UNCLASSIFIED

Australian Government
Australian Security Intelligence Organisation

ASIO submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure

No. 18 2018–19

www.asio.gov.au

S&P

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.

Contents

Scope of the review

The Australian Security Intelligence Organisation (ASIO) submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of Administration and Expenditure No. 18 provides a detailed account of ASIO's administration and budgetary activities during the 2018–19 financial year. The submission addresses specific information requests from the PJCIS, as set out in the inquiry's terms of reference (refer to **Appendix A**).

To place the administrative and budgetary information within its context, the submission includes an overview of the security environment.

Introduction

This reporting period marks the 70th anniversary of ASIO's founding. 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. Since then, ASIO has evolved into a workforce of nearly 2000 people, with officers located across Australia and the world.

The one constant over the past 70 years has been ASIO's resolute focus on protecting Australia, its people and its interests from those who wish us harm. This financial year has been another year of high operational tempo, where ASIO has again been at the forefront of confronting Australia's national security challenges.

ASIO'S ROLE AND FUNCTIONS

ASIO's purpose is to protect Australia, its people and its interests from threats to security. 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.

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

What we do

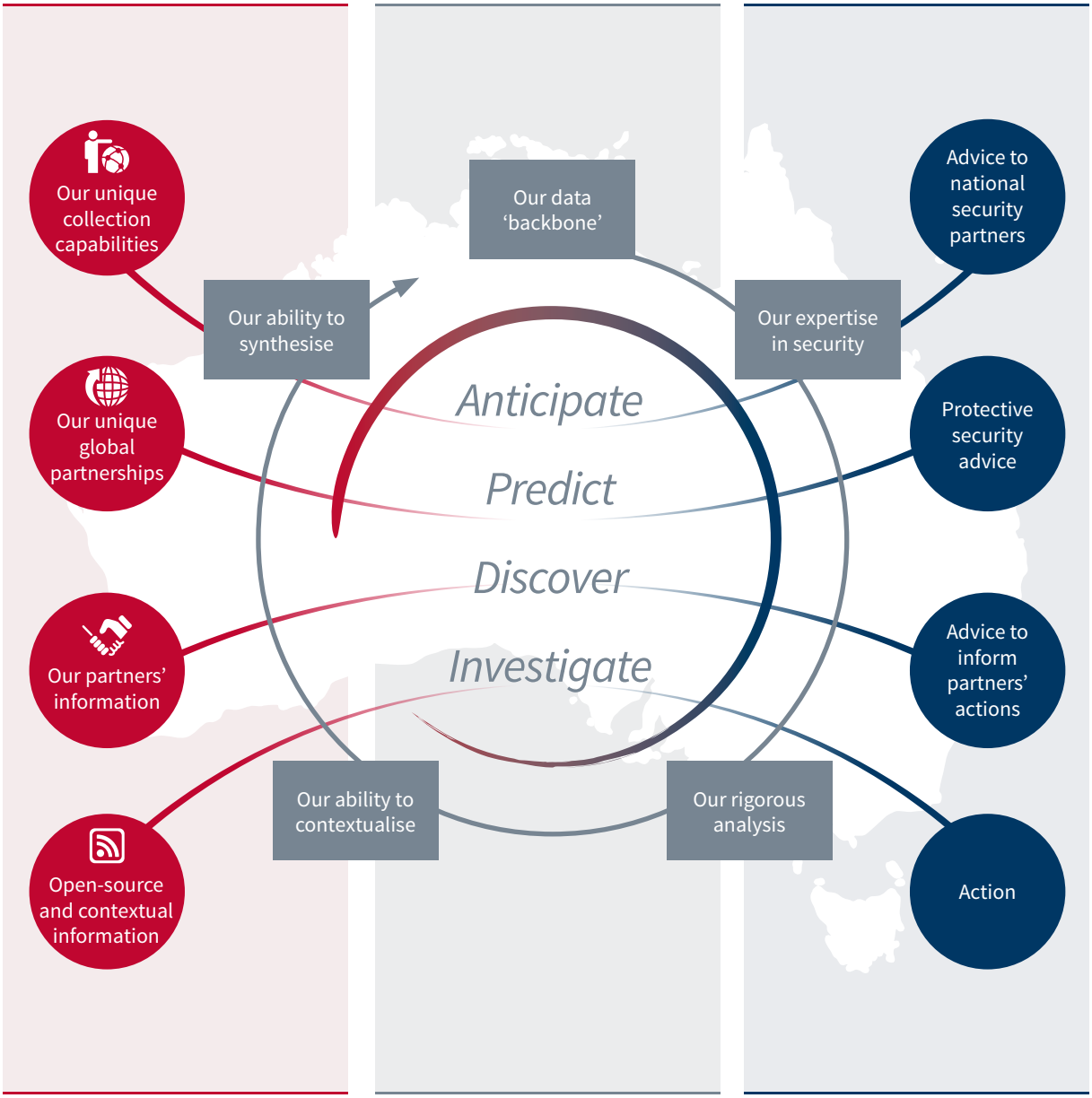
- counter terrorism
- counter espionage, foreign interference and malicious insiders
- counter serious threats to Australia's border integrity
- provide protective security advice to government and industry

How we do it

1 Harness our unique intelligence capabilities, partnerships and partner information

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

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



SECURITY ENVIRONMENT

Terrorism

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. 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. Individuals motivated by other forms of extremism and ideology are also present onshore.

Figure 2: 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.

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. Terrorist targeting of crowded places, in particular, has featured in recent terrorist attacks both onshore and globally.

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. A low-capability attack targeting people fulfils a number of key terrorist objectives, including casualties, public fear and anxiety, and media attention.

The more likely form of terrorism in Australia remains a low-cost, locally financed attack by an individual or small group using 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 its former territory. While ISIL's ability to direct external attack planning from the conflict zone in Iraq–Syria 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 Iraq–Syria 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. The increased availability of extremist material online reflects the expanding diversity of right-wing ideologies that fall within the extremist spectrum. Internationally, the March 2019 Christchurch, New Zealand, attacks have already been cited as inspiration for a number of extreme right-wing attacks overseas. Extreme right-wing groups in Australia are more organised than they have been in 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.

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.

Figure 3: 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.

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.

Disruptions of terrorist planning

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 following cases:

- On 20 November 2018, three individuals in Melbourne were arrested 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.
- On 20 June 2019, an individual in Melbourne was arrested 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.

During 2018–19 ASIO continued to support federal–state Joint Counter Terrorism Teams (JCTT) 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 the Australians remaining in Syria.

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. Acts of civil disobedience or opportunistic violence at protests are possible, particularly at events attended by counter-protesters.

On 5 January 2019, right-wing protesters gathered at St Kilda Beach, Melbourne, to protest against African crime gangs and local attacks. Left-wing groups organised a counter-protest to this event, leading to confrontation and scuffles between the groups, and traffic disruption when the two groups obstructed a roadway.

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.

While ASIO's adversaries may have changed over the past 70 years, the challenges they pose have not. Foreign states, seeking access to privileged and classified information, continue to target Australian Governments at all levels, academia and research institutions, critical infrastructure, and industry. Australia's research and development of innovative technologies and its military modernisation program are particularly attractive targets for espionage by foreign states seeking to gain an advantage to the detriment of Australia's security and prosperity.

These activities against Australian interests have become enduring and increasingly complex features of the Australian security landscape. The threat has escalated markedly over much of the past two decades.

Australia's telecommunications sector is also an attractive target, as it underpins Australia's critical infrastructure and provides opportunities for foreign states to conduct activities that pose a persistent threat to national security. The security and integrity of these networks, and of the communications and data they carry, are of the utmost importance. The implementation of the *Telecommunications and Other Legislative Amendments (Telecommunications Sector Security Reforms) Act 2017* during the reporting period has helped to better secure these vital assets.

Australia's place in the global economy and its integration into global supply chains and services mean that espionage and foreign interference now has an impact on a greater number of, and more diverse, parts of the Australian community than it did in the past, and the range of vectors through which it is being pursued has expanded.

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, freedom of association and freedom of 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 diminishes Australia's sovereignty, reshapes Australian decision-making to further foreign interests, and undermines public confidence in the integrity of Australian democratic institutions and processes.

We remain 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.

Important legislative reform in 2018–19 has provided ASIO and our partners with new laws to counter espionage and foreign interference. The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* and the *Foreign Influence Transparency Scheme Act 2018* are strengthening Australia against acts detrimental to its security and providing the Australian public with a greater degree of transparency in relation to those who represent the interests of foreign states. These measures 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.

Figure 4: What is an act of foreign interference?

