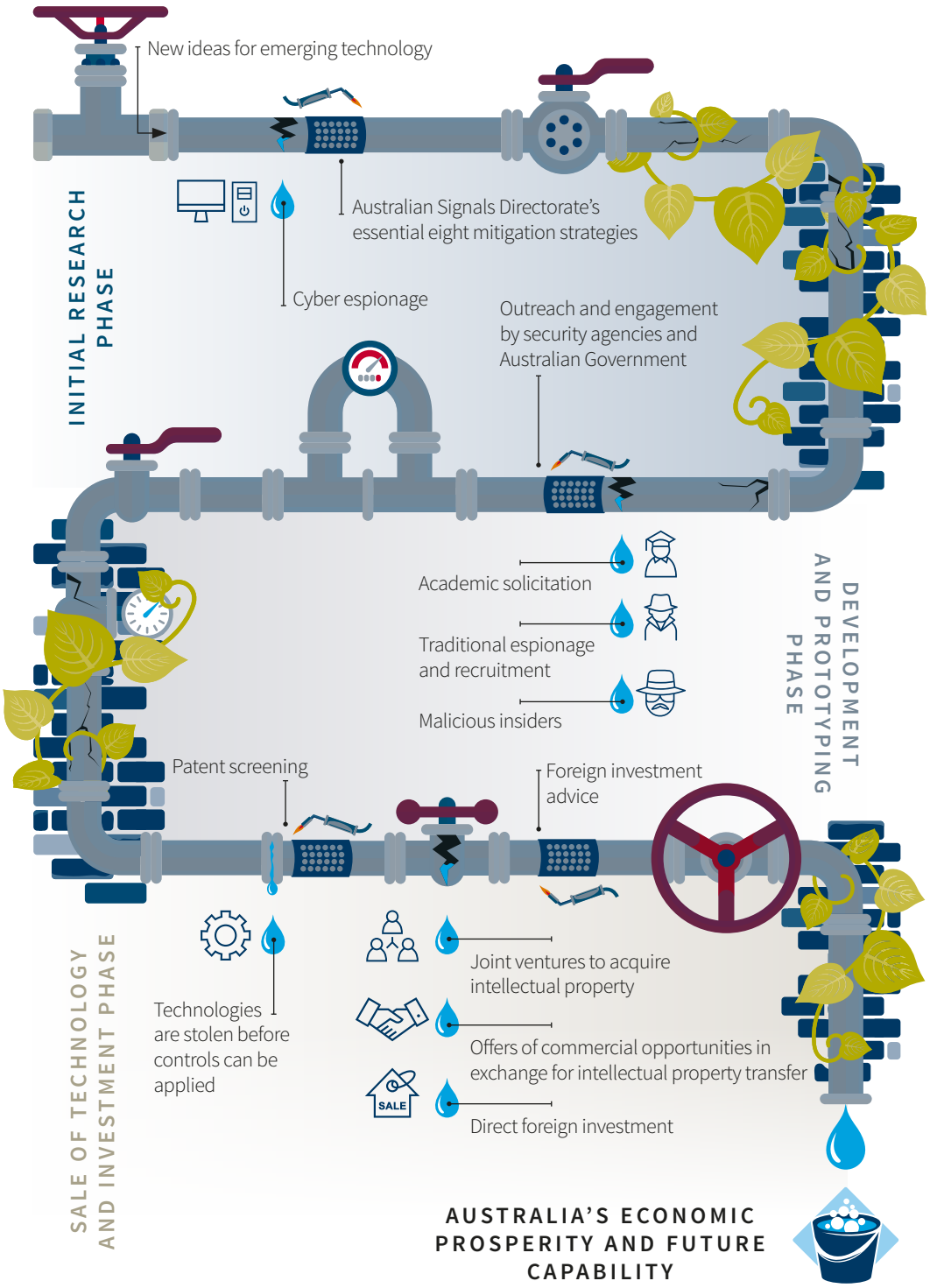
We continue to observe foreign states seeking to monitor and control the activities, opinions and decisions of sections of the Australian community in a way that impinges on the freedom of speech, association and action of members of the Australian public,

media organisations and government officials. If left unchecked, such interference enables foreign states to exercise power and influence in a way that undermines Australia's sovereignty and confidence in the integrity of its system of government.

We are keenly aware of the importance of foreign investment to Australia's economic prosperity, and fully support the need to balance national security with broader national interest considerations. Foreign intelligence services seek to exploit Australia's businesses for intelligence purposes. That threat will persist across critical infrastructure, industries that hold large amounts of personal data, and emerging sectors with unique intellectual property that could provide an economic or strategic edge.

Foreign states continue to undertake acts of cyber espionage targeting Australian Government, academic, industrial and economic information technology networks and individuals, to gain access to sensitive and commercially valuable information—these threats to Australia's security continue to increase in scale and sophistication. Cyber espionage is a relatively low-risk and scalable means of obtaining privileged information, which adds another potent method to the array of espionage techniques through which foreign intelligence agencies and other hostile actors can target Australians and Australian interests.

Emerging technology pipeline



4

REPORT ON PERFORMANCE

4

ASIO annual performance statement 2018–19

Introductory statement

I, as Director-General of Security and the accountable authority of ASIO, present the 2018–19 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

ASIO's purpose

ASIO's purpose[3] 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 2018–19 we pursued this purpose through four key activities:

- **key activity 1:** countering terrorism;
- **key activity 2:** countering espionage, foreign interference, sabotage and malicious insiders;
- **key activity 3:** countering serious threats to Australia's border integrity; and
- **key activity 4:** providing protective security advice to national security partners.

In addition, we continued to progress the enterprise transformation program commenced in July 2018, through reforms to our operating model, leadership and workforce management practices, and use of technology. The successful delivery of the transformation program will be essential to ensure ASIO continues to evolve as an organisation that can respond effectively to the challenges of a rapidly changing and uncertain security environment.

Results for 2018–19

ASIO's *Corporate Plan 2018–19* 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 2019.

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'.

[3] ASIO *Corporate Plan 2019–20* adopts a revised purpose statement for the Organisation: 'As the nation's security service, ASIO protects Australia from violent, clandestine and deceptive efforts to harm its people and undermine its sovereignty'. The performance statement in this annual report addresses the purpose statement and associated performance measures contained in ASIO's *Corporate Plan 2018–19*.

Key activity 1: countering terrorism

Performance objective

Our advice informs Australian Government policy development and responses to terrorism

2018–19 result

ACHIEVED

Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

Support for policy and legislative development

During 2018–19, we continued to provide effective advice to support policymakers and legislators in developing their responses to terrorist attacks and terrorism-related threats.

A significant focus remained the Australian Government's response to the threats posed by Australians who travel overseas to fight with or are supportive of terrorist organisations. Our participation in this whole-of-government response can be seen in the provision of advice and assessments, relevant to our remit, to inform Australian Government considerations of the development of the Strengthening the Citizenship Loss Provisions Bill 2018 and the Counter-Terrorism (Temporary Exclusion Orders) Bill 2019.

We also provided advice and briefings to assist policymakers and legislators in developing the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. This included a range of case studies demonstrating the use of encryption by the subjects of counter-terrorism investigations to frustrate security and law enforcement agencies' efforts to identify and disrupt harmful activities. We also provided advice on legislative proposals relating to compulsory questioning powers; the sharing of online violent, abhorrent material; and religious discrimination.

Security environment awareness

Our assessments of the terrorism threat environment continued to be in high demand during 2018–19 among our federal, state and territory policy, security and law enforcement partners. We published 983 intelligence and security reports on local and international counter-terrorism matters during the reporting period. Our assessments informed stakeholders on a wide range of current terrorism-related matters, including terrorist weapons and tactics, right-wing extremism in Australia, and the threat posed by ISIL and al-Qa'ida.

We provided stakeholders with regular assessments and statistics on Australians linked to extremist groups involved in the Syria/Iraq conflict who were located overseas or had returned to Australia, to raise awareness of the threat posed by these individuals and to inform mitigation strategies. A number of whole-of-government products and processes have been informed by the statistics we have developed on foreign fighters, returnees, subjects of investigation and caseloads—including talking points, and ministerial briefings and requests.

We contributed to the security awareness of the Australia-New Zealand Counter-Terrorism Committee (ANZCTC) through regular briefings at committee meetings. Our knowledge informed the committee's consideration of strategic risks and consequent resourcing decisions.

Stakeholder evaluation

Stakeholders participating in our annual stakeholder survey continued to hold our advice informing counter-terrorism policy and responses in high regard, advising it played a crucial role in the development of ministerial-level decisions. They particularly noted the briefings provided by ASIO senior officers to key stakeholders, where ASIO not only explained the advice but also its likely impact and potential legal implications. Although Operation Silves—which disrupted a terrorist attack plan against aviation—occurred almost two years ago, the impact is still felt, with stakeholders noting that ASIO advice heavily informs government responses and further mitigation strategies.

Stakeholders also commended the quality of our assessments and range of analytical products, including our willingness to publish liaison reports. The threat assessments produced by the National Threat Assessment Centre (NTAC) were viewed by stakeholders—particularly those with significant overseas travel—as a valuable complement to the Department of Foreign Affairs and Trade's Smart Traveller advice. Stakeholders also commented positively on the increasing number of joint reports prepared with other agencies, which was seen as indicative of the greater collaboration between ASIO and partner agencies and our willingness to draw on the expertise of others.

Key activity 1: countering terrorism

Performance objective

National security partners use our advice to disrupt and defend against terrorism

2018–19 result

ACHIEVED

Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

Counter-terrorism disruptions

In 2018–19 ASIO intelligence made a direct contribution to the identification and disruption of terrorism-related threats to Australians and Australian interests.

Notable disruptions informed by ASIO during the period included:

- the arrest of three individuals in Melbourne on 20 November 2018 in relation to a possible terrorist attack. The individuals were subsequently charged with one count of other acts done in preparation for, or planning, terrorist acts under subparagraph 101.6 of the Criminal Code (Commonwealth);
- the arrest of an individual in Melbourne on 20 June 2019 in relation to possible foreign incursions offences. The individual was charged with acts in preparation for foreign incursions contrary to subparagraph 119.4 of the Criminal Code; and
- the arrest of three individuals in Sydney on 2 July 2019 (the culmination of an intensive covert investigation since late 2018) in relation to a range of terrorism and other offences. One of those arrested was charged with three terrorism offences, including undertaking acts in preparation for or planning terrorist acts, preparations for foreign incursions, and membership of a terrorist organisation. The terrorist activity for which these individuals were eventually charged was first uncovered by ASIO intelligence operations and referred to the federal–state Joint Counter Terrorism Team for investigation.

We supported federal–state Joint Counter Terrorism Teams in the prosecution of individuals for terrorism and related offences. This included Khaled Khayat's 1 May 2019 conviction for conspiracy to do acts in preparation for, or planning, terrorist acts in relation to his involvement in the 2017 Sydney aviation plot. We continued to contribute support to counter-terrorism judicial proceedings—some of which resulted in convictions and sentences during the reporting period. Furthermore, ASIO intelligence contributed to the Australian Federal Police (AFP) being able to swear arrest warrants for more than a third of those Australians remaining in Syria.

During 2018–19, our assessments informed the decision-making of the Minister for Foreign Affairs in relation to the cancellation of passports of individuals linked to extremist groups in the Syria/Iraq conflict. The passports were cancelled, both to prevent travel to the Syria–Iraq region and to limit the ability of the individuals already there to move beyond the region. We also provided advice on the effectiveness of, and the security rationale for, passport cancellations in relation to the Syria/Iraq conflict.

Our advice also informed Department of Home Affairs processes in relation to the loss of citizenship (under section 35 of the *Australian Citizenship Act 2007*) of individuals linked to extremist groups in the Syria/Iraq conflict.

Threat mitigation measures

Our advice informed a range of national measures implemented throughout 2018–19 to mitigate the threat posed by terrorism.

- Our advice informed the relisting of Hamas's Izz al-Din al-Qassam Brigades, al-Shabaab, Kurdistan Workers' Party, Lashkar-e-Tayyiba, and Palestinian Islamic Jihad as terrorist organisations under Part 5.3 of the Criminal Code.
- We contributed legal and analytical expertise in support of high-risk terrorism offender regimes, including the Australian Government's continuing detention order regime and the implementation by New South Wales of the *Terrorism High Risk Offenders Act 2017* (NSW).
- We continued to work with federal, state and territory partners on a multi-agency approach to the treatment of 'residual risk' posed by individuals of counter-terrorism interest who have been, but are not currently, under active investigation.
- Our assessments formed an integral part of the Australian Government's framework for managing Australians of counter-terrorism interest who either are detained offshore or express a desire to return to Australia. Our assessments were also relied on heavily by partners in developing plans to manage the return of these individuals and mitigate the risk they present on their return.
- We have established a National Intelligence Community (NIC) Counter-Terrorism Discovery Program consisting of embedded officers from ASIO, AFP, Australian Criminal Intelligence Commission (ACIC), Australian Transaction Reports and Analysis Centre (AUSTRAC), and the Department of Home Affairs to proactively identify new threats, thereby providing assurance in relation to threats that may emerge outside existing NIC coverage.

Prioritising threats

We supported Australian and international partners' counter-terrorism efforts by providing advice on where operational resources could be placed for greatest effect. This prioritisation advice—which includes weekly and monthly updates on investigation priorities and associated requirements—was highly valued by partners and informed their own operational priorities.

Stakeholder evaluation

Stakeholders regarded our advice and intelligence reports as valuable contributions to the effort to disrupt and defend against terrorism. In the wake of the March 2019 attacks in Christchurch, New Zealand, stakeholders viewed our coverage of the extreme right wing in Australia to be effective, acknowledging that significant foundational work had occurred before the attacks.

A significant number of our stakeholders—particularly in the states and territories and in the business and tertiary education sectors—continued to regard our reports and assessments as indispensable in informing their terrorism defences. A key component of this knowledge-sharing was the dissemination work performed by the Business and Government Liaison Unit (BGLU), through its website and sectoral briefing days.

Strong praise for our counter-terrorism work was received from federal and state government and law enforcement stakeholders. They commented favourably on the manner in which we engage with our counter-terrorism partners; and a number of key stakeholders advised they believed the operational success of disruption operations was achieved mainly through our close collaboration with partner agencies. While stakeholders advised that working relationships established over a number of years were operating effectively, they noted there was no sense of complacency, with a number of initiatives in play to further enhance counter-terrorism collaboration.

Case study: disrupting politically motivated violence

Politically motivated violence (PMV) remains a threat to Australia. Since September 2014 there have been 16 major disruption operations in relation to imminent attack planning, and seven 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 it has built, in person or online, will continue to adversely affect both the global and Australian security environment for years to come.

Over the reporting period, ASIO, working as part of the Joint Counter Terrorism Teams, was instrumental in identifying, investigating and disrupting the activities of a number of Australian citizens who continued to materially support or participate in terrorism—including preventing Australians from travelling offshore to join extremist groups. While some who come to our attention require urgent investigation and immediate action, the identification, investigation and ultimate disruption of others can take months, if not years, to culminate. The following is an example.

In 2016 we began a security intelligence investigation in New South Wales into an Australia-based individual whom we assessed adhered to an Islamist extremist ideology supportive of ISIL and PMV. Through our continued investigation between 2017 and 2019, we identified the individual's aspiration to conduct a terrorist attack in Australia, and also identified like-minded associates both in Australia and overseas. We worked closely with our law enforcement partners in relation to their criminal investigation into the individuals, and provided unique intelligence and investigative support.

The investigation culminated in the arrest on 2 July 2019 of three individuals, one of whom was charged with multiple terrorism offences, including acts in preparation for, or planning, terrorist acts.

Following the arrest, we published threat assessments to assist our partners and stakeholders—including government, policy agencies, law enforcement, and industry—in understanding the threat and the potential reactions to the law enforcement activity.

Key activity 2: countering espionage, foreign interference, sabotage and malicious insiders

Performance objective

2018–19 result

Our advice informs Australian Government policy development and responses to espionage, foreign interference, sabotage and malicious insiders

ACHIEVED

Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

Broadening Australian Government understanding of the threat, and supporting the development and implementation of response strategies

To support policy development and inform responses to espionage, foreign interference, sabotage and malicious insiders, we published 269 intelligence and security products during the reporting period. Topics included the threats to Australian research and technology (including through technology transfer); foreign interference in the tertiary education sector; foreign intelligence interest in professional social media sites; as well as foreign intelligence service targeting of Australian Government and Defence interests and Australian Government personnel and facilities, both in Australia and abroad.

- Our advice on the scale of the foreign intelligence threat to Australian emerging technologies informed the development of a cohesive national strategy addressing the scope of technology transfer.
- We continued to contribute to awareness and understanding of the threat posed by cyber espionage undertaken against or through Australia, and emerging cyber espionage, by working closely with the Australian Cyber Security Centre. Specifically, we provided a unique insight into, together with the capability to understand, the intent, nature and harm of cyber enabled espionage and foreign interference activity.

Our advice and assessments during the reporting period continued to provide an important foundation for the work of the Home Affairs National Counter Foreign Interference Coordinator (NCFIC). Our intelligence-led 'knowledge base' directly influenced the development and understanding of a whole-of-government strategy and complementary package of initiatives to counter the foreign interference threat.

A major piece of work undertaken during the reporting period was an assessment of the ways in which entities may disrupt, impair or otherwise interfere with the Australian electoral system. The assessment directly informed the Electoral Integrity Assurance Taskforce's recommendations on mitigating the threat to the integrity of Australia's electoral system.

We provided highly valued advice to ministers and their offices on the threat of foreign intelligence services targeting Australian Government delegations travelling overseas, and measures to mitigate this threat. These briefings resulted in the adoption of security countermeasures that reduced the risk to privileged government information. We also provided advice to the Australian Government on covert intelligence activity in Australia's political environment, and advice on foreign intelligence service targeting of Australian Government personnel and facilities for intelligence collection purposes.

We continued to work with policy partners to support a renewed focus on Pacific partnerships.

Mitigating threats to critical infrastructure

Our advice continued in 2018–19 to be instrumental in providing our key stakeholders in the Home Affairs Critical Infrastructure Centre (CIC), the Department of Defence, the Treasury and the Foreign Investment Review Board (FIRB) with an understanding of threats associated with foreign ownership and control of critical infrastructure.

We provided in-depth analysis and briefings on matters such as risks arising from the aggregation of ownership in critical infrastructure, threats to the telecommunications sector and the circumvention of foreign investment scrutiny processes, to support stakeholders' decision-making and the development of mitigation measures.

We provided advice to the CIC to inform the centre's engagement with carriers and carriage service providers, to ensure telecommunications facilities are adequately protected from unauthorised interference. This included advice in relation to 43 Telecommunications Sector Security Reforms (TSSR) notifications. We further supported the CIC by participating in its outreach to and engagement with the telecommunications industry. We also contributed to the review of 31 carrier licence applications.

We provided 275 foreign investment assessments to the Treasury to support the FIRB's consideration of investment proposals. Our assessments provided advice on the potential for a foreign power to conduct espionage, foreign interference or sabotage through its involvement in specific investments. We commenced support to the Department of Defence by providing foreign ownership, control and influence checks for defence industry seeking to join the Defence Industry Security Program (DISP). These checks are intended to provide a degree of greater assurance for the supply chain and support the Department of Defence's implementation of the reformed DISP.

To build international understanding of the issues Australia is facing in the foreign investment field, we participated in working groups with international partners, and provided them with information to help develop their own recommendations.

Stakeholder evaluation

Stakeholders continued to have confidence in our contribution to counter–espionage and foreign interference policy development and responses, with advice seen as hitting the mark and being very influential. Our ability to draw on the views and experiences of overseas counterparts, especially the Five-Eyes counterpart agencies, to inform our advice was also highly valued. It was noted that, while we seemed to be managing the desire from multiple sources for advice on foreign interference, demand was expected to outstrip our current capacity.

Stakeholders noted favourably our close work with the FIRB and the CIC when providing advice to support decision-making and risk mitigation measures in relation to investments in critical infrastructure.

Key activity 2: countering espionage, foreign interference, sabotage and malicious insiders

Performance objective

2018–19 result

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

PARTIALLY ACHIEVED

Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

Defence and defence industry support

Our work with the Department of Defence and with defence industry continued to expand during the reporting period, and to deliver outcomes to help mitigate the risk of foreign intelligence services compromising Australia's critical defence capabilities and acquisition program.

We contributed advice in support of the Department of Defence's review of a range of security policies, including risk assessments, the reformed DISP, and the inclusion of security considerations in acquisition decisions. We provided an assessment on foreign intelligence services targeting of Australian Defence interests including the Future Submarine Program, and briefed Defence personnel on strategies to reduce the risk of foreign intelligence services targeting them, in particular online and during overseas travel. The increase in demand for these briefings over the reporting period demonstrated that our advice was considered valuable and relevant by our Defence partners.

In relation to defence industry, we provided threat briefings and advice on espionage and foreign interference threats and mitigations to numerous Defence primes, and small to medium-sized defence industry companies, during the period. Feedback after the briefings indicates that several companies have enhanced their security procedures and policies, while others have been alerted to threats they would not previously have recognised. We also provided assistance to companies in developing security awareness programs for their staff and senior executives.

- We continuously refine our briefings based on feedback from our partners and stakeholders, and have developed more targeted briefings for particularly vulnerable areas.

- The interaction between our senior executives and defence industry leaders has increased, including briefings to company and corporate boards.
- We have also worked more closely with the Department of Defence on synthesising and actioning leads generated through contact and incident reports to identify early indications of foreign intelligence service targeting.

We worked with the Department of Defence to implement a new initiative requiring mandatory membership of the BGLU website for new members of the DISP. This has improved our ability to provide unclassified advice directly to a much larger number of defence industry providers, especially small and medium enterprises we have not traditionally had contact with, while also improving our ability to contribute advice to protect the government's Defence capability investment throughout more of the supply chain.

Personnel security assessments

Our personnel security assessments continued to play a critical role in assisting partner agencies to protect classified and sensitive government information, areas and resources.

In 2018–19, we completed 32 887 personnel security assessments, comprising 28 796 assessments for Baseline, Negative Vetting (NV) 1 and 2 clearances and 4091 Positive Vetting (PV) clearances. We completed a number of adverse and qualified personnel security assessments, containing information and recommendations on an individual's suitability to be granted or continue to hold a clearance. As a result of these assessments, the risk to sensitive government information and/or areas was mitigated.

- Feedback from the Australian Government Security Vetting Agency (AGSVA)—the central security vetting agency—acknowledged that the PV caseload had significantly reduced and we had succeeded, in the main, in meeting Key Performance Indicator benchmarks for PV, NV1, and NV2 security assessments. The increase in timeliness has enabled AGSVA to meet its benchmarks and has enabled sponsoring entities to onboard staff in a timely manner.
- The contribution provided by ASIO secondees to the AGSVA—in line with the recommendations of the Independent Intelligence Review of June 2017—has reinforced the cooperation between our two agencies and enabled a greater sharing of knowledge and expertise.

Enhancing understanding of the threat

In addition to producing personnel security assessments, we provided briefings around Australia to AGSVA staff, industry vetting providers and other government agencies through the AGSVA Stakeholder Engagement Forum and Government Security Committee. These briefings were well received, with participants confirming the advice provided had assisted them to better understand the general foreign intelligence service threat environment as well as agency-specific risks, ASIO's role in the security clearance process, and the impact of legislative change on the clearance process.

We provided assessments and advice that assisted Australian Government agencies to make intelligence-based decisions on the suitability of individuals to hold security clearances, and to mitigate insider threat risks. Our tailored protective security briefings for clearance holders have increased awareness of the threat posed by foreign intelligence services, and the security obligations of Australian Government employees while in Australia and overseas, including contact reporting.

Espionage and foreign interference legislation

We worked closely with the AFP during the reporting period, to progress implementation of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*, including through capability building and review of espionage lead information.

We assess that passage of the espionage and foreign interference legislation has had an impact on espionage and foreign interference in Australia, and caused some foreign intelligence services to re-assess the risks associated with clandestine foreign intelligence operations conducted in or against Australia. However, we anticipate the most capable foreign intelligence services will adapt their behaviour over time to circumvent the new legislation.

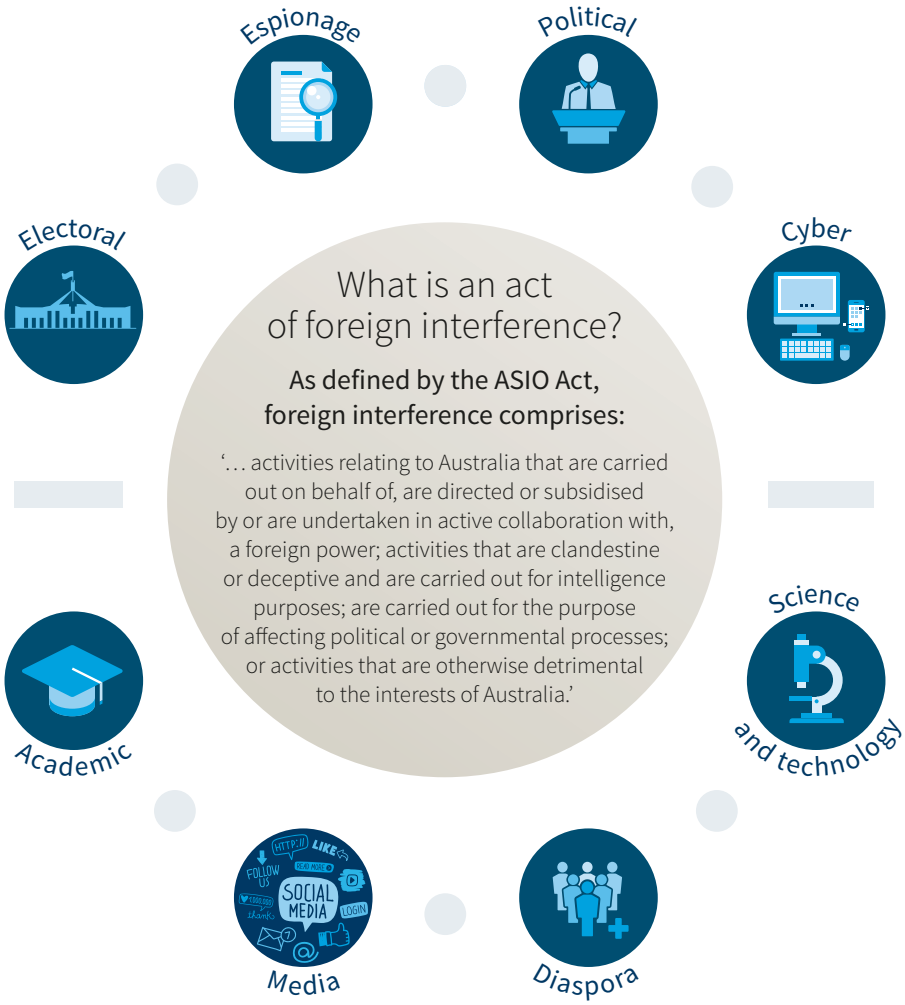
'Partially achieved' result

Our capacity to provide our partners with advice is being outstripped by demand; hence our assessment that this result was 'partially achieved'. Measures we have instigated to meet these challenges include providing dedicated resourcing in key regional positions, collaborating with external partners in delivering briefings and advice, engaging with industry peak bodies to capture broader industry cross-sections, and streamlining internal and external partner agency processes. Notwithstanding these measures, the significant growth in demand for our advice will continue to present a challenge for ASIO, necessitating a continued focus on the most valuable activities in collaboration with our strategic partners.

Stakeholder evaluation

Stakeholders expressed high regard for our assessments and advice on counter-espionage intelligence and investigations, believing it to be well targeted and appropriate, and, where relevant, having made a positive business impact. There was, however, a significant hunger for more assessments on this threat.

Stakeholders appreciated the increasing accessibility they had to ASIO staff as our efforts to counter espionage and foreign interference become more prominent. Compared with previous years, stakeholders were more aware and had a greater understanding of the Contact Reporting Scheme, particularly its potential value and how to access it, with a number of non-government stakeholders interested in being more engaged in the scheme.