Case study 1:
Preventing hostile intelligence approaches through social media

During the reporting period, ASIO produced a report 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 heightened awareness of this vector being used for hostile intelligence activity and led to action by stakeholders to better manage security risks. It also provided some new intelligence back to ASIO.

Our report was distributed to stakeholders across government, business and industry. We also included advice on the topic in our outreach activities, ongoing security awareness briefings, and specific engagements with government, the defence industry, and research institutions.

Border integrity

During the reporting period, we contributed advice that informed policy to streamline referral criteria for security assessments of visa and citizenship applications, and the operation of the Aviation Security Identification Card (ASIC) and Maritime Security Identification Card (MSIC) schemes. We continued to produce security assessments to help the Department of Home Affairs and other agencies manage security risks, thereby mitigating threats to Australia's security by ensuring the denial of entry to Australia, or the cancellation of already held visas to Australia, of individuals who pose a security risk. Terrorism concerns accounted for most of the visa and citizenship adverse security assessments issued in the reporting period.

We contributed to a number of government coordination forums on border security issues and supported the development of Australian Government policy on border security. Intelligence derived from our investigations contributed directly to the operational activities of member agencies from Operation Sovereign Borders (OSB). We also supported OSB by providing advice on the threat environment, contributing to contingency plans and investigating Australia-based links to people-smuggling ventures.

Case study 2:
Prevention of entry to Australia of individual with terrorism affiliations

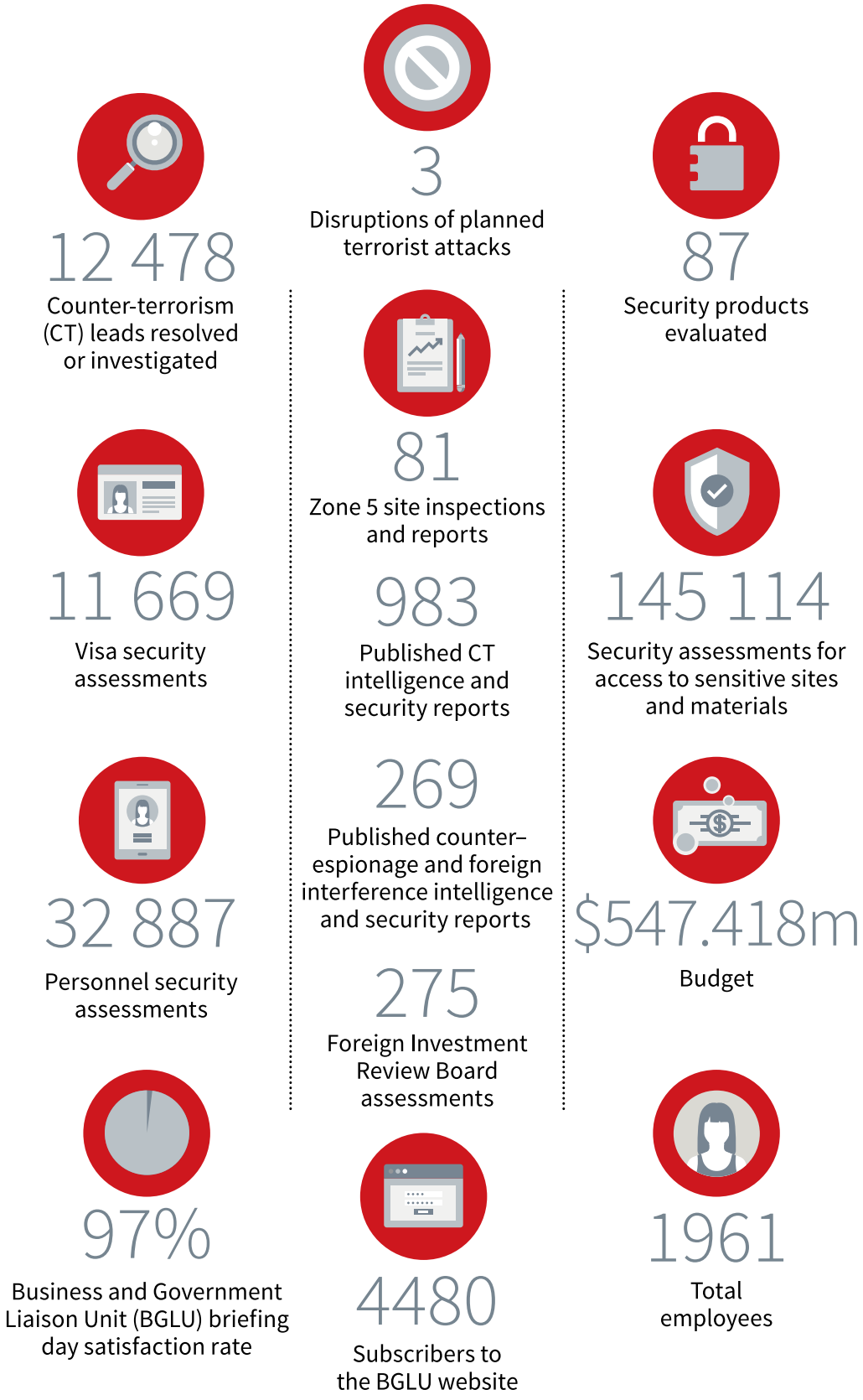
Australia's border integrity and security are critical elements in Australia's defence against the terrorist threat. In the reporting period, we continued to mitigate these threats to Australia by furnishing security assessments to the Department of Home Affairs.

One of the many cases we investigated involved an offshore visa applicant who was assessed to have previously provided logistic support to individuals affiliated with the 11 September 2001 attacks in the United States. We assessed that the individual presented an avoidable risk to Australia's security, and issued an adverse security assessment in early 2019, resulting in refusal of the individual's visa to Australia.

This example demonstrates that individuals who have terrorist affiliations or who are supportive of ideologies committed to politically motivated violence continue to seek to travel to Australia, across a range of visa categories.

Our investigation was carried out with the cooperation of our domestic and international partner networks, which are invaluable in helping to keep Australians safe.

Figure 5: ASIO at a glance 2018–19



STRATEGY AND GOVERNANCE

Strategic direction and priorities

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

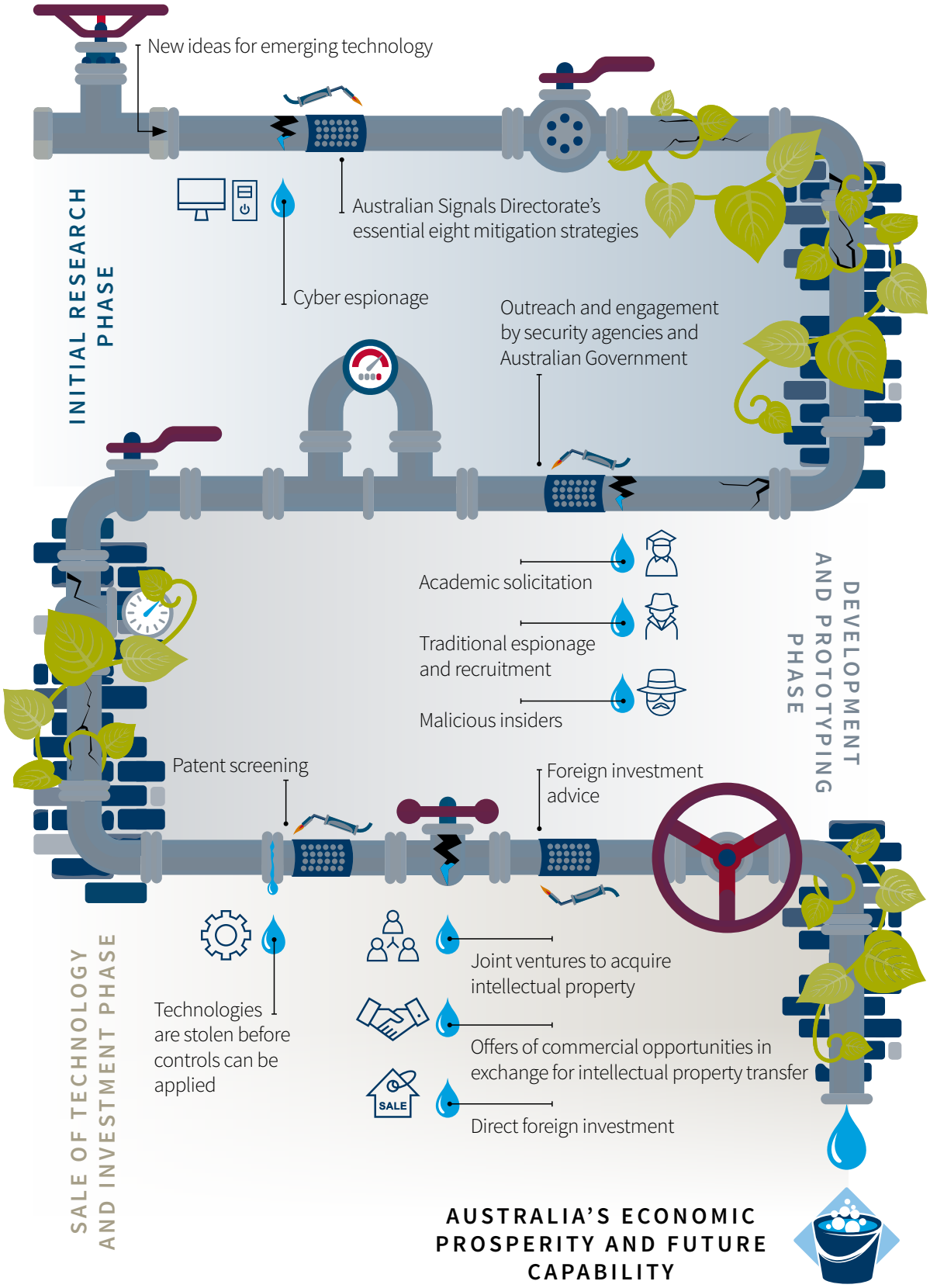
In 2018 we began the Transformation program to implement the recommendations of Mr David Thodey AO's 2017 report *A digital transformation of the Australian Security Intelligence Organisation*. This program positions us to take advantage of modern data and technology platforms and equips us with the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