Key activity 2: countering espionage, foreign interference, sabotage and malicious insiders

Performance objective

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

2018–19 result

PARTIALLY ACHIEVED

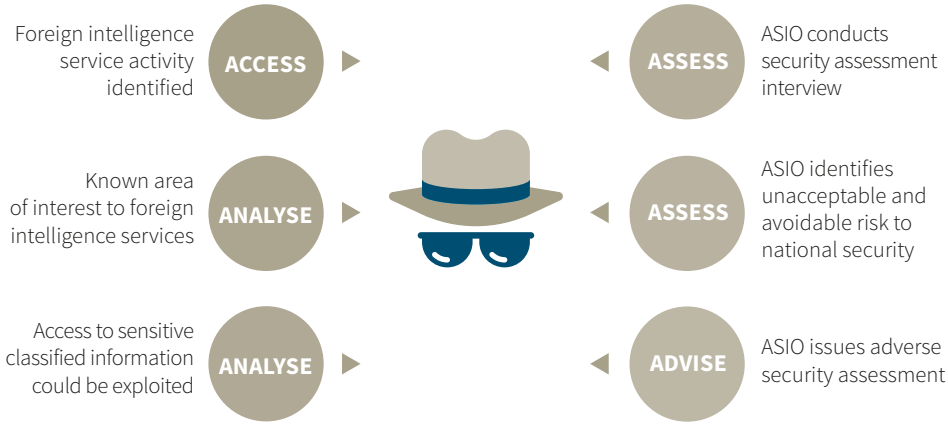
Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

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 outcomes achieved in this area are classified.

The ongoing high tempo of counter-terrorism and counter-espionage investigations and operations continued in 2018–19 to limit the resources available within ASIO to meet the foreign intelligence collection requirements of Australia's foreign intelligence agencies. While the collection operations we conducted on behalf of partners during the reporting period yielded valuable and unique intelligence, the 'partially achieved' result acknowledges that we were unable to progress other collection operations requested by partners.

Stakeholder evaluation

The few key stakeholders we engage with in this area advised we continued to demonstrate a high level of cooperation in operations to collect foreign intelligence in Australia. In acknowledging the quality of our work—together with the significant contribution it makes to their operational success—stakeholders commented particularly favourably on our agility in planning and executing collection operations.



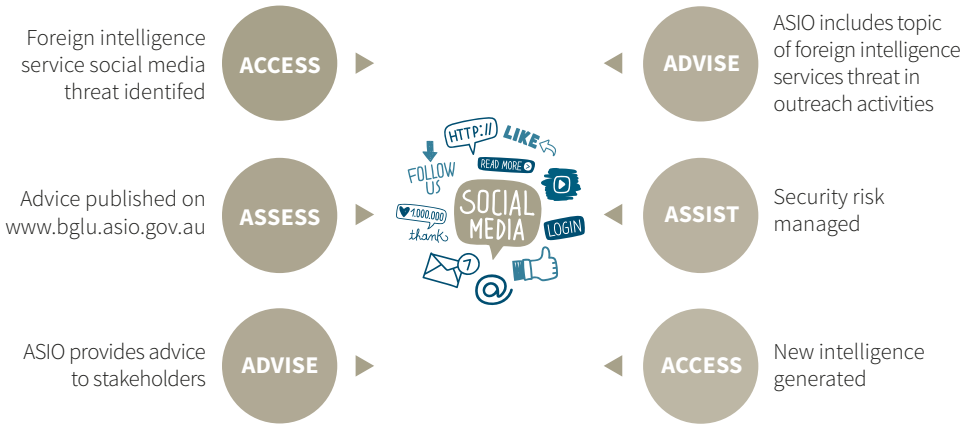
Case study:
clearance holder in contact with a foreign intelligence service

4

An ASIO investigation revealed that an Australian Government clearance holder was in ongoing contact with a foreign intelligence service in Australia. We assessed this contact could allow the clearance holder's access to sensitive classified information to be exploited. The clearance holder worked in an area of the Australian Government of interest to the foreign intelligence service.

ASIO conducted a security assessment interview of the clearance holder to determine whether they had been the unwitting subject of an intelligence cultivation. We subsequently assessed that their continued access to sensitive information allowed through a security clearance would represent an unacceptable and avoidable risk to national security from espionage and acts of foreign interference.

Our adverse security assessment recommended the clearance holder's security clearance be revoked. This recommendation was accepted by the vetting agency, and appropriate action was taken in concert with the clearance sponsor.



Case study:
preventing hostile intelligence approaches through social media

During the year, we developed advice describing how hostile intelligence services use LinkedIn and other social media platforms to target people in positions that could fulfil a wide range of intelligence objectives.

The report's release generated awareness of this vector being used for hostile intelligence activity, led to action by stakeholders to better manage security risks, and provided some new intelligence back to ASIO.

Our advice was distributed to stakeholders across government, business and industry, including to Business and Government Liaison Unit (BGLU) subscribers. We included advice on the topic in our outreach activities, through ongoing security awareness briefings, and in specific engagements with government, defence industry, and research institutions.

Stakeholders used our advice to respond to this threat vector and improve their security awareness and systems. Their feedback on the report itself was also positive.

- The ASIO Stakeholder Survey highlighted users, including in defence industry, identifying this report as a good example of ASIO advice directly influencing management of security risks.
- Feedback from working-level users across stakeholder groups showed they drew on our advice to generate their own messaging and amplify awareness within their organisation using internal corporate communications channels.

- In a small number of organisations, security teams were considering making policy changes in response to receiving our advice; for example, to limit or restrict social media access on their corporate networks.

The report also generated some new intelligence back to ASIO by prompting clearance holders to report social media approaches, based on our advice of how hostile intelligence actors craft social media approaches.

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

Performance objective

2018–19 result

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

ACHIEVED

Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

During the reporting period, we continued to support the development of Australian Government policy on border security. We contributed advice that informed policy and decision-making on Operation Sovereign Borders, regional processing arrangements, community cohesion initiatives, the operation of the Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) schemes, and the streamlining of the referral criteria for national security assessments of visa and citizenship applications. We also continued to contribute to a number of government coordination forums on border security issues.

Stakeholder evaluation

The Department of Home Affairs viewed ASIO as a capable partner providing a valued contribution to the effort to disrupt serious threats to Australia's border integrity, through the identification and assessment of threats and our substantial contribution to the inter-agency process. Furthermore, the department considered our contribution to policy development to be appropriate and influential.

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

Performance objective

2018–19 result

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

ACHIEVED

Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

Support for Operation Sovereign Borders

We continued to support Operation Sovereign Borders by investigating Australia-based links to people-smuggling ventures, contributing to contingency plans, and providing advice to the Joint Agency Task Force on the threat environment. During the reporting period, the intelligence derived from our investigations contributed directly to the operational activities of Operation Sovereign Borders member agencies. We also drew on our analytical and operational work to contribute to the intelligence requirements of the Department of Home Affairs, undertake security assessment interviews, and furnish adverse security assessments in relation to people-smuggling activities.

Visa security assessments

We provided 11 699 security assessments to the Department of Home Affairs in 2018–19 to support its decision-making on the issuing of a range of visas (see Table 1 below). These assessments included a relatively small number of adverse security assessments in relation to individuals whom we assessed to be directly or indirectly a risk to security within the meaning of section 4 of the ASIO Act. Most of the adverse security assessments were issued on counter-terrorism grounds. These assessments informed the taking of prescribed administrative action by the Department of Home Affairs to mitigate the threat posed by these individuals, including through visa refusal and cancellation, and refusal of Australian citizenship. In providing these assessments, we met all current service-level agreements with the department on visa security assessments.

Throughout the reporting period, we worked closely with the Department of Home Affairs to further refine the security assessment referral criteria in relation to national security, resulting in a decrease in the department's referrals to ASIO for assessment across the caseloads. We contributed to the training of Home Affairs staff in the Australia-wide visa processing network to ensure the referrals made to ASIO optimally reflect those cases which could pose the greatest risk to national security. We engaged regularly with the Department of Home Affairs to ensure that systems and policies in relation to border alerts were appropriate and fit for purpose, and also provided training and advice to Home Affairs staff to facilitate appropriate resolution of border alerts.

Table 1: Visa security assessments

Type of entry	2016–17	2017–18	2018–19
Temporary visas	3782	1746	1219
Permanent residence and citizenship	2248	294	155
Onshore protection (air)	212	66	32
Offshore refugee/humanitarian	2265	919	747
Illegal maritime arrivals	546	95	40
Other referred caseloads	5305	2334	2121
Resolution of national security border alerts*	8133	7353	7385
TOTAL	**22 491****	**12 807****	**11 699**

* In previous annual reports, we have not reported the number of resolved national security border alerts; however, in recognition of the importance of this work stream, we have commenced reporting the figures for this work this year.

**In ASIO's *Annual report 2016–17*, the total number of visa security assessments was 14 358; in ASIO's *Annual report 2017–18*, the total number of visa security assessments was 5454. Noting, however, the decision to include the 'resolution of national security border alerts' work stream, we have amended the totals to allow for a comparison of like figures.

Access security assessments

In 2018–19 we provided 135 005 access security assessments to the Department of Home Affairs (AusCheck), including in relation to individuals seeking ASICs and MSICs. We also provided 10 109 access security assessments in relation to individuals seeking access to security-sensitive chemicals, biological agents or nuclear sites. No adverse or qualified access security assessments were issued during the reporting period.

Stakeholder evaluation

Stakeholders viewed ASIO's analytical capability, advice and reporting as a valuable contribution to the effort to disrupt serious threats to Australia's border integrity. Particular note was made of our willingness to collaborate and engage positively and productively in support of this mission. Our foreign fighter profiles continued to be viewed by stakeholders as providing an important contribution to enhancing border security, while our willingness to draw on our extensive range of liaison partners, often providing unique perspectives, was appreciated and valued.

Case study: furnishing of security assessments

The terrorism threat level in Australia remains at 'Probable', which means that credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability on the part of terrorist groups or entities to undertake attacks here. Australia's border integrity and security are critical elements in Australia's defence against the terrorist threat.

In 2018–19, ASIO continued to mitigate these threats to Australia through the furnishing of security assessments to the Department of Home Affairs. For example, we investigated the case of an offshore visa applicant assessed to have previously provided logistic support to individuals affiliated with the 9/11 attacks. We assessed the individual presented an avoidable risk to Australia's security, and issued an adverse security assessment in early 2019, resulting in refusal of the visa. This example demonstrates persons with terrorist affiliations or persons supportive of ideologies committed to politically motivated violence continue to seek to undertake travel to Australia, across a range of visa categories. Our investigations are carried out with the cooperation of our domestic and international partner networks. These partnerships are invaluable in helping to keep Australians safe.

Key activity 4: providing protective security advice to national security partners

Performance objective

2018–19 result

Our protective security advice and services assist national security partners to manage security risks

ACHIEVED

Source: *ASIO Corporate Plan 2018–19*; addresses ASIO PBS 2018–19

Throughout the reporting period, our protective security advice and services continued to assist federal, state and territory governments and agencies, and industry, to manage their security risks by equipping them with credible, intelligence-backed reporting, enabling them to effect positive and effective protective security regimes. As with previous years, our Business and Government Liaison Unit (BGLU) acted as a central outreach mechanism between ASIO and our government and industry stakeholders.

- The BGLU facilitated nine government and industry briefings, including five interstate briefings. Two of these interstate briefings were specifically designed for defence industry personnel, to address the demand for our advice from this sector. Briefing sessions also targeted the health sector, the education sector, and the terrorist threat to crowded places. Attendees of six of the nine briefing days were asked to provide feedback, with 97 per cent of survey respondents advising the briefing sessions met their expectations—an increase from 92 per cent in the previous year.
- The BGLU continued to produce and disseminate domestic and international security information through its secure website. During the reporting period, 47 ASIO reports—including seven ASIO-T4 Protective Security directorate (ASIO-T4) protective security managers guides—were disseminated through the website, and subscribers grew by nearly 30 per cent, from 3262 to 4480.

In 2018–19 we continued to develop our academic outreach program in concert with other government agencies, such as the Australian Cyber Security Centre (ACSC). We expanded our engagement with more than 25 universities, research institutes, think tanks and supporting entities. This engagement enabled us to enhance the foreign intelligence threat awareness of executives and boards as well as key staff engaged in research of value to foreign intelligence services. During the reporting period, we also provided advice to help universities identify espionage and foreign interference risks to their people, assets, international partnering and business, including attempted and actual compromises of their infrastructure.

Physical protective security advice and services

ASIO-T4 provided high-quality, comprehensive and timely intelligence-led protective security advice and services to our national security partners throughout 2018–19. Instances of our partners using our advice and services to inform their approach to protective security include the following.

- The ANZCTC Crowded Place Advisory Group (CPAG) Capability Adviser forum sought ASIO-T4's expertise for input into the development of jurisdiction protective security training packages for crowded places, which focused on mitigating the risk of a terrorist attack. These courses have served to address the knowledge gap within this field by increasing the protective security awareness of general duties police and district regional managers, and increasing the capability of state and territory police protective security units to conduct vulnerability assessments of crowded places and fixed facilities.
- We published seven new protective security manager guides, including *Introduction to protective security measures* and *University and research institutes—sensitive area security*. These guides are considered to be best-practice protective security guidance produced by the Australian Government, and they continue to improve the protective security capability across government, public sector and industry partners.
- International partners asked to participate as observers at ASIO-T4's 'Introduction to Counter Terrorism Protective Security Advice' course. This course, and the other courses run by ASIO-T4, remain oversubscribed, and feedback from attendees continued to be very positive.

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

		2016–17	2017–18	2018–19
Physical security certification program				
Zone 5 facilities*	Site inspections and reports	80	89	81
	Certifications issued	39	60	40
Courier services	Site inspections and reports	3	1	8
	Endorsements issued	0	0	8
Security products evaluated				
Security products evaluated		179	71	87
Protective security review				
Protective security risk review reports		1	1	0
Communications				
Publications	Protective security circulars	6	6	1
	Security manager guides	5	10	7
	Security equipment guides	1	4	1
	Technical note annex	2	0	0
Training	Protective security training courses	4	4	6
	Safe maintainer courses	2	2	1
	SCEC**-approved locksmith briefing	1	1	1
	SCEC-approved consultant briefing	1	0	2

* The Australian Government Protective Security Policy Framework mandates that all Zone 5 facilities within Australia must be certified by ASIO-T4 before becoming operational. In some cases, ASIO inspection reports recommend that facility owners introduce additional measures to achieve certification. The difference between the number of inspection reports completed (81) and certifications issued (40) reflects work underway by facility owners to implement report recommendations.