During the reporting period, we took critical steps in the foundational stages of the Transformation program. For example, we approached the open market for the first time to engage with new technology partners, ensuring we will be using the latest in digital and technological innovation. We also established a portfolio management capability to optimise allocation of our resources and investments across the enterprise, and we began work to develop a new operating model to ensure our functions continue to work seamlessly together to deliver security intelligence outcomes.

Information and communications technology initiatives

Foundational Transformation work in 2018–19 included establishing the foundational teams, platforms, relationships and ways of working that are necessary to scale and accelerate the Transformation program in future years. We conducted an open, unclassified Request for Expressions of Interest (REOI) process to secure strategic technical partners to help us build our future technology platforms. This resulted in a shortlist of potential technology partners, which we will use in a Request for Tender process in 2019–20 to select preferred partners to help us deliver the Transformation program.

Figure 6: Emerging technology pipeline



Strategic plans

The roadmap for ASIO's Transformation is the ASIO Strategy 2018–23. Launched in October 2018, the strategy sets the direction to realise ASIO's 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. The strategy reframes our vision and purpose and sets out the steps ASIO will take over the coming years to ensure we continue to evolve as a modern, fit-for-purpose security intelligence organisation.

Home Affairs portfolio

After moving to the Home Affairs portfolio in May 2018, ASIO was fully engaged in the transition process. The changes have not affected ASIO's functions or statutory independence and have delivered the expected strengthened levels of cross-agency cooperation. We have worked diligently to integrate our Organisation into our new portfolio and deliver the efficiencies, coordination and results-driven change the Australian Government expects.

Corporate Plan

ASIO's 2018–19 corporate plan set out ASIO's priorities, performance framework and approach to managing risk for the reporting period. The plan recognised the significant challenges of operating in an environment of heightened threats, technological change and increasing demands for our advice and services, and flagged that ASIO's transformation into a world-class digital organisation would help us respond to these challenges.

Organisation structure

Throughout 2018–19 we began adjusting our Organisational structure to align with the objectives of the Transformation program. While this work is ongoing, key changes include the formal establishment of the Enterprise Transformation Office, which incorporates functions such as new policy implementation, and strategy and capability for our operations and assessments. We also established a data function and the Chief Data Officer position.

Organisation performance evaluation and accountability

To fulfil our obligations under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), we have a range of appropriate control, compliance and accountability frameworks to assess, monitor and report on ASIO's performance. These frameworks include our corporate plan, annual performance statement, annual stakeholder survey and annual report.

The corporate governance framework provides the oversight mechanisms for monitoring and evaluating performance and ensuring appropriate resources are allocated to achieve our Counter, Shape, Build objectives. Collectively, these mechanisms identify key strategic outcomes and advise on whether or not ASIO is achieving its expected or desired performance objectives.

Figure 7: Organisation 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

First Assistant Director-General

- Technical Capabilities
- Operational Capabilities
- Information
- Data

Assistant Director-General

- Data and Technical Analysis
- Physical Surveillance
- IT Infrastructure Services
- Telecommunication Operations
- Operations Services
- Business Information Systems
- Computer Operations
- Training
- Information Services
- Close Access Operations
- Strategy and Performance

Deputy Director-General
OPERATIONS AND ASSESSMENTS GROUP

First Assistant Director-General

- Counter-Espionage and Interference
- Counter-Terrorism
- Security Advice and Assessments
- Centre for Counter-Terrorism Coordination

Assistant Director-General

- Counter-Espionage and Interference A
- Counter-Terrorism Mission
- National Threat Assessment Centre
- Centre for Counter-Terrorism Coordination
- Counter-Espionage and Interference B
- Counter-Terrorism Investigations 1
- Border Investigations and Assessments
- 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

Corporate governance

The Director-General of Security is the accountable authority for ASIO under the PGPA Act. ASIO's Executive Board and corporate governance committees support the Director-General to fulfil his responsibilities under the PGPA Act. Their collective 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.

Corporate governance committees

During the reporting period, ASIO's governance committees supported the leadership and decision-making of the Director-General as outlined below.

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 the 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 towards our Transformation, and diversity and inclusion goals.

Transformation Oversight Committee

The Transformation Oversight Committee (TOC) is part of ASIO's Transformation governance framework. It was established to provide oversight, leadership and governance to ensure the Transformation program's momentum is maintained and that it delivers value. The TOC is accountable for realising the Transformation's vision, delivery and performance.

Intelligence Committee

The Intelligence Committee (IC) oversees the governance arrangements of, and makes decisions about, 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 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 of, and makes decisions about, 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 defined in ASIO's corporate plan 2018–19. The SC reported to the Executive Board on ASIO's performance against its security objectives.

Finance Committee

The Finance Committee (FC) oversaw the governance arrangements of, and made decisions about, 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 defined in ASIO's corporate plan 2018–19. The FC's responsibilities were subsumed by the Executive Board in October 2018.

Workforce Committee

The Workforce Committee (WC) oversaw the governance arrangements of, and made decisions about, 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 defined in ASIO's corporate plan 2018–19. The WC's responsibilities were subsumed by the Executive Board in November 2018.

ASIO Diversity and Inclusion Council

The ASIO Diversity and Inclusion Council (ADIC) is responsible for developing, implementing and reviewing strategies that support staff diversity and inclusion in ASIO.

During the reporting period, the ADIC oversaw the governance arrangements of, and made decisions about, 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 Diversity and Inclusion Strategy 2018–20.

Audit and Risk Committee

In compliance with section 45 of the PGPA Act, the Audit and Risk Committee (ARC) provides independent advice to the Director-General and the Executive Board on ASIO's financial and performance reporting responsibilities, risk oversight and internal control system.

The ARC also oversees external audit activity and internal audit activity (in accordance with the Internal Audit Charter), by setting priorities for audit, fraud control and evaluation planning. The ARC considers the findings of internal audits and evaluations, and monitors the implementation of management-endorsed recommendations. The ARC also periodically reviews governance arrangements and internal control systems to provide advice to the Director-General on their adequacy to meet legislative requirements.

During the reporting period, the ARC provided independent assurance and advice to the Director-General and the Executive Board on ASIO's financial and performance reporting responsibilities, risk oversight and management system, and internal control system. In line with its terms of reference, the ARC had four external members, including an external chair, Mr Geoff Knuckey, and observers from the Australian National Audit Office.

Fraud control and management

ASIO's Fraud Management Group continued to oversee fraud control and management arrangements within ASIO, reporting to the ARC. Fraud is managed in line with the Commonwealth Fraud Control Framework.

We revised ASIO's fraud control and management arrangements 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.

Internal Audit directorate

The Internal Audit directorate is an important element of ASIO's governance framework. Its function is to provide assurance to the Director-General that ASIO's risk, control and compliance measures are appropriate and efficient. Its annual work program is endorsed by the ARC and based on an annual assessment of business risks and internal controls. It includes compliance audits—some mandatory, as required by either legislation or agreements—and performance reviews.

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.