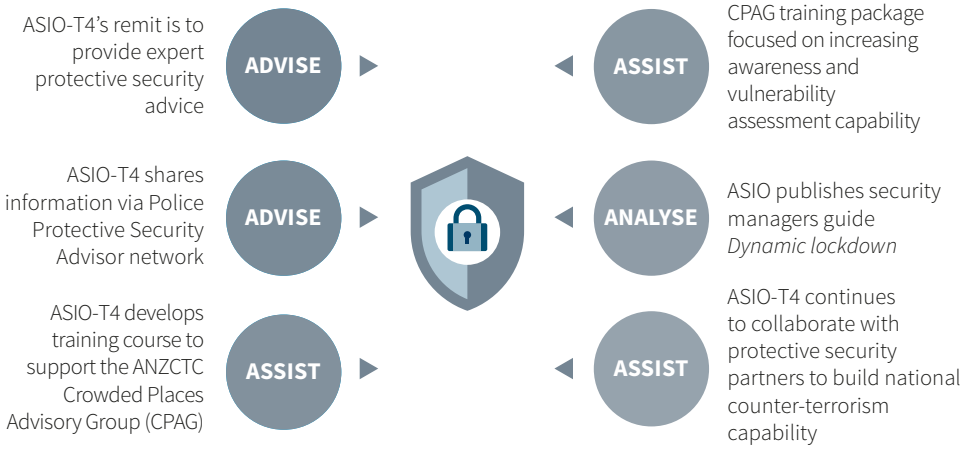
** Security Construction and Equipment Committee

Stakeholder evaluation

Stakeholders regarded ASIO-T4's protective security advice and services—including briefings, reports and guides—highly favourably and of great use in managing security risks. The quality of ASIO-T4's physical security advice was widely respected, and those who interacted with ASIO-T4 saw it as an authority whose advice could be relied on. ASIO-T4's *Security managers handbook: introduction to protective security measures* released during March 2019 was highly regarded by many stakeholders.

Stakeholders continued to value the program of sectoral briefing days and 'roadshows', seeing them as a clear expression of ASIO listening to its customers and delivering high-quality briefings. Government officials particularly expressed their gratitude for frank and focused briefings provided for ministers, especially those on terrorism, espionage, foreign interference and the malicious insider threats.

Stakeholders viewed ASIO as having made significant progress in the last year in establishing effective partnerships across key industry sectors, particularly with some small and medium enterprises and key participants in the supply chain for important capabilities. ASIO engagement with stakeholders, where it occurred, was regarded highly and considered very valuable. However, stakeholders noted with some concern the size of the task—given the large number of participants in key industry sectors—and expressed interest in assisting ASIO in raising security across the entire supply chain.



ASIO-T4 case study: building national capability to protect crowded spaces

ASIO-T4's role is to provide expert protective security advice to the Australian Government and other entities, including state and territory governments, select commercial companies, and owners and operators of national critical infrastructure. ASIO-T4 is a key contributor of protective security advice and guidance to the Australia-New Zealand Counter-Terrorism Committee (ANZCTC).

We reported in our 2017–18 annual report that ASIO-T4 established a national police counter-terrorism protective security adviser network to share information and promote collaboration on protective security matters. To support this network, in 2018–19 ASIO-T4 developed a protective security training course focused on mitigating the risk of a terrorist attack. Federal, state and territory police supporting the work of the ANZCTC Crowded Places Advisory Group (CPAG) were prioritised for attendance on the new course, which received overwhelmingly positive feedback from participants.

Analysis of performance

ASIO's purpose is to protect Australia, its people and its interests from threats to security by providing advice to assist the Australian Government, federal, state and territory national security partner agencies, and industry, to defend against and disrupt these threats. Our 2019 Stakeholder Survey—which sought views on our performance from 74 senior executives across government and industry sectors—found that ASIO was achieving this purpose. Our advice continues to be highly regarded and in high demand. Many respondents commented positively on our willingness to work closely with stakeholders and to expand our engagement to a wider range of stakeholders within government and industry.

We have, however, assessed that we have only 'partially achieved' two of the eight strategic performance objectives set out in our corporate plan for 2018–19, both of which fall within our countering espionage, foreign interference, sabotage and malicious insiders key activity (see performance objectives 2b and 2c above). While our work in these areas is highly regarded by stakeholders, the higher level of espionage and foreign interference threat facing Australia, combined with greater awareness of that threat among government and industry stakeholders, has increased demand for our advice and support, which is putting pressure on current resources.

With the terrorist threat showing no signs of significantly decreasing, ASIO has limited scope to redirect internal resources to address this steadily increasing gap between demand for our counter–espionage and foreign interference advice and our ability to inform, advise, support and assist. We will necessarily continue to prioritise our finite resources—across our counter-terrorism, counter–espionage and foreign interference, border integrity and protective security advice programs—towards addressing activities of the greatest potential harm to Australians and Australian interests.

Report on financial performance

Financial performance

The operating environment in 2018–19 continued to be challenging, resulting in ongoing pressure on our resources and sustainability. The financial result was a deficit of $14.4 million (excluding depreciation), which represents 3 per cent of budget, compared with a small surplus of $1.0 million last financial year. The loss includes a mandatory accounting adjustment of $8.3 million for employee and make-good provisions due to interest rate movement; and the remaining $6.1 million overspend, despite measures to reduce expenditure, relates to necessary supplier costs. We have followed the appropriate government process as a result of the loss.

As part of the budget for 2018–19, ASIO received $24.4 million to assist with maintaining operating activities as well as transformation planning. Both measures will receive funding in 2019–20. In addition to this, a detailed business case for transformation will be considered as part of the 2019–20 Mid-Year Economic and Fiscal Outlook process.

Our Departmental Capital Budget (DCB) funding was $85.6 million in 2018–19 as a result of previous years' appropriation re-phasing. Next financial year, the DCB will be $61.6 million, and in 2020–21 it will stabilise at a lower figure of approximately $45 million annually. Consequently, 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.

We will continue to contribute to Australian Government savings measures, including the efficiency dividend, which will have a significant impact on our operating budget and DCB in 2019–20 and across the forward estimates. The Organisation will continue to identify and implement efficiencies and rigorously prioritise activities. However, further consideration will be given during 2019–20 to the sustainability of our current operations, in the light of our projected DCB and operating budget, and our anticipated future operating environment.

A table summarising ASIO's total resources for 2018–19 is provided at Appendix A. Our total expenses by outcomes for this reporting period are at Appendix B.

5

MANAGEMENT AND ACCOUNTABILITY

5

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 role is to provide strategic direction, manage risk, coordinate effort and evaluate performance in support of ASIO's mission and the corporate governance arrangements for the work programs for which they are responsible.

ASIO Executive Board

The Executive Board is the Director-General's peak advisory committee. Its membership comprises the Director-General, the Deputy Directors-General, an external member and the Chief Transformation Officer. The board met on a monthly basis 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, and diversity and inclusion goals.

Intelligence Committee

The Intelligence Committee (IC) oversees the governance arrangements and makes decisions relating to ASIO's security intelligence program. The IC met fortnightly during the reporting period and conducted triannual reviews of performance and risk relating to the key activities as defined in ASIO's *Corporate Plan 2018–19*. The IC reported to the Executive Board on ASIO's performance against the key activities.

Security Committee

The Security Committee (SC) oversees the governance arrangements and makes decisions relating to ASIO's internal security program. The SC met bimonthly during the reporting period and conducted a triannual review of performance and risk relating to its support of the key activities as defined in ASIO's *Corporate Plan 2018–19*.

Finance Committee

The Finance Committee (FC) oversaw the governance arrangements and made decisions relating to ASIO's financial management program. The FC met twice during the reporting period and conducted a triannual review of performance and risk relating to its support of the key activities as defined in ASIO's *Corporate Plan 2018–19*.

Workforce Committee

The Workforce Committee (WC) oversaw the governance arrangements and made decisions relating to ASIO's workforce program. The WC met four times during the reporting period and conducted a triannual review of performance and risk relating to its support of the key activities as defined in ASIO's *Corporate Plan 2018–19*.

ASIO Diversity and Inclusion Committee

The ASIO Diversity and Inclusion Committee (ADIC) oversaw the governance arrangements and made decisions relating to ASIO's diversity and inclusion program. The ADIC met five times during the reporting period and conducted a triannual review of performance and risk relating to its support of the key activities as defined in ASIO's *Corporate Plan 2018–19*.

Audit and Risk Committee

The Director-General of Security established the Audit and Risk Committee (ARC) in compliance with 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 ASIO's financial and performance reporting responsibilities, system of risk oversight and management, and system of internal control.

Under the ARC's terms of reference, 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 control and management arrangements were revised during the reporting period, with the development of the ASIO Fraud Strategy Statement 2019–21, underpinned by the ASIO Fraud Control Plan 2019–2021.

The Fraud Control Plan 2019–2021 was informed by an ASIO-wide fraud risk assessment conducted during the reporting period, and documents ASIO's approach to fraud awareness, prevention, detection, reporting and investigation. As part of this framework, all staff must complete mandatory e-Learning on ethics and accountability, which includes modules on fraud, every three years.

The updated Fraud Strategy Statement 2019–21 outlines our fraud control and management arrangements, and is available online at www.asio.gov.au/asio-fraud-strategy-statement.html.

Internal Audit directorate

The Internal Audit directorate is an important element of ASIO's governance framework. Its function provides assurance to the Director-General that ASIO's risk, control and compliance measures are appropriate and efficient.

As part of its responsibility for ASIO's assurance and audit function, the directorate undertakes compliance audits and performance reviews. Subject to security policies and operational considerations, it has unrestricted access to all ASIO premises, work areas, documentation and information that it considers necessary to meet its responsibilities.

ASIO Strategy 2018–23

During the reporting period, ASIO took critical steps towards the enterprise transformation recommended in David Thodey AO's report *A digital transformation of the Australian Security Intelligence Organisation*. One such step was the preparation of the ASIO Strategy 2018–23 (see Figure 2) to provide a roadmap for the transformation process. The strategy reframed our vision and purpose, and set out the steps we will take over the coming years to ensure we evolve as a modern, fit-for-purpose security intelligence organisation. The vision and plans within the strategy have been incorporated into the *ASIO Corporate Plan 2019–20*.

Vision

Trusted intelligence to secure Australia

Purpose

As the nation's security service, ASIO protects Australia from violent, clandestine and deceptive efforts to harm its people and undermine its sovereignty.

We will achieve our vision, and deliver our purpose, by focusing our efforts on three services—**Counter**, **Shape**, and **Build**.

Counter violent, clandestine or deceptive efforts to harm Australians and undermine Australia's democratic institutions and system of government.

Shape and inform efforts to foster institutional and community resilience, through the use of our unique understanding of the Australian and global security environments.

Build capability across Australia's national security community through investing in our people, sharing our experience with partners, and leading the development of intelligence capabilities.

ASIO's success is built on six core activities—**access**, **analyse**, **assess**, **advise**, **assist** and **act**.

We commit to continually refine and innovate how we conduct these activities to drive comprehensive change and improve how we all work.

We will invest in tradecraft and capability development, adopt new systems to automate many low-value manual processes, and explore new ways to apply sophisticated technology and data analytics to advance our intelligence efforts and enterprise management.

Imperative to the success of our core activities are eight key enablers—**people and culture; authorising environment and assurance; security; risk; technology, capabilities and infrastructure; information, data and systems; governance and strategic partnerships**.

We will deliver reforms to our work practices to become more agile and adaptive, invest in our people to meet our future workforce needs, acquire new technologies to modernise our operations, and elevate our engagement with our partners.

Figure 2: ASIO Strategy 2018–23 summary

External scrutiny

Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is a key element of the external independent oversight and accountability framework that serves to provide assurance to the Australian community in relation to ASIO's performance of its functions. The PJCIS performs an annual review of ASIO's administration and expenditure and scrutinises the non-operational aspects of ASIO's work, focusing on the effectiveness of policies, governance and expenditure. During the reporting period, we provided unclassified and classified written submissions to the PJCIS Review of Administration and Expenditure No. 17 (2017–18), as well as further supporting information to questions on notice.

In addition, the PJCIS conducts inquiries into national security legislation and matters relating to ASIO and other intelligence agencies. During 2018–19, ASIO contributed either directly or through consultation with the Department of Home Affairs to a number of PJCIS inquiries, including inquiries on the listing of terrorist organisations, the Review of the Counter-Terrorism Legislation Amendment Bill, three inquiries (one ongoing) on the Telecommunications and Other Legislation (Assistance and Access) legislation, the Review of the Australian Citizenship Amendment (Strengthening the Citizenship Loss Provisions) Bill, and the Review of the Counter-Terrorism (Temporary Exclusion Orders) Bill 2019, as well as the ongoing inquiry into Australia's mandatory data retention framework.

Senate Legal and Constitutional Affairs Committee

We appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate estimates process on 22 October 2018, 18 February 2019 and 8 April 2019. 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).

Inspector-General of Intelligence and Security

The primary role of the Inspector-General of Intelligence and Security (IGIS) is to assist ministers in overseeing and reviewing the activities of the intelligence agencies for legality and propriety. The IGIS performs this function through inspections, inquiries and investigations into complaints. The Inspector-General is also required to assist the government in assuring the parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny. The IGIS retains statutory powers akin to those of a royal commission.

The Australian community's trust and confidence in how we fulfil our legislative requirements and embody ethical standards is critical to our reputation and ongoing effectiveness as Australia's security intelligence organisation. Every ASIO officer is responsible for complying with our 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 2018–19 the IGIS regularly inspected activities across our operational functions, and investigated a small number of complaints that were received by the office. In addition the IGIS finalised an inspection project on surveillance devices. Details of the project and inspections can be found in the IGIS annual report, available online from www.igis.gov.au. We are committed to acting with legality and propriety, and in 2018–19 continued to take action to address areas identified by the IGIS as requiring improvement and further attention.

In the 2018–19 reporting period, the IGIS finalised and made recommendations on three inquiries. We have accepted all inquiry recommendations and are at various stages of implementation in consultation with the Office of the IGIS and relevant agencies.

During the reporting period, we continued to support the IGIS's important work by providing information briefings to IGIS staff on operational matters, 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 report to the Prime Minister and the parliament on an ongoing basis. This includes considering whether the laws contain appropriate safeguards for protecting individuals' rights, remain proportionate to any threat of terrorism or threat to national security or both, and remain necessary. Under the Act, the Prime Minister may also refer a counter-terrorism or national security matter to the INSLM, either at the INSLM's suggestion or on the Prime Minister's initiative.

The current INSLM, Dr James Renwick SC CSC, was appointed on 13 February 2017. During the reporting period, we contributed to his current inquiry on the Citizenship Act's citizenship loss provisions for terrorism offences, through the provision of classified briefings and documentation.

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.

In performing their 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.

In March 2019, Mr Robert Cornall AO was reappointed as the Independent Reviewer for a further two years. His annual report for the reporting period is at Appendix I.

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 prosecutions, judicial and merits review of security assessments, and civil lawsuits.

The Administrative Appeals Tribunal (AAT) reviewed a number of security assessments. While they primarily involve matters concerning politically motivated violence, we saw an increasing trend in applications for review of personnel security assessments.

Separately, current and former ASIO employees brought review proceedings challenging Comcare decisions. AAT decisions are reported on the Australasian Legal Information Institute website, Austlii, www.austlii.edu.au.

Tribunal reviews—security assessments

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

Of these:

- four matters were pending at the end of this reporting period;
- three assessments were remitted to ASIO for new assessments to be prepared, which resulted in the issuing of three non-prejudicial assessments in this reporting period;
- five applications were dismissed;
- two matters were heard, with both decisions remaining reserved at the end of this reporting period; and
- one decision was handed down, affirming the adverse security assessment which was the subject of the review.

Criminal prosecutions

Working collaboratively with law enforcement partners and prosecuting authorities, we provided information for use as evidence, with appropriate protections, to prosecutions, and responded to subpoenas and disclosure requests.

Federal and High Court reviews—security assessments

ASIO was involved in Federal and High Court proceedings, both as a respondent and as an interested third party, working closely with other stakeholders to manage the collective Commonwealth interest.

Our commitment to diversity and inclusion

We take actions which demonstrate we are a diverse and inclusive employer of choice.

We analyse our separations and reasons staff might choose to leave ASIO.

We apply a diversity and inclusion lens to our recruitment campaigns.

We undertake diversity and inclusion initiatives that contribute to staff engagement, satisfaction and work–life balance.

We incorporate diversity and inclusion into initial induction training.

We provide staff with relevant tools and information to empower them to build inclusive teams and harness diversity.

Management of human resources

Management of human resources

The Thodey Review made key recommendations about the importance of reforming organisational culture and people management processes to achieve enterprise transformation. In 2018–19 we continued to advance these key recommendations by:

- using more agile recruiting models, and improving the management, development and deployment of professional staff and skills; and
- raising digital literacy across the workforce.

We began this process in 2018 while continuing to advance key human resource (HR) initiatives.

Workplace agreement

We continued to operate under our 10th Workplace Agreement, which was agreed in 2016 and expires in 2019. The agreement meets our requirements 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 planning and consultation process for our 11th Workplace Agreement commenced in late 2018, and formal negotiations commenced in June 2019.

We reinstated the Staff Workplace Relations Officer position, which is embedded in Human Resources and helps to ensure effective communication with employees.

Strategic workforce management

We developed and launched the ASIO People Strategy 2019–23, which focuses on our vision for our workforce of 'the right people with the right capabilities, in the right place at the right time, performing to their full potential to achieve organisational objectives'.

This strategy guides our people and strategic workforce initiatives to ensure the Organisation is flexible and forward-looking, in order to identify duplication and create efficiencies; make informed, data-driven decisions on the development (internal) or acquisition (external) of future capabilities; position our Organisation to realise capabilities at the time they are required; and internally reskill or redeploy capabilities as our environmental and technological drivers evolve.

Performance management

We continued to refine our performance framework through the year. We again achieved a 100 per cent rate of compliance for employee participation in the performance cycle, and we shifted to measuring contributions against ASIO's Leadership Charter and employees' broader corporate contribution. A new behavioural indicators tool that identifies examples of leadership behaviours across all levels of the organisation was developed to assist staff in assessing their contribution within the refined performance framework.

Our early intervention initiatives continue to mature as line managers and employees employ our coaching framework and supporting tools to further strengthen our high-performance culture.

Further, we refined our probation procedures, with a focus on organisational suitability and more tailored support for both probationers and line managers. This fortified our recruitment and performance methodology and broader performance framework.

Diversity and inclusion

We continued to embed diversity and inclusion practices in our work. Initiatives included the creation of a diversity and inclusion blog and two new staff-led diversity networks, focusing on Aboriginal and Torres Strait Islander people and an equitable workplace for all genders.

ASIO's gender equity network, AGENda, was officially launched in March 2019. AGENda aims to unlock the potential of the whole organisation by making ASIO equitable for staff regardless of gender. By attracting and retaining a dedicated and diverse workforce, ASIO will be better able to meet the challenges of our increasingly complex mission.

Other diversity and inclusion staff-led networks—focused on cultural heritage, disability and introverts—have been very active this year and are having a positive impact. 'Listen and learn' sessions provided the opportunity for senior leaders to hear firsthand the stories and opportunities of individuals from diverse backgrounds, to continue strengthening our workplaces' inclusiveness. In May 2019 ASIO became the first organisation to achieve silver in the first year of participation in the Australian Workplace Equality Index—Australia's national benchmarking instrument for LGBTI workplace inclusion. ASIO ranked third among federal government agencies and 15th nationwide in a field of 158 entrants.

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

Mudyi—Aboriginal and Torres Strait Islander Staff Network

ASIO's Mudyi Network was formally established in February 2019. Mudyi, which means 'friend' in the Wiradjuri language, is committed to promoting an inclusive workplace culture that values and celebrates ASIO's Aboriginal and Torres Strait Islander staff and culture and their contribution to ASIO's mission.

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 senior management and ASIO Staff Association representatives to discuss the health of the workplace, and provided advice on the development and formulation of our human resources policy.

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 four formal contacts from staff;
- undertaking one preliminary review of investigative matters;
- responding to HR on four policy matter queries;
- undertaking two health checks of business areas; and
- carrying out two investigations relating to the Code of Conduct.

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

In 2018–19 the ASIO Ombudsman did not participate in any work related to public interest disclosures.

ASIO commenced a procurement process to engage the next ASIO Ombudsman.

Asset management

The Ben Chifley Building continued to support the business and capability needs of ASIO and its partners. Our corporate suites, including Australia's largest security-accredited auditorium, hosted a range of events over 2018–19. ASIO continues to collaborate closely with the Australian Federal Police and other key partners on a range of joint accommodation projects.

Procurement

Throughout 2018–19 we adhered to the Commonwealth Procurement Rules and associated policy and guidelines. Our compliance was monitored through our Audit and Risk 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 39 new consultancy contracts involving total actual expenditure of $17.7 million (GST inclusive). In addition, 15 ongoing consultancy contracts were active during the period, involving total actual expenditure of $1.8 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 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; 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 over the life of each contract, is available on request to the PJCIS, which oversees our administration and expenditure.

This incorporates our annual reporting obligations under Public Governance, Performance and Accountability Rule 2014—17AG Information on management and accountability.

Australian National Audit Office access clauses

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 arrangements, contracts and standing offers are available on request to the PJCIS.

This incorporates our annual reporting requirements for Public Governance, Performance and Accountability Rule 2014—17AG Information on management and accountability.

Other mandatory information

Advertising and market research

We spent $1.02 million on advertising in 2018–19, predominantly on recruitment campaigns (see also Appendix G). ASIO does not fall within the definition of agencies covered by the reporting requirements of section 311A of the *Commonwealth Electoral Act 1918*.

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 E provides information on the diversity of our workforce, including statistics on people with a disability.

Information required by another Act or instrument

Archives Act 1983

ASIO is an exempt agency under the *Freedom of Information Act 1982* but is subject to the release of records under the *Archives Act 1983*, which allows public access to Commonwealth records in the 'open period'. In accordance with changes to the Archives Act in 2010, the open period is transitioning from 30 to 20 years and currently covers all Commonwealth records created before 1998. ASIO works closely with the National Archives of Australia in facilitating access to ASIO records, while balancing various and sometimes competing priorities.

In 2018–19, ASIO received 344 applications for access to ASIO records and completed a total of 410 requests, equating to 57 783 folios. Sixty per cent of requests were completed within the 90-day legislative timeframe: despite the completion of longstanding cases, this percentage reflects the higher volume and complexity of assessments.

Table 3: Access to ASIO records

	2016–17	2017–18	2018–19
Applications for record access	480	345	344
Requests completed	485	310	410
Pages assessed	46 997	36 312	57 783
Percentage of requests completed within 90 days	77.8%	66.7%	60%

Australian Security Intelligence Organisation Act 1979

Section 94 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) requires that ASIO's annual report include statements on the Organisation's questioning and questioning and detention warrants, special intelligence operation authorisations, telecommunications data access authorisations, and use of technical assistance requests, technical assistance notices and technical capability notices.

The statement on questioning and questioning and detention warrants is provided at Appendix J. In order to ensure compliance with the determination made by the Minister for Finance under section 105D of the PGPA Act, and to avoid prejudice to ASIO's activities, Appendix K relating to special intelligence operations, Appendix L relating to telecommunications data access authorisations, Appendix M relating to technical assistance requests, technical assistance notices and technical capability notices, and Appendix N relating to the use of special powers under warrant have been removed from the annual report tabled in the Parliament.

These classified appendices will be separately provided to ASIO's minister and, as required by the ASIO Act, to the Leader of the Opposition. Copies of the classified appendices will also be provided to the Attorney-General, Inspector-General of Intelligence and Security, and the Independent National Security Legislation Monitor. Appendix L relating to telecommunications data authorisations will also be provided to the Parliamentary Joint Committee on Intelligence and Security.

Work Health and Safety Act 2011

Schedule 2, Part 4 of the *Work Health and Safety Act 2011* requires non-corporate Commonwealth entities to include in their annual report information on health and safety outcomes and initiatives taken during the reporting period to ensure the health, safety and welfare of workers who carry out work for them.

Our report for 2018–19 is provided at Appendix F.

Commonwealth Electoral Act 1918—advertising and market research

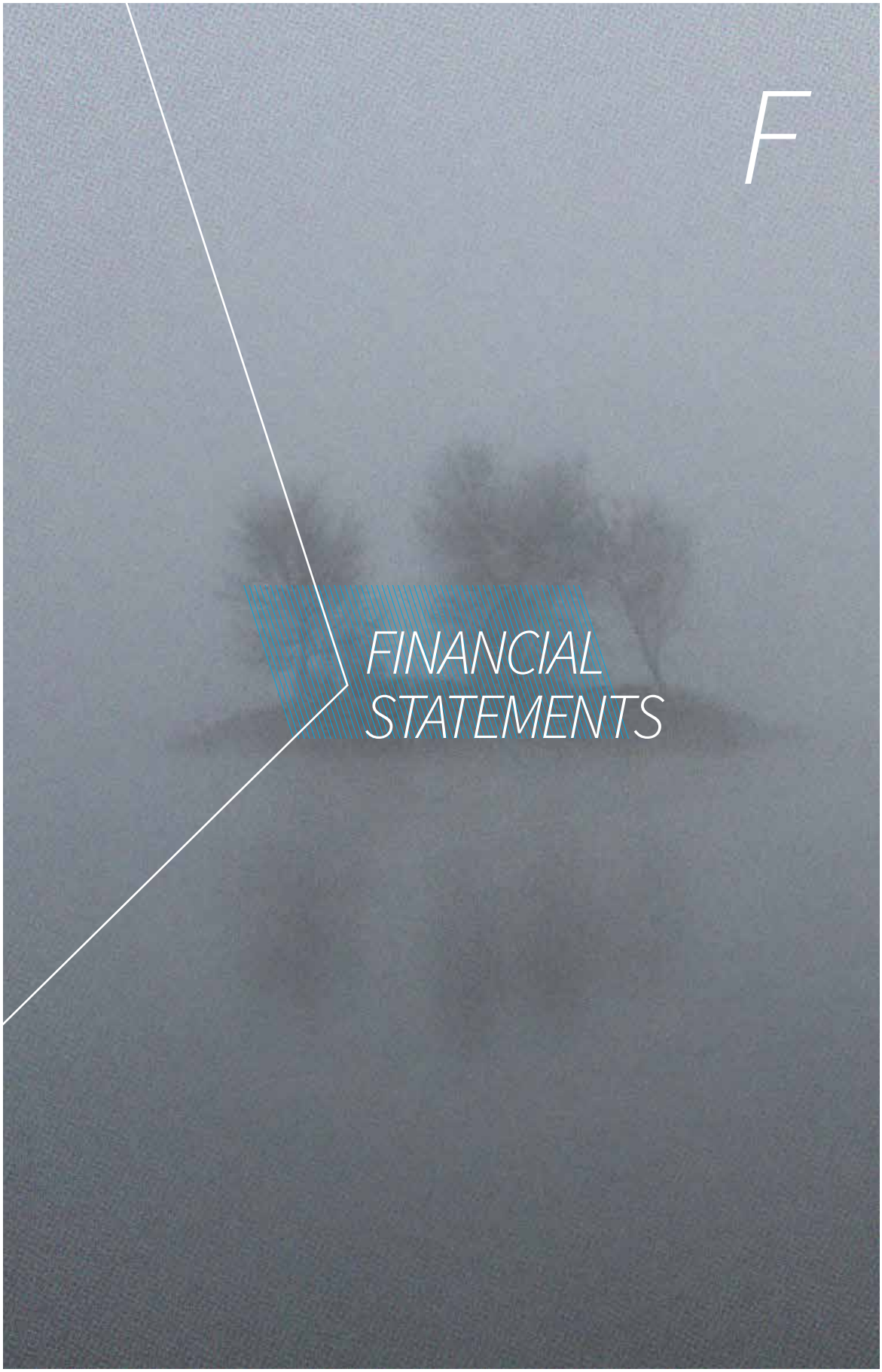
Section 311A of the *Commonwealth Electoral Act 1918* requires annual reporting by each Commonwealth department on amounts paid by, or on behalf of, the Commonwealth department for advertising and market research.