Legislative and policy compliance

During 2018–19 ASIO operated under a decentralised compliance model, where we managed compliance issues using existing management structures. Following an internal review of our compliance posture, during the reporting period we established a centralised Compliance directorate to ensure a formal and structured Organisation-wide approach to supporting compliance and to promote our assurance posture.

The Compliance directorate was set up at the end of May 2019 and tasked with implementing the centralised compliance function over two years. The directorate is focused on ensuring that ASIO continues to demonstrate a commitment to the highest standards of ethics and compliance with all applicable laws, regulations, rules and policies. The directorate promotes a culture of compliance in the conduct of ASIO's operations and broader work.

The objectives of ASIO's centralised compliance function are to:

- promote a culture of frank and open disclosure of compliance breaches;
- document, continuously review and update ASIO's internal business processes to ensure they comply with applicable laws and regulations;
- provide employees with training and assistance to become effectively involved in compliance activities to meet their obligations;
- maintain monitoring and reporting systems to identify instances of noncompliance or internal control failure, and to protect ASIO and its staff from deliberate or inadvertent breaches and consequential penalties;
- take prompt action where necessary to address instances of noncompliance or other circumstances that present an unacceptable exposure to risks of noncompliance, which include legal, reputational and operational capability risks;
- assess compliance against predetermined objectives and assessment criteria; and
- review the compliance framework periodically to ensure it is consistent with better practice and ASIO's needs.

Performance

ASIO's annual performance objectives are established in its corporate plan, in line with PGPA Act requirements. Performance is monitored against those objectives throughout the year, and an evaluation of their progress is summarised in ASIO's annual performance statement. The performance statement is informed by a variety of data sources—in particular, ASIO's annual stakeholder survey, which captures our stakeholders' independent evaluation of ASIO's performance. The annual performance statement is published in ASIO's annual report.

The *ASIO annual report 2018–19* was tabled in parliament on 15 October 2019 and is available at www.asio.gov.au and www.transparency.gov.au. The report highlights key performance outcomes for the reporting period, including:

- contributing to the identification, disruption and subsequent government and industry responses to three planned terrorist attacks in Australia;
- engaging with Australian Government policymakers to support consideration of legislative amendments to strengthen Australia's national security apparatus, particularly through the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*;
- publishing 1227 intelligence reports on terrorism, espionage and foreign interference, and border security issues, to support the work of the Australian Government and our national security partners; and
- commencing the foundation stages of ASIO's Transformation.

The effectiveness of ASIO's performance during the 2018–19 reporting period was corroborated by the findings of the ASIO annual stakeholder survey.

Performance challenges

As shown in our annual report, we achieved six of the eight performance objectives outlined in our 2018–19 corporate plan. The two objectives assessed as 'partially achieved' fall within our 'Countering espionage, foreign interference, sabotage and malicious insiders' key activity. This 'partially achieved' assessment recognises that the escalating threat of espionage and foreign interference facing Australia, combined with greater awareness of that threat among stakeholders, has increased demand for ASIO advice, putting pressure on current resources.

We continue to prioritise our finite resources to address the activities of greatest potential harm to Australians and Australian interests.

In relation to ASIO's financial performance, the operating environment in 2018–19 continued to be challenging, resulting in ongoing pressure on 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. The Transformation program is designed to alleviate some of the pressures on ASIO's budgets.

Risk

We continue to view enterprise risk management and assessment as a key enabler, imperative for the success of the Organisation and its objectives. Under the PGPA Act, the Director-General of Security is ASIO's accountable authority, supported by our Executive Board. Independent of this, the Audit and Risk Committee conducts periodic reviews of ASIO's risk management and risk assessment processes, and the Australian National Audit Office and the Office of the Inspector-General of Intelligence and Security provide external oversight.

We apply risk management with consideration and care across our operations. We endeavor to consistently improve in this area and, accordingly, we will implement a new risk management framework over the next reporting period.

EXPENDITURE

Budget

ASIO's budget is set out in the Portfolio Budget Statement, and the audited outcome published in ASIO's annual report. Portfolio Budget Statements are prepared annually, consistent with the Commonwealth's budgeting requirements, and Portfolio Additional Estimates Statements prepared if new measures are approved by the government after the Budget.

In 2018–19 ASIO received revenue from government totaling $526.1 million, comprising $435.2 million in operating funding and for capital activities, $85.6 million in Departmental Capital Budget (DCB), and $5.4 million in equity injection. 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 the previous 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.

ASIO's DCB funding was $85.6 million in 2018–19 as a result of previous years' appropriation re-phasing. In 2019–20, the DCB will be $61.3 million, which includes $17.0 million of terminating funding, and in 2020–21 it will stabilise at a lower figure of approximately $44 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.

ASIO continues 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. For example, the impact of these measures over the past four years has been $95.3 million, and it is expected to be $96.4 million over the next four years. ASIO will continue to identify and implement efficiencies and rigorously prioritise activities. However, we will give further consideration, during 2019–20 and 2020–21, to the sustainability of our current operations, in light of our projected DCB and operating budget and our anticipated future operating environment, noting that a Transformation objective is to alleviate financial and resourcing pressures.

Figure 8: Revenue from government, equity injections, Departmental Capital Budget for the period 2016–19 ($000)

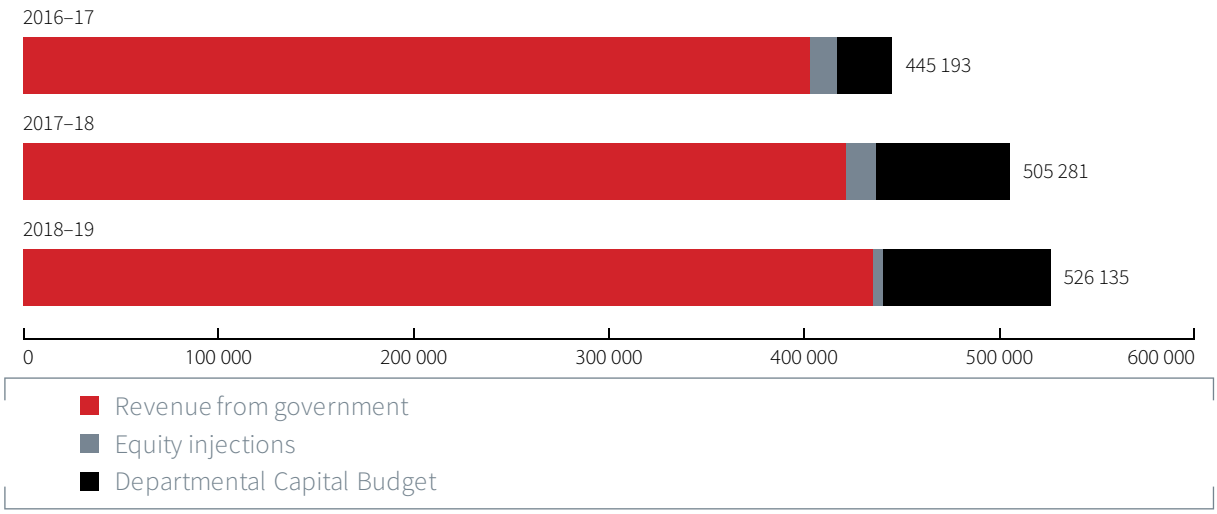
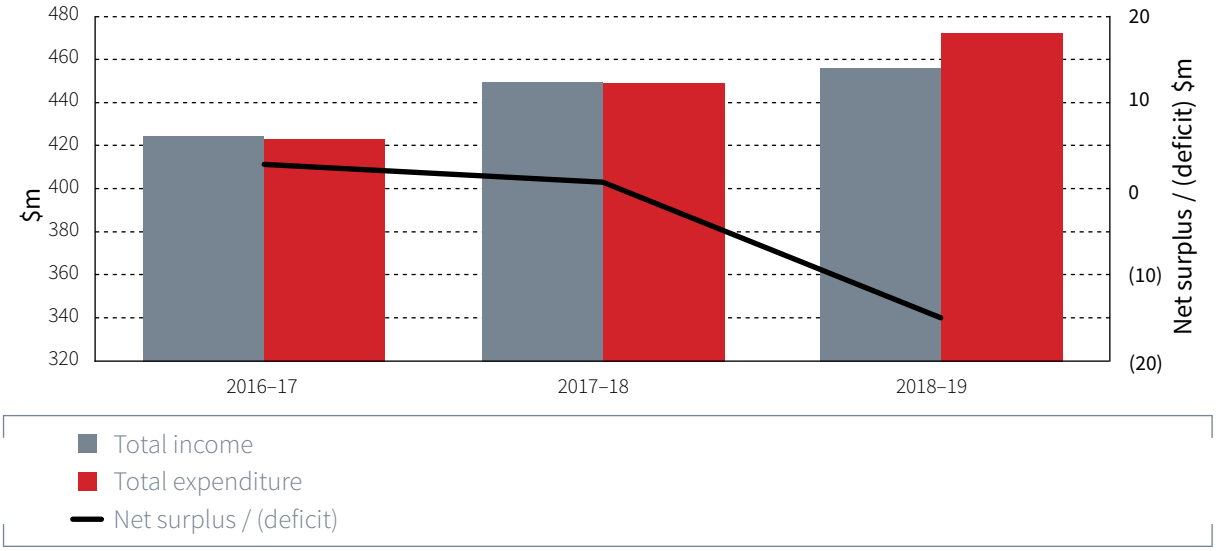


Figure 9: Financial performance (total income, total expenditure, net surplus/deficit) for the period 2016–19

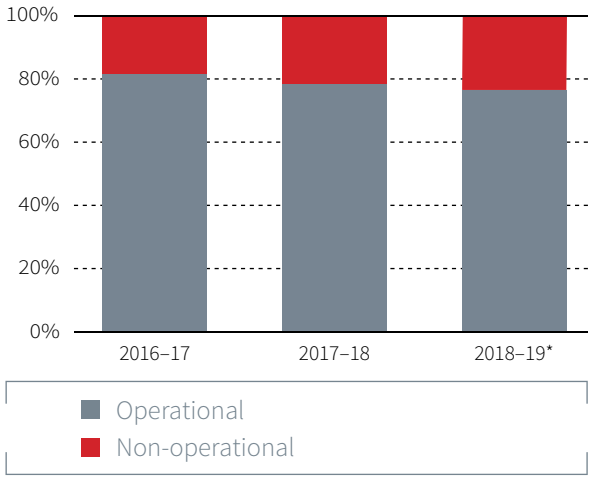


Resource allocation

The allocation of resources across ASIO's activities reflects the Organisation's strategic direction, set by our Executive Board. The board also ensures ASIO's budget and resource allocation align with organisational priorities.

Consistent with the previous reporting period, ASIO's expenditure continued to be predominantly operationally related (76.4 per cent). During the reporting period, ASIO's expenditure split between operational and non-operational activities moved by approximately 2.0 per cent, resulting in an overall increase in non-operational spending, from 21.6 per cent to 23.6 per cent of ASIO's budget. While ASIO has actively rationalised its non-operational component, pressures have still resulted in the increased non-operational component. The shift is largely due to uncontrolled external factors increasing the operating cost. For example, in 2018–19 ASIO's property operating expenditure increased by 4 per cent and our information and communication technology costs increased by 11 per cent.

Figure 10: Resource allocation



Note:
*2018–19 Australian Intelligence Missions allocation of resourcing to Corporate Management

Capital expenditure

Capital funding consists of equity injections and DCB; in 2018–19 ASIO's expenditure was primarily DCB related. During 2018–19 capital expenditure decreased by 8 per cent; however, there was still a significant capital program of $78.6 million. The reduction reflects reduced resources available for procurement and purchasing activities. The 2019–20 DCB will be reduced to $61.3 million (including $17.0 million of additional terminating funding agreed in the 2019–20 Budget), and in 2020–21 it will stabilise at a lower figure of approximately $44 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.

Figure 11: Purchase of capital items

Procurement

Throughout 2018–19 ASIO adhered to the Commonwealth Procurement Rules and associated policy and guidelines. Our compliance was monitored through the Audit and Risk Committee (ARC). No significant issues were identified, and overall compliance was acceptable.

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

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

During 2018–19 ASIO 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).

ASIO 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 to the PJCIS on its request.

Financial controls

ASIO prepares annual financial statements in accordance with the provisions in subsection 42(2) of the PGPA Act and the Financial Reporting Rules. The Australian National Audit Office (ANAO) audits ASIO's financial statements, including an annual examination of ASIO's internal systems and key financial controls. In 2018–19 ASIO did not receive any adverse audit qualifications from the ANAO as part of its independent audit reporting to parliament.

Within ASIO, since October 2018, the Chief Finance Officer (CFO) reported bimonthly to the Executive Board. Reporting includes current and future Organisational financial performance matters and strategic financial management planning. ASIO's financial management practices are underpinned by a financial management information system, with integrated internal controls aligned to ASIO's financial framework. The CFO also provides quarterly briefings to ASIO's ARC to support the committee's role of providing independent assurance about ASIO's internal governance, risk and control framework.

Internal assurance

In addition to audits conducted by the ANAO and internal system controls, ASIO's Internal Audit function also undertakes financial audits, providing assurance to the Director-General as the accountable authority, the Executive Board and the ARC. ASIO's Internal Audit work program is based on an annual assessment of business risks and internal controls and includes both compliance audits and performance reviews.

The ARC provides independent advice to the Director-General and the Executive Board on ASIO's financial and performance reporting responsibilities, risk oversight and internal control system (refer to 'Audit and Risk Committee', above). During 2018–19 the Chief Financial Officer reported quarterly to the ARC on ASIO's financial performance.

HUMAN RESOURCE MANAGEMENT

Overview

The report by Mr David Thodey AO, *A digital transformation of the Australian Security Intelligence Organisation*, made key recommendations about the importance of reforming ASIO's Organisational culture and people management processes to achieve enterprise transformation. In 2018–19 we advanced these key recommendations to mature our ability to manage our people capabilities by defining the requirement to progress five interrelated projects:

- People
- Workforce
- Systems, Data and Workforce Analytics
- Change Management
- Adaptive Leadership.

We defined and progressed our transformative approach in parallel with continuing to optimise and evolve key human resource (HR) initiatives, to lay solid foundations for the developing reforms program.

Cascading from the ASIO Strategy 2018–23 is the ASIO People Strategy 2019–23, which we developed and launched in the reporting period. The strategy focuses on our vision of a flexible, highly skilled and engaged workforce underpinned by HR practices and technology, to enable us to have '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 will guide our people and strategic workforce initiatives, to ensure that ASIO is flexible and forward-looking; to create efficiencies; to make informed, data-driven decisions on the development (internal) or acquisition (external) of future capabilities; to position our Organisation to realise capabilities at the time they are required; and, internally, to reskill or redeploy capabilities as our environmental and technological drivers evolve.

Data-driven insights for ASIO as an enterprise are central to our ability to do this. Throughout 2018–19 we focused on maturing our workforce analytics capability, developed and implemented an HR Enterprise Data Warehouse, and delivered an initial suite of dashboard workforce reports. This work lays the foundation for the development of more advanced workforce analytics capabilities.

Workforce statistics

At the end of 2018–19, ASIO employed 1877 full-time equivalent staff; an increase of 62 ongoing employees (3.4 per cent) from the end of 2017–18. This growth is required to support four New Policy Proposals, in addition to offsetting natural attrition.

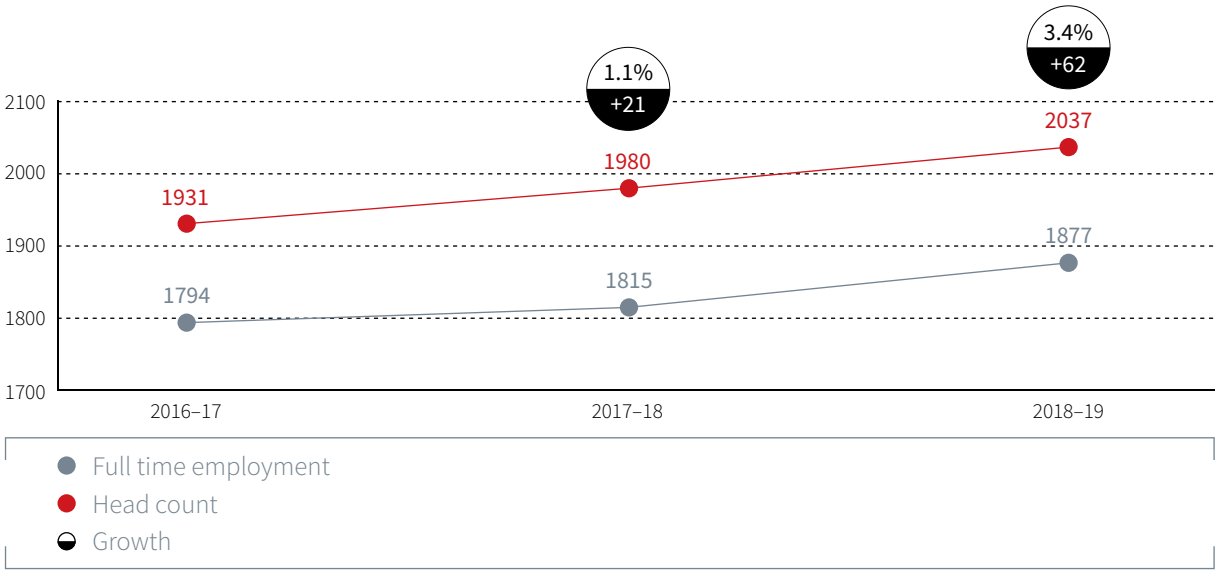
The number of ASIO employees accessing flexible work arrangements through part-time employment increased in the reporting period. We assess this to be a result of proactive policies in support of flexible working arrangements, driven through the ASIO2020 program—specifically the Diversity and Inclusion Strategy—as well as the release of the 'If not, why not' guidelines on flexible working arrangements and the establishment of Diversity and Inclusion networks.