Our report for 2018–19 is provided at Appendix G.

Environment Protection and Biodiversity Conservation Act 1999

Section 516A of the *Environment Protection and Biodiversity Conservation Act 1999* requires Commonwealth entities to report on how the activities of the entity during the period accorded with the principles of ecologically sustainable development.

Our report for 2018–19 is provided at Appendix H.



F

FINANCIAL STATEMENTS

CONTENTS

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

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2019 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

8 August 2019

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 ('the Entity') for the year ended 30 June 2019:

(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 Entity as at 30 June 2019 and its financial performance and cash flows for the year then ended.

The financial statements of the Entity, which I have audited, comprise the following statements as at 30 June 2019 and for the year then ended:

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

Basis for opinion

I conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the Entity 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 Entity, the Director-General of Security is responsible under the *Public Governance, Performance and Accountability Act 2013* (the Act) for the preparation and fair presentation of annual financial statements that comply with Australian Accounting Standards – Reduced Disclosure Requirements and the rules made under the 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 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 ability of the Entity 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 the Director-General of Security 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

Rebecca Reilly
Executive Director

Delegate of the Auditor-General

Canberra
8 August 2019

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2019

	Notes	2019 $'000	Original budget 2019 $'000	2018 $'000
EXPENSES				
Employee benefits	1.1.A	272 077	284 310	248 944
Suppliers	1.1.B	198 646	174 910	199 453
Depreciation and amortisation	2.2.A	104 066	90 937	89 365
Other	1.1.C	1395	-	559
Impairment loss allowance on financial instruments	1.1.D	-	-	7
TOTAL EXPENSES		**576 184**	**550 157**	**538 321**
OWN-SOURCE INCOME				
Revenue				
Sale of services	1.2.A	15 147	21 491	16 494
Other revenue	1.2.B	7300	1739	11 531
Gains	1.2.C	25	145	143
TOTAL OWN-SOURCE INCOME		**22 473**	**23 375**	**28 168**
Net cost of services		***(553 711)***	***(526 782)***	***(510 152)***
REVENUE FROM GOVERNMENT	3.1	**435 196**	**435 845**	**421 767**
DEFICIT ON CONTINUING OPERATIONS		**(118 515)**	**(90 937)**	**(88 385)**
OTHER COMPREHENSIVE INCOME				
Changes in asset revaluation surplus		-	-	36 811
TOTAL COMPREHENSIVE LOSS		**(118 515)**	**(90 937)**	**(51 574)**

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

STATEMENT OF FINANCIAL POSITION
as at 30 June 2019

	Notes	2019 $'000	Original budget 2019 $'000	2018 $'000
ASSETS				
Financial assets				
Cash and cash equivalents	2.1.A	23 517	16 213	23 552
Trade and other receivables	2.1.B	85 894	77 971	70 807
Accrued revenue		575	1734	753
Total financial assets		***109 986***	***95 918***	***95 112***
Non-financial assets				
Prepayments		26 969	21 986	26 919
Land and buildings	2.2.A	145 865	132 775	161 127
Property, plant and equipment	2.2.A	136 412	125 682	146 458
Computer software	2.2.A	57 783	75 974	59 274
Total non-financial assets		***367 029***	***356 417***	***393 778***
TOTAL ASSETS		***477 015***	***452 335***	***488 890***
LIABILITIES				
Payables				
Suppliers	2.3.A	9373	24 033	8829
Other payables	2.3.B	26 637	2665	24 704
Total payables		***36 010***	***26 698***	***33 533***
Provisions				
Employee provisions	2.4.A	91 336	83 796	78 834
Restoration obligations	2.4.B	6794	3786	6072
Total provisions		***98 130***	***87 582***	***84 906***
TOTAL LIABILITIES		**134 140**	**114 280**	**118 439**
NET ASSETS		**342 875**	**338 055**	**370 451**
EQUITY				
Parent equity interest				
Contributed equity		843 097	843 097	752 158
Reserves		69 858	33 046	69 858
Accumulated deficit		(570 080)	(538 087)	(451 565)
TOTAL EQUITY		**342 875**	**338 055**	**370 451**

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

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2019

	2019 $'000	Original budget 2019 $'000	2018 $'000
RETAINED EARNINGS			
Opening balance	(451 565)	(447 150)	(363 172)
Comprehensive income			
Deficit for the period	(118 515)	(90 937)	(88 393)
Closing balance	***(570 080)***	***(538 087)***	**(451 565)**
ASSET REVALUATION RESERVE			
Opening balance	69 858	33 046	33 047
Other comprehensive income			
Changes in asset revaluation surplus	-	-	36 811
Closing balance	***69 858***	***33 046***	**69 858**
CONTRIBUTED EQUITY			
Opening balance	752 158	752 158	668 644
Transactions with owners			
Contributions by owners			
Equity injection—appropriation	5367	5367	14 939
Departmental capital budget	85 572	85 572	68 575
Closing balance	***843 097***	***843 097***	**752 158**
CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT	**342 875**	**338 055**	**370 451**

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 2019

	Notes	2019 $'000	Original budget 2019 $'000	2018 $'000
OPERATING ACTIVITIES				
Cash received				
Appropriations		461 812	435 762	477 892
Sales of services		18 063	18 611	10 498
Net GST received		25 404	20 766	22 083
Other		7155	1693	11 381
Total cash received		***512 434***	***476 832***	**521 854**
Cash used				
Employees		260 102	282 467	245 562
Suppliers		217 985	174 893	220 169
Section 74 receipts		43 188	19 979	30 176
Total cash used		***521 275***	***477 339***	**495 907**
NET CASH USED BY OPERATING ACTIVITIES		**(8841)**	**(507)**	**25 947**
INVESTING ACTIVITIES				
Cash received				
Proceeds from sales of property, plant and equipment		709	-	948
Total cash received		***709***	-	**948**
Cash used				
Purchase of property, plant and equipment		41 183	50 928	55 244
Purchase of computer software		38 057	40 587	32 553
Total cash used		***79 240***	***91 515***	**87 797**
NET CASH USED BY INVESTING ACTIVITIES		**(78 531)**	**(91 515)**	**(86 849)**
FINANCING ACTIVITIES				
Cash received				
Contributed equity		87 337	90 939	67 116
Total cash received		***87 337***	***90 939***	**67 116**
NET CASH FROM FINANCING ACTIVITIES		**87 337**	**90 939**	**67 116**
Net increase (decrease) in cash held		(35)	(1083)	6214
Cash and cash equivalents at the beginning of the reporting period	2.1.A	23 552	17 296	17 338
CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD		**23 517**	**16 213**	**23 552**

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); and
- Australian Accounting Standards and Interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial statements have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets and liabilities at fair value. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position. The financial statements are presented in Australian dollars.

New accounting standards

ASIO adopted AASB 9 Financial Instruments which became effective during 2018–19. The application did not materially impact the financial statements of ASIO. Refer to note 4.2 for further information.

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

	2019 $'000	2018 $'000
1.1 EXPENSES		
1.1.A Employee benefits		
Wages and salaries	205 231	195 219
Superannuation		
Defined contribution plans	20 631	17 915
Defined benefit plans	15 606	15 117
Leave and other entitlements	30 423	20 361
Separation and redundancies	186	332
Total employee benefits	**272 077**	**248 944**
1.1.B Suppliers		
Goods supplied	7704	8702
Services supplied	147 421	146 582
Operating lease payments	42 674	42 239
Workers' compensation premiums	847	1930
Total supplier expenses	**198 646**	**199 453**

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 a review based on the consumer price index and market appraisal.

Commitments are GST-inclusive where relevant.

Commitments for minimum lease payments are payable:		
Within 1 year	54 587	53 793
Between 1 to 5 years	215 101	213 380
More than 5 years	254 031	312 641
Total operating lease commitments	***523 719***	***579 813***
1.1.C Other expenses		
Finance costs: unwinding of discount—restoration obligations	739	124
Write-down and impairment of property, plant and equipment	539	419
Losses from asset sales	117	16
Total other expenses	**1395**	**559**
1.1.D Impairment loss allowance on financial instruments		
Impairment of receivables	-	7
Total impairment on financial instruments	**-**	**7**

	2019	2018
	$'000	$'000

1.2 OWN-SOURCE REVENUE AND GAINS

1.2.A Sale of services	**15 147**	**16 494**

Accounting policy

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	6015	10 297
Resources received free of charge—remuneration of auditors	145	150
Royalties	1	8
Other	1139	1076
Total other revenue	**7300**	**11 531**

Sub-lease rental income commitments

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

Commitments for rental income are receivable:

Within 1 year	3797	2722
Between 1 to 5 years	16 607	9318
More than 5 years	15 606	9196
Total rental income commitments	***36 010***	***21 236***

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

Other gains	25	143
Total gains	**25**	**143**

Accounting policy

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

2. Financial position

	2019 $'000	2018 $'000
2.1 FINANCIAL ASSETS		
2.1.A Cash and cash equivalents	**23 517**	**23 552**

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	**4543**	7615
Appropriation receivable	**77 623**	57 449
GST receivable	**3728**	5743
Total trade and other receivables	**85 894**	**70 807**

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

Credit terms for goods and services were within 30 days (2018: 30 days).

Financial assets were assessed for impairment at 30 June 2019. No indicators of impairment have been identified.

Accounting policy

Trade receivables are:

- held for the purpose of collecting contractual cash flows where the cash flows are solely payments of principal and interest and not provided at below-market interest rates;
- adjusted on initial measurement for expected credit losses; and
- subsequently measured at amortised cost using the effective interest method adjusted for any loss allowance.

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 2018					
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 1 July 2018	***6410***	***154 717***	***146 458***	***59 274***	***366 859***
Additions by purchase	219	830	39 306	30 882	71 237
Additions—internally developed	-	-	-	7395	7395
Depreciation and amortisation expense	(374)	(15 937)	(48 020)	(39 735)	(104 066)
Disposals—other	-	-	(1332)	(33)	(1365)
Net book value 30 June 2019	**6255**	**139 610**	**136 412**	**57 783**	**340 060**
Gross book value	6692	160 024	192 148	179 628	538 492
Accumulated depreciation, amortisation and impairment	(437)	(20 414)	(55 736)	(121 845)	(198 432)
Net book value 30 June 2019	**6255**	**139 610**	**136 412**	**57 783**	**340 060**

Computer software

The carrying value of computer software included $29.131 million (2018: $23.844 million) purchased software and $28.652 million (2018: $35.430 million) 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	-	-	4295	4861	9156
Between 1 to 5 years	-	-	974	715	1689
Total capital commitments	***-***	***-***	***5269***	***5576***	***10 845***

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

Depreciation rates (useful lives), residual values and methods are reviewed at each reporting date. Depreciation rates applying to each class of depreciable asset are based on the following useful lives:

	2019	2018
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 2019. 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 (2018: 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.

ASIO engaged the services of Jones Lang Lasalle (JLL) 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. An annual assessment as at reporting date determined the carrying amount of the assets is not materially different from the fair value.

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 Current Replacement Cost approach. Under the Current 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 2019 are detailed above in Note 2.2.A.

	2019	2018
	$'000	$'000
2.3 PAYABLES		
2.3.A Suppliers		
Trade creditors and accruals	**9373**	8829
Total suppliers	**9373**	**8829**

Settlement is usually made within 30 days.

2.3.B Other payables		
Salaries	**1854**	1905
Superannuation	**275**	263
Unearned income	**1119**	2092
Amortisation of rent expense	**21 269**	17 769
Lease incentives	**490**	556
Fringe benefits tax	**1630**	2119
Total other payables	**26 637**	**24 704**
2.4 PROVISIONS		
2.4.A Employee provisions		
Leave	**91 336**	78 834
Total employee provisions	**91 336**	**78 834**

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 12 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 employees' superannuation schemes 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.

	2019	2018
	$'000	$'000
2.4.B Restoration obligations	**6794**	**6072**
Carrying amount 1 July 2018	6072	4938
Reduction in value	(17)	-
Unwinding of discount or change in discount rate	739	124
Revaluation as at 30 June	-	1010
Closing balance	***6794***	***6072***

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
2019			
Appropriation Act			
Annual appropriation[1]	**435 196**	85 572	5367
PGPA Act			
Section 74 transfers	**43 188**	-	-
Total appropriation	**478 384**	**85 572**	**5367**
Appropriation applied (current and prior years)	**(450 183)**	(80 572)	(6765)
Variance	***28 201***	***5000***	***(1398)***

[1] $0.649 million (net) was returned to Government due to new government measures after original budget and in accordance with section 51 of the PGPA Act.

Operating appropriation remains unspent in 2019 due to the timing of supplier purchases.

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: $8.014 million (2018: $8.029 million).

2018			
Appropriation Act			
Annual appropriation	421 767	68 575	14 939
PGPA Act			
Section 74	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***

The 2018 operating appropriation variances were due to prior year appropriations applied in 2018. Capital appropriations were unspent due to the timing of asset purchases.

	2019	2018
	$'000	$'000
3.1.B Unspent departmental annual appropriations (recoverable GST exclusive)		
Appropriation Act (No. 1) 2016–17	-	22
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
Appropriation Act (No. 1) 2018–19	**96 140**	**-**
Appropriation Act (No. 2) 2018–19	**5000**	**-**
Total	**101 140**	**81 023**

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	**(14 449)**	**972**
Depreciation and amortisation	(104 066)	(89 365)
Deficit as per statement of comprehensive income	(118 515)	(88 393)

F

4. Managing uncertainties

	2019 $'000	2018 $'000
4.1 CONTINGENT ASSETS AND LIABILITIES		
Quantifiable contingencies		
ASIO's contingent liabilities relate to claims for damages or costs. The amount represents an estimate of ASIO's liability based on precedent in such cases. ASIO is defending the claims.		
Contingent liabilities		
Balance from previous period	60	-
New contingent liabilities recognised	-	60
Liabilities realised	(60)	-
Total contingent liabilities	**-**	**60**

Unquantifiable contingencies

At 30 June 2019, ASIO had a number of legal claims against it. ASIO has denied liability and is defending the claims. It is not possible to estimate amounts of any eventual payments that may be required in relation to these claims.