Table 1: Head count of staff by load and employment status

	2016–17			2017–18			2018–19		
Status	Ongoing	Non-ongoing	Total	Ongoing	Non-ongoing	Total	Ongoing	Non-ongoing	Total
Full-time	1611	12	**1623**	1640	10	**1650**	1681	9	**1690**
Part-time	240	18	**258**	260	21	**281**	280	16	**296**
Casual	-	50	**50**	-	49	**49**	-	51	**51**
Total	1851	80	**1931**	1900	80	**1980**	1961	76	**2037**

Note:
1. Data includes the Director-General and excludes secondees into ASIO and locally engaged staff.

Figure 12: Staffing growth (full-time equivalent actual and head count)



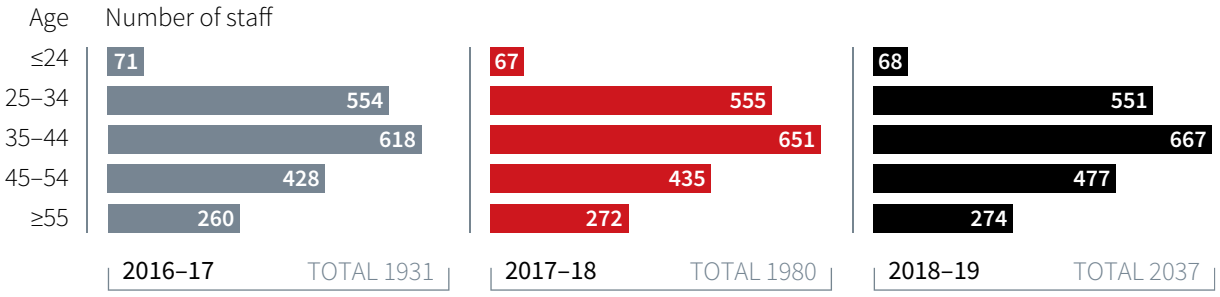
Note:
1. Data includes the Director-General and excludes secondees into ASIO and locally engaged staff.

Table 2: Head count of staff by gender and employment status

	2016–17				2017–18				2018–19			
Gender	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Female	844	10	14	**868**	882	8	12	**902**	918	6	14	**938**
Male	1007	20	36	**1063**	1018	23	37	**1078**	1043	19	37	**1099**
Total	1851	30	50	**1931**	1900	31	49	**1980**	1961	25	51	**2037**

Notes:
1. Data includes the Director-General and excludes secondees into ASIO and locally engaged staff.
2. Data is derived from the nominal establishment.

Figure 13: Age profile



Note:
1. Data includes the Director-General and excludes secondees into ASIO and locally engaged staff.

Table 3: Head count of employees by classification and employment status

		2016–17				2017–18				2018–19			
		Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Director-General	DG	1	-	-	**1**	1	-	-	**1**	1	-	-	**1**
Senior Executive Service	SES Band 3	2	-	-	**2**	4	-	-	**4**	4	-	-	**4**
	SES Band 2	11	-	2	**13**	12	-	3	**15**	13	-	3	**16**
	SES Band 1	34	2	1	**37**	37	2	1	**40**	46	1	3	**50**
Senior officers	AEE2–3	175	3	1	**179**	187	5	1	**193**	185	3	1	**189**
	AEE1	365	3	3	**371**	407	5	3	**415**	483	5	3	**491**
Employees	AE1–6	1128	21	42	**1191**	1099	18	40	**1157**	1083	16	40	**1139**
Employees (total)	AE1–6 (including technical specialists)	1263	22	43	**1328**	1252	19	41	**1312**	1229	16	41	**1286**
Total		1851	30	50	**1931**	1900	31	49	**1980**	1961	25	51	**2037**

Notes:
1. Data includes the Director-General and excludes secondees into ASIO and locally engaged staff.
2. Data is derived from the nominal establishment.

Table 4: Head count of employees by location and employment status

	2016–17				2017–18				2018–19			
	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Canberra-based	1312	17	37	**1366**	1358	23	36	**1417**	1413	18	38	**1468**
Other locations	539	13	13	**565**	542	8	13	**563**	548	7	13	**569**
Total	1851	30	50	**1931**	1900	31	49	**1980**	1961	25	51	**2037**

Note:
1. Data includes the Director-General and excludes secondees into ASIO and locally engaged staff.

Commencements and separations

Commencements

Our effort to grow to support our capability and meet our Transformation objectives is ongoing. In 2018–19 we achieved a net growth of 62 ongoing staff.

Table 5: Commencements by classification

		2016–17	2017–18	2018–19
Director-General	DG	-	-	-
Senior Executive Service	SES Band 3	-	-	-
	SES Band 2	2	1	1
	SES Band 1	1	1	8
Senior officers	AEE2/3	4	10	3
	AEE1	22	17	16
Employees	AE1–6	114	94	130
Employees (total)	AE1–6 (including technical specialists)	136	123	152
Total		**165**	**152**	**180**

Notes:
1. Includes the Director-General and ongoing, non-ongoing and casual employees.
2. Excludes secondees into ASIO and locally engaged staff.

Separations

Of the 124 ongoing, non-ongoing and casual employees who separated from ASIO in the reporting period, the highest percentages came from the following cohorts:

- by tenure—ASIO officers with a tenure of 10–14 years (31 per cent), closely followed by ASIO officers with a tenure of 15 years or more (24 per cent);
- by classification—AE6 officers and equivalents (43 per cent);
- by age—ASIO officers 55 years of age and over (35 per cent), followed by ASIO officers aged between 35 and 44 years of age (28 per cent).

These separations are proportionate to the percentage of employees within their respective cohorts; except for ASIO officers aged 55 years and over (35 per cent of separations), which comprise 13 per cent of ASIO's workforce. Retirement comprised 59 per cent of separations within this age group.

Of the separating ongoing ASIO Officers, 29 per cent resigned and commenced employment with Australian Public Service agencies, and 27 per cent accepted employment within the private sector.

Table 6: Separations by classification

		2016–17	2017–18	2018–19
Director-General	DG	-	-	-
Senior Executive Service	SES Band 3	-	-	-
	SES Band 2	2	3	1
	SES Band 1	3	5	-
Senior officers	AEE2/3	11	8	14
	AEE1	27	21	25
Employees	AE1–6	55	60	72
Employees (total)	AE1–6 (including technical specialists)	67	67	84
Total		**98**	**110**	**104**

Notes:
1. Includes the Director-General and ongoing, non-ongoing and casual employees.
2. Excludes secondees into ASIO and locally engaged staff.

Table 7: Separations by reason

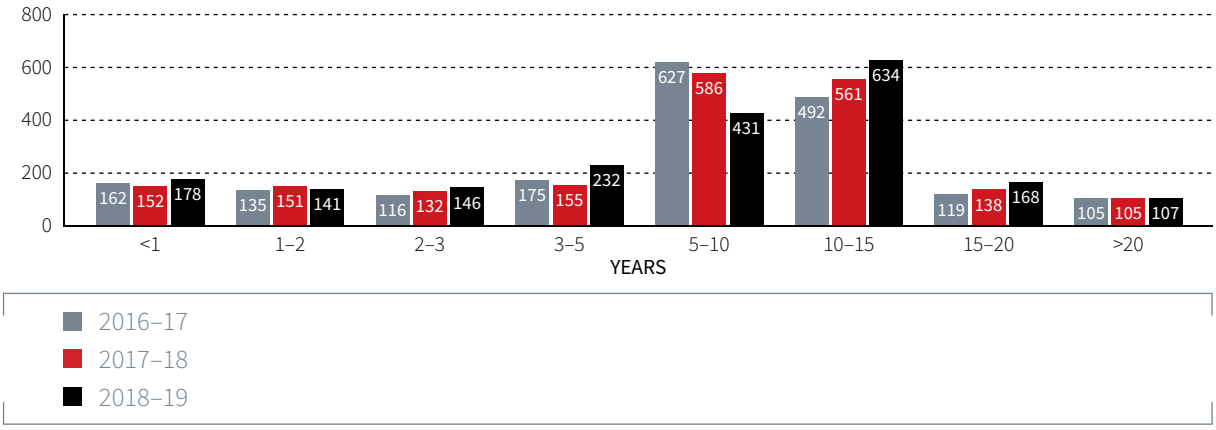
	2016–17		2017–18		2018–19	
Reason	Total	% of head count	Total	% of head count	Total	% of head count
Resignation	**80**	4%	**67**	3%	**83**	4%
Age retirement	**10**	1%	**18**	1%	**26**	1%
Retirement: invalidity	**1**	0%	**1**	0%	**2**	0%
Other	**67**	3%	**56**	3%	**75**	4%
Total	**158**	8%	**142**	7%	**186**	9%

Notes:
1. Head count includes the Director-General and ongoing, non-ongoing and casual employees.
2. Percentages are of the total head count as at the start of each financial year.
3. 'Other' includes contract expired, contract terminated, deceased, dismissed and voluntary redundancy.
4. 'Other' includes secondees into ASIO and locally engaged staff.