Accounting policy

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

4.2 FINANCIAL INSTRUMENTS		
4.2.A Categories of financial instruments		
Financial assets under AASB 139		
Loans and receivables		
Cash	-	23 552
Trade receivables	-	7615
Accrued revenue	-	753
Financial assets under AASB 9		
At amortised cost		
Cash	23 517	-
Trade receivables	4543	-
Accrued revenue	575	-
Total financial assets	**28 635**	**31 920**
Financial liabilities		
At amortised cost		
Trade creditors and accruals	9373	8829
Total financial liabilities	**9373**	**8829**

Classification of financial assets on the date of initial application of AASB 9

	Note	AASB 139 original classification	AASB 9 new classification	AASB 139 carrying amount at 1 July 2018 $'000	AASB 9 carrying amount at 1 July 2018 $'000
Cash	2.1.A	Loans & receivables	Amortised cost	23 552	23 552
Trade receivables	2.1.B	Loans & receivables	Amortised cost	7615	7615
Accrued revenue		Loans & receivables	Amortised cost	753	753
Total financial assets				**31 920**	**31 920**

The net fair values 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 2019 was the impairment of trade receivables.

Accounting policy

Financial assets

With the implementation of AASB 9 Financial Instruments for the first time in 2019, ASIO classifies its financial assets as 'measured at amortised cost'. Financial assets included in this category must meet two criteria:

- the financial asset is held in order to collect the contractual cash flows; and
- the cash flows are solely payments of principal and interest on the principal outstanding amount.

Amortised cost is determined using the effective interest method, with income recognised on an effective interest rate basis.

Financial assets are recognised when ASIO becomes party to a contract and, as a consequence, has a legal right to receive or obligation to pay cash and derecognised when the contractual rights to the cash flows from the financial asset expire or are transferred upon trade date.

Comparatives have not been restated on initial application.

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 assets are assessed for impairment at the end of each reporting period based on an amount equal to the lifetime expected credit losses. A write-off directly reduces the gross carrying amount of the financial asset.

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

	2019	2018
	$'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	1975	1737
Long-term employee benefits	265	120
Post-employment benefits	334	276
Total key management personnel remuneration expenses[1]	**2574**	**2133**

The number of key management positions is 5 (2018: 4).

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 2018–19 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 expenses were $22.75 million in 2018–19.

5.3 MAJOR BUDGET VARIANCES

The following provides an explanation of variances between the original budget as presented in the 2018–19 Portfolio Budget Statements (PBS) and the 2018–19 final actual result. The budget is not audited. Explanations are provided for major budget variances only. Variances are treated as major when it is considered important for the reader's understanding or is relevant to an assessment of the discharge of accountability and to an analysis of ASIO's performance.

The nature and timing of the Commonwealth's budget process can also contribute to the variances. ASIO's major budget impacts include:

- Estimated actual outcomes were published in the 2018–19 PBS before the closing 2017–18 and opening 2018–19 statement of financial position was known. Therefore, the opening balances of the statement of financial position were estimates.
- The original budget as presented in the 2018–19 PBS is amended by Government throughout the year. ASIO's budget for 2018–19 was updated as part of the 2018–19 Mid-Year Economic Fiscal Outlook (MYEFO) and again as part of the 2019–20 PBS process where estimated actuals for 2018–19 are presented as comparatives for the 2019–20 budget figures.

Expenses

The total variance between expenses and the original budget is an increase of $26.027 million (5%). The overall increase is due to:

- employee benefits which were $12.233 million lower than original budget due to the growth in the number of employees being less than anticipated and the timing of recruitment being towards the end of the financial year;
- supplier expenses which were $23.736 million higher than the original budget as a result of the engagement of expert consultants/contractors to progress the review of ASIO's technology state and business reform planning; and
- depreciation and amortisation expenses which were $13.129 million higher than original budget due to the 2017–18 revaluation of fixed assets post budget development which increased the carrying value of property, plant and equipment and buildings.

Income

Income is $1.552 million (0.3%) lower than original budget. The decrease is due to:

- a reduction of $0.649 million in appropriation funding as a result of new Government decisions;
- an increase in other revenue of $5.561 million relating to rental income. The vacation of a sub-tenant was uncertain at the time of the budget development and was ultimately delayed until September 2018. Income relating to the sub-leasing of office premises was unknown at the time of budget preparation; and
- revenue from the sale of services was $6.344 million less than budget. This budget is dependent on requests and activities undertaken by external parties which was less than anticipated. The introduction of a flexible cost recovery model for protective security activities has resulted in a fluctuation in revenue generation which was not reflected in the budget.

Assets

Total assets are $24.680 million higher (5%) than original budget. Financial assets are $14.068 million higher than budget, largely due to the difference between the actual and budgeted opening balances. These funds form part of the receivables balance and will be available in 2019–20.

Non-financial assets are $10.611 million higher than original budget as a result of:

- the difference in the opening actuals balance in July 2018 compared to the original budget set in May 2018 of $32.430 million. This is offset by higher depreciation expense, in part as a result of the 2017–18 revaluation exercise; and
- an increase in prepayments of $4.983 million due to a number of multi-year prepayments for IT software contracts which were not anticipated in the original budget.

Liabilities

Total liabilities are $19.860 million higher (17%) than original budget. The increase is attributed to:

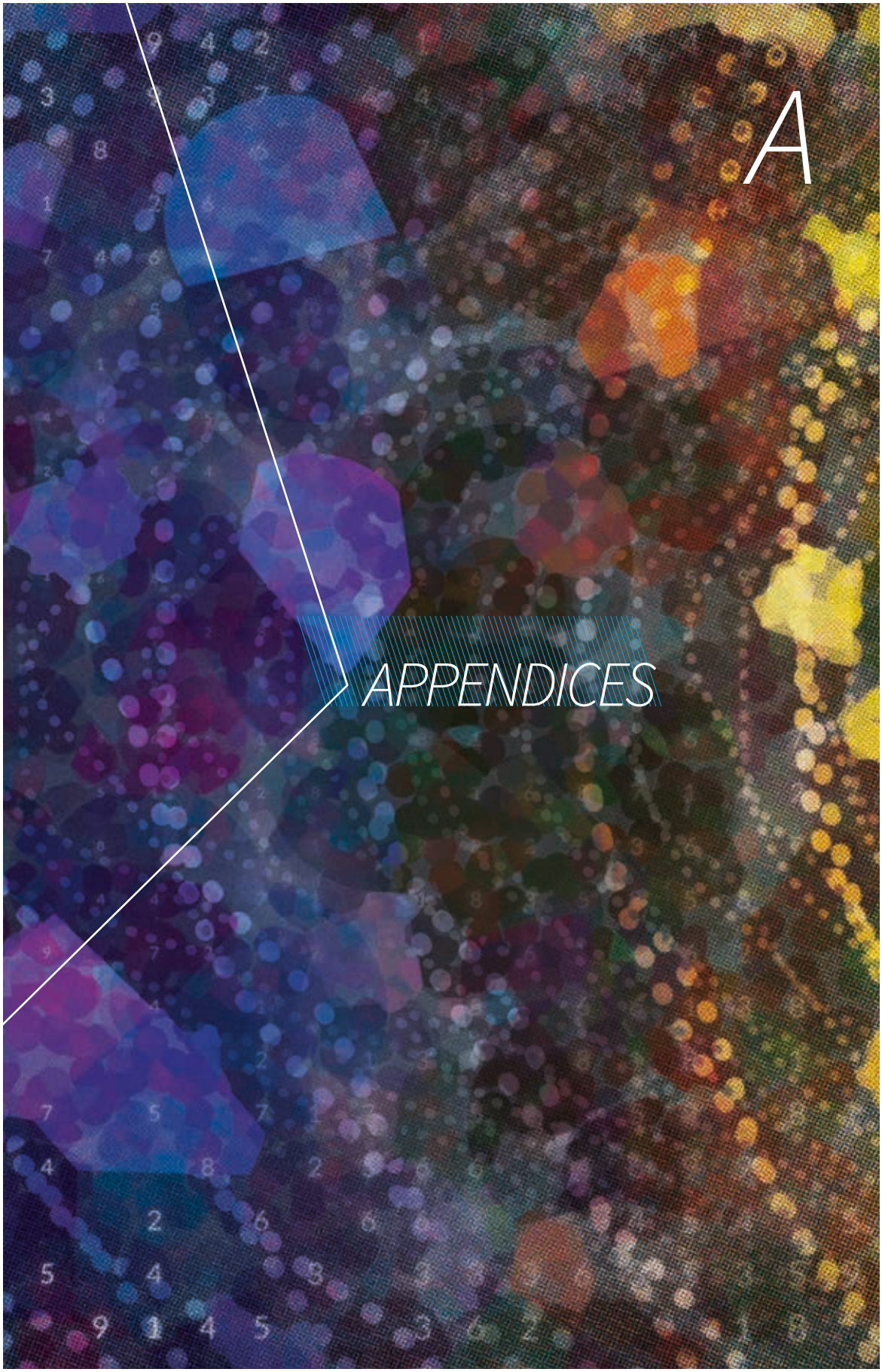
- an increase to provisions for rent amortisation due to the stage of leases. Potential changes were not factored into the original budget;
- an increase of $7.540 million in employee provisions due to a decrease in the discount rate used to calculate the provision; and
- an increase to the provision for restoration obligations due to the 2017–18 revaluation which was finalised post budget development.

Statement of changes in equity

Total equity is over budget by $4.820 million due to differences between the actual and budgeted opening balances.

Statement of cash flows

The amounts reported in the statement of cash flows are interrelated with figures disclosed in the statement of comprehensive income and statement of financial position. Consequently, cash flow variances are attributable to the relevant variance explanations provided above.


A
APPENDICES

Appendix A: agency resource statement

	Actual available appropriation 2019 $'000	Payments made 2019 $'000	Balance remaining 2019 $'000
ORDINARY ANNUAL SERVICES[1]			
Departmental appropriation			
Prior year appropriation[2]	51 051	51 051	-
2018–19 appropriation	435 196*	387 636	47 560
Section 74 relevant agency receipts[3]	43 188	38 125	5063
2018–19 capital budget	85 572*	65 572	20 000
Cash on hand	23 552	35	23 517
Total ordinary annual services	***638 559***	***542 419***	***96 140***
OTHER SERVICES			
Departmental non-operating[4]			
Equity injections	5367*	367	5000
Total other services	***11 765***	***6765***	***5000***
TOTAL NET RESOURCING AND PAYMENTS FOR ASIO	**650 324**	**549 184**	

[1] Appropriation Act (No. 1) and Appropriation Act (No. 3).

[2] Includes an amount of $15.0m from 2017–18 for the Departmental Capital Budget.

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

[3] $21.283m per Portfolio Budget Statement plus $21.905m underestimate at time of PBS.

[4] Appropriation Act (No. 2) and Appropriation Act (No. 4).

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

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* 2019 $'000	Actual expenses 2019 $'000	Variation 2019 $'000
Program 1.1: Security Intelligence			
Departmental expenses			
Appropriation[1]	435 196	435 196	-
Expenses not requiring appropriation in the budget year	104 211	91 082	(13 129)
Total for Program 1.1	***539 407***	***526 278***	***(13 129)***
Total expenses for Outcome 1	**539 407**	**526 278**	**(13 129)**

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

[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

Information about remuneration for key management personnel

		Short-term benfits			Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration
Name	Position title	Base salary[1] $	Bonuses $	Other benefits and allowances $	Superannuation contributions $	Long service leave[2] $	Other long-term benefits $	$	$
Duncan Lewis	Director-General[3]	534 013	0	43 821	96 638	129 492	0	0	803 964
Heather Cook	Deputy Director-General	389 093	0	5 039	66 178	37 257	0	0	497 566
Wendy Southern	Deputy Director-General[4]	428 269	0	5039	63 962	10 940	0	0	508 210
Peter Vickery	Deputy Director-General	337 133	0	36 809	64 066	54 845	0	0	492 852
Name witheld[5]	Chief Transformation Officer[6]	213 327	0	25 133	44 162	33 611	0	0	316 234

[1] Includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*.

[2] Does not represent one year's leave accrual at officer's current salary. Value is in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*. This may result in a negative leave figure where an officer resigns during the year and leave is paid out on termination.

[3] The remuneration in this table differs from that shown in *Remuneration Tribunal (Remuneration and Allowances for Holders of Full-time Public Office) Determination 2018* because the Department of Finance (in *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports*) specifies a different basis of determining the value of annual and long service leave, and superannuation.

[4] The remuneration in this table differs from that disclosed in ASIO's financial statements as at 30 June 2019. Additional information was received from the secondee's home agency after the financial statements were finalised.

[5] ASIO Chief Transformation Officer (CTO) is a non-declared officer. To comply with section 92 of the *ASIO Act 1979* and the determination issued to ASIO under Section 105D of the *Public Governance Performance and Accountability Act 2013*, the CTO's name has not been provided in the annual report.

[6] 1 July 2018 to 27 April 2019.

Information about remuneration for senior executives

		Short-term benfits			Post- employment benefits	Other long-term benefits		Termination benefits	Total remuneration
Remuneration band	Number of senior executives	Average base salary[1] $	Average bonuses $	Average other benefits and allowances $	Average superannuation contributions $	Average long service leave[2] $	Average other long-term benefits $	Average termination benefits $	Average total remuneration $
$0 to $220 000	26	71 192	0	3115	11 771	-2783	0	0	83 294
$220 001 to $245 000	4	174 073	0	3976	23 108	28 336	0	0	229 492
$245 001 to $270 000	5	194 800	0	14 070	39 407	13 557	0	0	261 832
$270 001 to $295 000	12	218 667	0	12 029	39 554	17 429	0	0	287 679
$295 001 to $320 000	21	219 918	0	14 107	39 488	31 429	0	0	304 941
$320 001 to $345 000	5	247 008	0	16 375	41 281	27 323	0	0	331 987
$345 001 to $370 000	4	265 046	0	11 549	51 638	30 789	0	0	359 021
$370 001 to $395 000	4	286 906	0	18 497	48 746	25 037	0	0	379 187
$420 001 to $445 000	1	327 316	0	30 732	52 477	28 683	0	0	439 208
$445 001 to $470 000	1	362 375	0	9206	53 882	26 138	0	0	451 602
$495 001 to $520 000	1	397 984	0	44 527	41 425	27 276	0	0	511 212

[1] Includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports.*

[2] Does not represent one year's leave accrual at officer's current salary. Value is in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports.* This may result in a negative leave figure where an officer resigns during the year and leave is paid out on termination.