Tenure

During the reporting period, the average tenure for all ASIO separating employees—including secondees into ASIO, locally engaged staff and contractors—was eight years. The average tenure at separation for ongoing employees only is 12 years.

Figure 14: Length of service



Note:
1. Data includes the Director-General and excludes secondees into ASIO and locally engaged staff.

Workplace Agreement

ASIO continued to operate under its 10th Workplace Agreement, which was agreed in 2016 and notionally expired in March 2019. Consultation for our 11th Workplace Agreement began ahead of the nominal expiry of the existing agreement and remains in progress.

ASIO is required to adhere to the Public Sector Bargaining Policy and to adopt the employment principles of the Australian Public Service where they are consistent with the effective performance of the Organisation, including those relating to negotiating terms and conditions of employment.

ASIO Consultative Council

The ASIO Consultative Council (ACC) is a deliberative and advisory forum established in 2015 to enable ASIO's management and staff to meet regularly in a structured way, to discuss and resolve issues of interest and concern. The ACC supports communication between management and staff, thereby contributing to more effective and responsive decision-making. Staff are represented on the council by the Staff Association President and two vice-presidents.

Individual performance management

In recognition of the critical role of leadership in promoting a high-performance, innovative and inclusive culture, we revised our performance framework during 2018–19 to include employee commitments to the ASIO Leadership Charter. The updated framework includes recognition of voluntary employee commitments over and above the performance of daily roles, along with mechanisms to support and manage flexible working arrangements as part of individual performance management.

The release of key role competencies as part of the revised ASIO job family model further enriched performance discussions, with a focus on enhanced clarity of performance expectations, feedback and career pathways.

To support our Transformation, and to better enable contemporary ways of working, we began a project to implement an online talent management tool. This tool will help individuals and their managers identify training needs and will allow more effective career planning and talent development. We expect the project to be finalised in 2019–20.

Performance management processes

We continued to refine performance management policy and processes during 2018–19. Building on reforms undertaken in previous reporting periods, we achieved 100 per cent employee participation in the performance cycle process.

To further strengthen our high-performance culture, we reviewed and amended performance cycle processes. These are designed to strengthen the quality of employee and line manager discussions and are supported by a training and coaching framework and early intervention strategies to enhance performance. In addition, the continued development of new technologies designed to support two-way exchanges, better align individual objectives with Organisational priorities and goals and help identify current and future development needs remained a priority through the period.

Diversity and inclusion

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

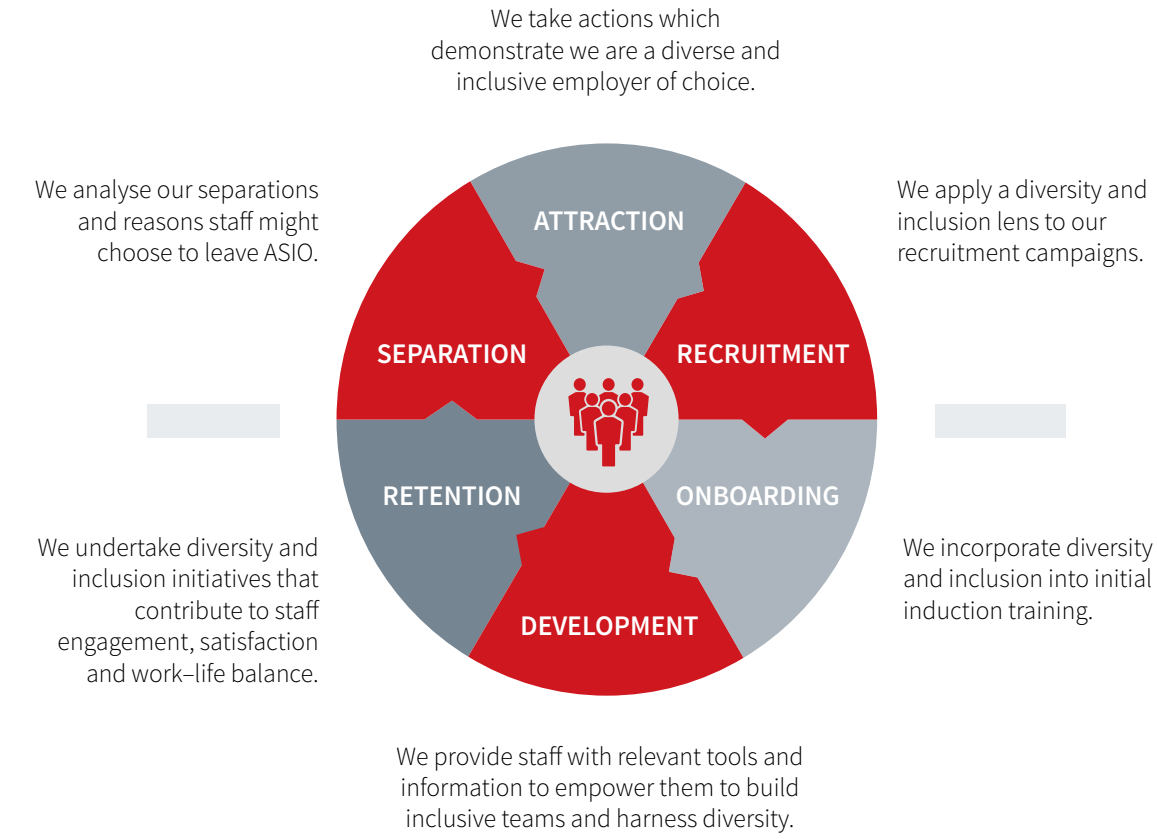
During 2018–19 we undertook a range of diversity and inclusion initiatives, including:

- establishing family room facilities in regional offices to provide support for staff members with caring responsibilities;
- continuing the ASIO-wide 'if not, why not' approach to flexible working arrangements;
- supporting staff-initiated and -led diversity networks, which form an essential part of creating a diverse and inclusive culture where all staff feel valued, respected, included and safe;
- creating an Aboriginal and Torres Strait Islander staff network and a gender equity network;
- delivering a number of cultural awareness initiatives, including 'SES Listen and Learn' sessions, which gave SES officers a direct insight into the lived experiences of ASIO staff with diversity characteristics, to better understand ASIO's diverse workforce and the challenges individuals can face in their everyday working life;
- continuing our commitment to the Male Champions of Change program; and
- continuing our commitment to reviewing our current targets, actions and transparency in relation to gender equality, particularly for shortlisting and promotion at the AEE1 level and above.

During the reporting period, ASIO became the first organisation ever to achieve silver accreditation in its first year of participation in the Australian Workplace Equality Index (AWEI) awards—Australia's national benchmarking instrument for LGBTQI workplace inclusion. We ranked third among federal government agencies and 15th nationwide in a field of 158 entrants.

We also gave staff opportunities to broaden their awareness and understanding of diversity and inclusion issues by offering active membership of groups including the Diversity Council of Australia, the Australian Network on Disability, and Pride in Diversity. We also offered staff access to a range of presentations and workshops, such as the National Intelligence Diversity and Inclusion Committee's International Women's Day event.