Information about remuneration for other highly paid staff

		Short-term benfits			Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration
Remuneration band	Number of highly paid staff	Average base salary[1] $	Average bonuses $	Average other benefits and allowances $	Average superannuation contributions $	Average long service leave[2] $	Average other long-term benefits $	Average termination benefits $	Average total remuneration $
$220 001 to $245 000	30	178 139	0	4671	29 096	20 708	0	0	232 615
$245 001 to $270 000	7	202 495	0	5574	30 526	17 538	0	0	256 134
$270 001 to $295 000	7	228 563	0	10 067	27 549	19 057	0	0	285 236
$295 001 to $320 000	2	251 163	0	2395	29 013	15 104	0	0	297 675
$320 001 to $345 000	3	249 993	0	43 053	29 411	11 327	0	0	333 784
$345 001 to $370 000	2	293 604	0	28 477	27 064	14 146	0	0	363 291
$420 001 to $445 000	1	339 869	0	51 019	29 375	10 873	0	0	431 136

[1] Includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports.*

[2] Does not represent one year's leave accrual at officer's current salary. Value is in accordance with Department of Finance requirements: *Resource management guide no. 138 Commonwealth entities executive remuneration reporting guide for annual reports.* This may result in a negative leave figure where an officer resigns during the year and leave is paid out on termination.

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 2019. 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: workforce statistics

Full-time equivalent actual

2017–18	**1814.9**
2018–19	**1876.6**

Head count of staff by load and employment status

	2017–18			2018–19		
	Ongoing	**Non-ongoing**	**Total**	**Ongoing**	**Non-ongoing**	**Total**
Full-time	1640	10	**1650**	1681	9	**1690**
Part-time	260	21	**281**	280	16	**296**
Total	**1900**	**31**	**1931**	**1961**	**25**	**1986**

Notes:
- Data includes the Director-General.
- Non-ongoing employees do not include locally engaged staff and secondees.
- Non-ongoing employees data reported in the 2018–19 annual report does not include casuals, as per Department of Finance requirements. The data reported in the 2017–18 annual report includes casuals.

Head count of staff by gender and employment status

	2017–18			2018–19		
	Ongoing	**Non-ongoing**	**Total**	**Ongoing**	**Non-ongoing**	**Total**
Female	882	8	**890**	918	6	**924**
Male	1018	23	**1041**	1043	19	**1062**
Total	**1900**	**31**	**1931**	**1961**	**25**	**1986**

Notes:
- Data includes the Director-General.
- Non-ongoing employees do not include locally engaged staff and secondees.
- Non-ongoing employees data reported in the 2018–19 annual report does not include casuals, as per Department of Finance requirements. The data reported in the 2017–18 annual report includes casuals.

Head count of employees by classification and employment status

		2017–18			2018–19		
		Ongoing	Non-ongoing	Total	Ongoing	Non-ongoing	Total
Senior Executive Service	Director-General	1	0	**1**	1	0	**1**
	SES Band 3	4	0	**4**	4	0	**4**
	SES Band 2	12	0	**12**	13	0	**13**
	SES Band 1	37	2	**39**	46	1	**47**
Senior officers	AEE2/3	187	5	**192**	185	3	**188**
	AEE1	407	5	**412**	483	5	**488**
Employees	AE1 to AE6 (including technical specialists)	1252	19	**1271**	1229	16	**1245**

Notes:
- Data includes the Director-General.
- Non-ongoing employees do not include locally engaged staff and secondees.
- Non-ongoing employees data reported in the 2018–19 annual report does not include casuals, as per Department of Finance requirements. The data reported in the 2017–18 annual report includes casuals.

A

Head count of employees by location and employment status

	2017–18			2018–19		
	Ongoing	Non-ongoing	Total	Ongoing	Non-ongoing	Total
Canberra-based	1358	23	**1381**	1413	18	**1431**
Other locations	542	8	**550**	548	7	**555**

Notes:
- Data includes the Director-General.
- Non-ongoing employees do not include locally engaged staff and secondees.
- Non-ongoing employees data reported in the 2018–19 annual report does not include casuals, as per Department of Finance requirements. The data reported in the 2017–18 annual report includes casuals.
- In order to avoid prejudice to ASIO's activities, a detailed breakdown of ASIO employee locations in Australian states and territories outside Canberra and overseas has not been provided in the annual report tabled in parliament. A figure for the total number of employees located outside Canberra is provided at 'Other locations'.

Diversity of ASIO employees showing head count and percentage

	2017–18		2018–19	
Available data	1816	92.5%	1883	94.8%
Identify as Indigenous	9	0.5%	7	0.4%
People with a disability	20	1.1%	21	1.1%
Non-English-speaking background	330	18.2%	362	19.2%

Notes:

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

Appendix F: work health and safety

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

A strategic review of health and safety programs and performance undertaken in 2016–17 has guided improvements to systems and governance arrangements. In particular, we reformed our consultative safety governance framework to improve safety risk outcomes across the business. We are leveraging these arrangements to align our safety risk management strategies and procedures, which will reinforce our ongoing compliance with and commitment to continual improvement.

Consistent with the *Work Health and Safety Act 2011* and the *Safety, Rehabilitation and Compensation Act 1988*, we have a preventative and early intervention approach to managing compensation and rehabilitation. We have reduced our workers compensation premium, while ensuring quality rehabilitation assistance for staff. No areas of non-compliance were identified in 2018–19, and we continued to enhance processes and maintain a positive relationship with Comcare.

We provided programs to support the physical and psychological health and safety of our staff. Our health and wellbeing program delivered cost-effective prevention initiatives, including an annual influenza vaccination program, a visual health initiative and mental health awareness activities.

In line with legislated notification obligations, ASIO reported one incident to Comcare in 2018–19. Comcare subsequently confirmed the incident was appropriately investigated and resolved. No notices were issued to ASIO under the *Work Health and Safety Act 2011*.

Appendix G: advertising and market research

Recruitment

We are committed to developing and implementing strategies to attract and select the right people at the right time for ASIO. In 2018–19 we had a greater focus on outreach to various markets and universities in combination with tailored marketing and advertising, in particular for non–intelligence related roles. At the time of reporting, ASIO had expended $975 556 towards marketing and advertising for recruitment activities and campaigns in the 2018–19 financial year.

We continue to partner closely with universities in Science, Technology, Engineering and Mechanics (STEM)–related fields to increase our technical capability through our Future Technologist Graduate Program. The entry-level Information Technology and Information Management traineeships provide an additional pathway for school leavers into the technology field in ASIO.

The dynamic labour market and the lengthy timeframes involved in recruiting staff for employment in our high-security work environment remain a challenge for ASIO. That said, work continued in 2018–19 to review and enhance processes to respond to these challenges. In 2019–20 we will seek to expand our graduate programs and introduce a corporate stream to provide a career pathway in functions such as finance, human resources, procurement and legal.

Non-intelligence roles remain an integral part of our recruitment focus, to provide support and partnerships to our core intelligence functions.

This entry also addresses subsection 17AH(1)(a) 'Other mandatory information' of the Public Governance, Performance and Accountability Rule 2014.

Appendix H: ecologically sustainable development and environmental performance

Environmental performance

ASIO is committed to reducing its carbon footprint and improving environmental performance.

In 2018–19 we achieved the following:

- reduced ASIO's total energy consumption by 255 853 kilowatt hours through the use of solar panels, saving approximately $38 500 and 234.8 tonnes of carbon emissions;
- used 15 054 kilolitres of captured stormwater for irrigation and toilet flushing, reducing reliance on potable and bore water and saving approximately $74 000 of potable water;
- used 1793 kilolitres of bore water for irrigation and toilet flushing, reducing reliance on potable water and saving approximately $8373 of potable water;
- recycled 12 612 kilograms of waste, including paper products, printer toner cartridges, batteries, scrap metal and fluorescent tubes;
- participated in the 12th consecutive Earth Hour event; and
- reduced our consumption of grid electricity through energy-saving initiatives, including
  - a 3.2 per cent reduction in energy consumption compared with the previous financial year—a saving of 828 000 kilowatt hours
  - the conversion of car park lighting to LED luminaires
  - improved Uninterrupted Power Supply efficiency through matching building loads, which reduces energy consumption
  - the fine tuning of the Building Management Control Systems, reducing air-conditioning energy and potable water consumption.

Appendix I: 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 previous term of appointment expired on 1 September 2018. He was reappointed for a further term of two years expiring on 26 March 2021.

The Independent Reviewer's terms of reference and other relevant information 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 thereafter while the individual remains in detention and ineligible to hold a visa because they are subject of an adverse security 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.

As at 30 June 2019, the Independent Reviewer had two adverse security assessments under consideration.

Appendix J: 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 questioning and detention warrants during the reporting period. The details are provided in the following table.

Subsection	Description	2016–17	2017–18	2018–19
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	0
94(1)(b)	The total number of warrants issued under that division during this reporting period	0	0	0
94(1)(c)	The total number of warrants issued under section 34E during this reporting period	0	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	0
94(1)(e)	The total number of warrants issued under section 34G during this reporting period	0	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	0
94(1)(f)(ii)	The number of hours each person spent in detention under such a warrant during this reporting period	0	0	0
94(1)(f)(iii)	The total of all those hours for all those persons during this reporting period	0	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	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 Act 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 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 of the entity**		
	Annual performance statements		
17AD(c)(i); 16F	Annual performance statement in accordance with paragraph 39(1)(b) of the PGPA Act and section 16F of the PGPA Rule.	Mandatory	Part 4
17AD(c)(ii)	***Report on financial performance***		
17AF(1)(a)	A discussion and analysis of the entity's financial performance	Mandatory	Part 4
17AF(1)(b)	A table summarising the entity's total resources and total payments	Mandatory	Appendices A and B
17AF(2)	If there may be significant changes in the financial results during or after the previous or current reporting period, information on those changes are provided, including: the cause of any operating loss of the entity; how the entity has responded to the loss and the actions that have been taken for 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)	A 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 operations of the entity	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)(a)(a)	Statistics on the entity's 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 E

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

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

PGPA Rule reference	Description	Requirement	Part of this report
	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 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
	Executive remuneration		
17AD(da)	Information about executive remuneration in accord with Subdivision C of Division 3A of part 2-3 of the Rule	Mandatory	Appendix C
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 and Appendix G
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

PGPA Rule reference	Description	Requirement	Part of this report
17AH(1)(d)	Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found	Mandatory	N/A (FOI exempt)
17AH(1)(e)	Correction of material errors in the previous annual report	If applicable, mandatory	
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 and questioning and detention warrants; special intelligence operation authorities; authorisations for access to telecommunications data; technical assistance requests, technical assistance notices and technical capability notices; and special powers under warrant.

Requirement	Refer to
Statement on use of questioning warrants and questioning and detention warrants	Appendix J
Statement on use of special intelligence operation authorities	Appendix K
Statement on use of authorisations for access to telecommunications data	Appendix L
Statement on use of technical assistance requests, technical assistance notices and technical capability notices	Appendix M
Statement on use of special powers under warrant	Appendix N

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 K, L, M and N have been deleted from the version of the annual report tabled in parliament to avoid prejudice to ASIO's activities.

Abbreviations and short forms

A

AASB—Australian Accounting Standards Board

AASB 9—Australian Accounting Standards Board Standard 'Financial Instruments'

AASB 119—Australian Accounting Standards Board Standard 'Employee Benefits'

AAT—Administrative Appeals Tribunal

ACSC—Australian Cyber Security Centre

ADIC—ASIO Diversity and Inclusion Committee

AE—ASIO employee

AEE—ASIO executive employee

AFP—Australian Federal Police

AGSVA—Australian Government Security Vetting Agency

ANZCTC—Australia-New Zealand Counter-Terrorism Committee

APS—Australian Public Service

ARC—Audit and Risk Committee

ASIC—Aviation Security Identification Card

ASIO Act—*Australian Security Intelligence Organisation Act 1979*

ASIO—Australian Security Intelligence Organisation

ASIO–T4—ASIO's Protective Security Directorate

AUSTRAC—Australian Transaction Reports and Analysis Centre

B

BGLU—Business and Government Liaison Unit

C

CIC—Critical Infrastructure Centre

CPAG—Crowded Place Advisory Group

D

DCB—Departmental Capital Budget

DISP—Defence Industry Security Program

E

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

F

FC—Finance Committee

FIRB—Foreign Investment Review Board

G

GST—Goods and Services Tax

H

HR—Human Resources

I

IC—Intelligence Committee

IE—intelligence employees

IGIS—Inspector-General of Intelligence and Security

INSLM—Independent National Security Legislation Monitor

ISIL—Islamic State of Iraq and the Levant

ITE—information technology employee

J

L

LGBTI—lesbian, gay, bisexual, transgender, intersex

M

MSIC—Maritime Security Identification Card

N

NCFIC—National Counter Foreign Interference Coordinator

NIC—National Intelligence Community

NTAC—National Threat Assessment Centre

NV—'Negative vetting' security clearance

O

P

PBS—Portfolio Budget Statement

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

PJCIS—Parliamentary Joint Committee on Intelligence and Security

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

STEM—Science, Technology, Engineering and Mechanics

T

TOLA Act—*Telecommunications and Other Legislation Amendment Act 2018*

TSSR—Telecommunications Sector Security Reforms

U

W

WC—Workforce Committee

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.

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.

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

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

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

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

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

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

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

qualified security assessment—ASIO does not make a prejudicial recommendation but does communicate information, an opinion or advice that is, or could be, prejudicial to the interests of the person in relation to the contemplated prescribed administrative action.

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

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

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

A

Index

A