Figure 15: Our commitment to diversity and inclusion



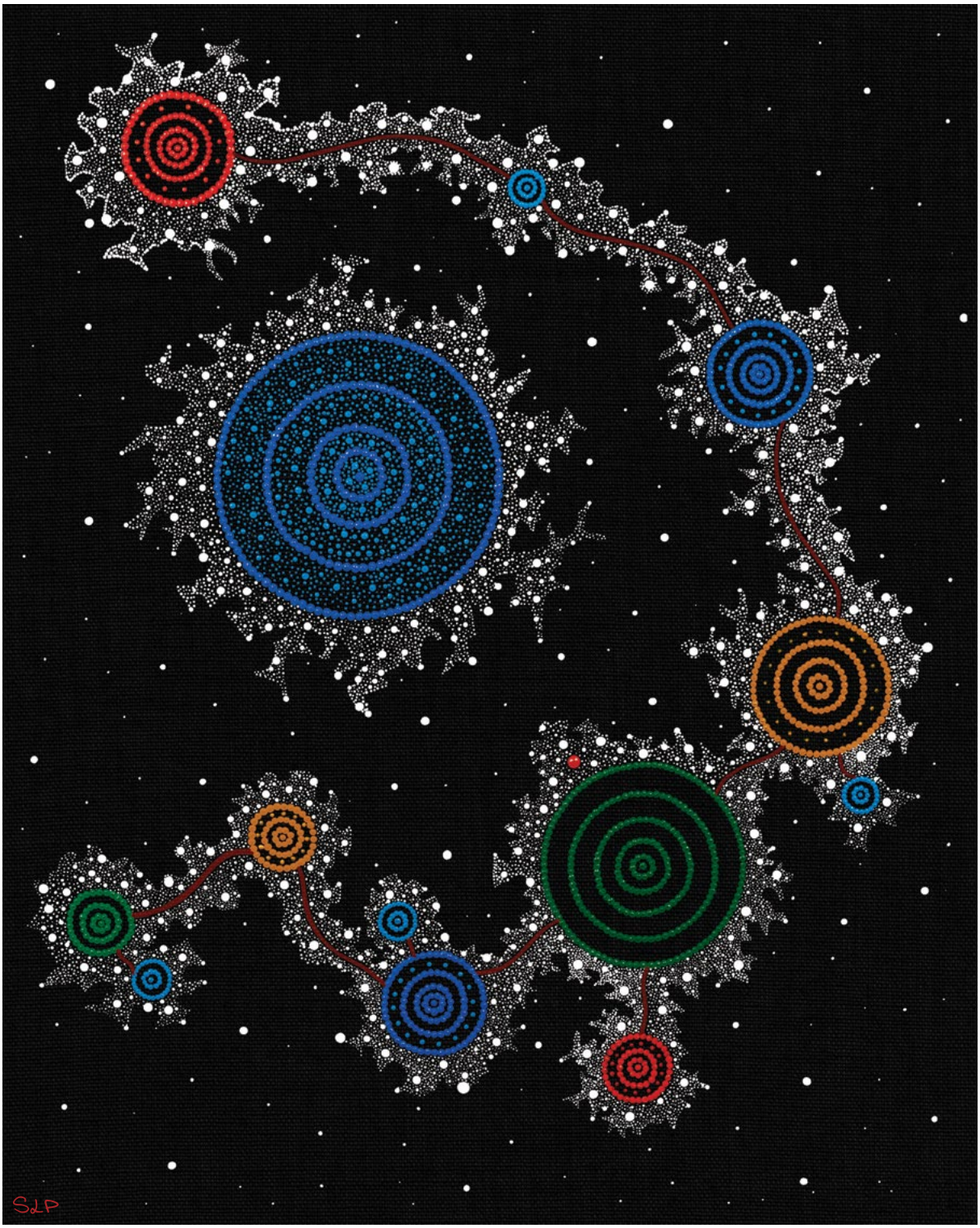
Mudyi—Aboriginal and Torres Strait Islander Staff Network

Our 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 our Aboriginal and Torres Strait Islander staff and culture and their contribution to ASIO's mission.

In April 2019, the Director-General approved the display of an Acknowledgment of Country artwork at ASIO's headquarters, the Ben Chifley Building. The artwork is titled 'Hope'. It is displayed on the following page, and a stylised version features on the cover of this submission.

The framed Acknowledgement of Country is a visual demonstration of our commitment to diversity and inclusion, symbolising ASIO's respect for the traditional Aboriginal or Torres Strait Islander custodians of the land. The artwork also reflects the broader objectives of the Australian Government in building Indigenous employment and cultural capability within the public sector.

Figure 16: Hope

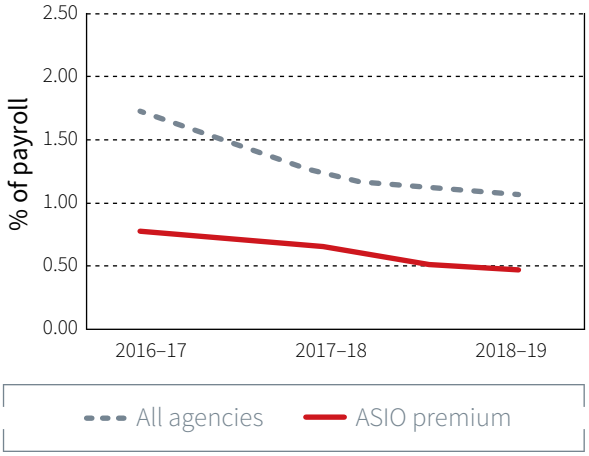


Work health and safety

We remain committed to ensuring the health, safety and wellbeing of our workforce. Our health, safety and wellbeing objectives include embedding a culture of safety risk awareness in all aspects of ASIO's decision-making; supporting strategies to eliminate or minimise risks to the health and safety of ASIO employees and visitors to ASIO premises; and providing support to ill and injured employees.

A key element in our health, safety and wellbeing approach is our focus on mental health. This includes programs to build mental health awareness and general resilience, and to prevent psychological injury. These programs are complemented by a range of corporate health and wellbeing initiatives that support the physical health and safety of our workforce.

Figure 17: Comparison of Comcare premium rates 2016–19



Note:
1. ASIO's Comcare premium rate has fallen from 0.53 per cent (revised rate) of payroll in 2017–18 to 0.46 per cent of payroll for 2018–19. The premium rate compares favourably with the overall premium for Commonwealth agencies in 2018–19, which is 1.06 per cent.

Our Health and Safety Representatives (HSRs) play an important role in creating a positive safety culture. They engage with work teams on the importance of maintaining a safe workplace and contribute to safety risk considerations through their contribution to the Executive Board's Enterprise Health, Safety and Wellbeing Subcommittee. Our corporate first aid officers provide a critical first-response function on a day-to-day basis, as well as when safety incidents occur.

In a heightened threat environment, we continue to direct significant resources towards safety training and personal security awareness programs, particularly in the context of operational activities. This includes ASIO situational awareness, general personal security, de-escalation and trauma first aid training programs. In some cases, relevant training is embedded in foundational and induction programs for particular work teams.

During the reporting period, we finished implementing the recommendations arising from a 2016–17 review of our work health and safety programs and performance. In particular, we optimised enhancements to safety governance structures, oversight of safety programs and performance monitoring.

We maintained an active early intervention approach to workplace injury rehabilitation and compensation case management during 2018–19. No areas of noncompliance were identified, and we continued to work closely with Comcare on both work health and safety, and rehabilitation.

In 2018–19, in line with legislated notification obligations, we notified one incident to Comcare. A Comcare inspector reviewed the incident and issued an Inspector Report with a number of recommendations, which were implemented. No notices were issued to ASIO under the *Work Health and Safety Act 2011*.

ASIO's Comcare premium rate has been consistently and significantly lower than the Commonwealth average since 2011–12. The premium rate for 2018–19 reduced to 0.46 per cent of payroll, down from 0.53 per cent in 2017–18. This reduction has primarily been influenced by the proactive management of medium-term and long-term claims, as well as a low claim frequency.

Recruitment

Attracting high-quality candidates to meet future capability and growth needs continues to be a high priority for ASIO. While the challenges of the competitive labour market, the geographical location of candidates, and the time frame and rigour needed to ensure stringent security clearance requirements remain, over the reporting period we continued to receive positive interest from applicants seeking to work with the Organisation.

To remain responsive to Organisational needs and competitive labour market demands, we continue to invest in future system enhancements to streamline processes and create greater efficiencies across all aspects of the recruitment pipeline, including recruitment, vetting, cognitive assessments and onboarding. We anticipate this work will culminate in a single recruitment system that will deliver greater speed and efficiency in the recruitment and onboarding process.

In addition, the ASIO job family model continues to mature, providing the flexibility to source and recruit candidates with the skills, capabilities and experience to fill a range of roles, rather than sourcing and recruiting for a specific job.

Other significant recruitment reforms underway include:

- developing our understanding of the attributes of successful, high-performing ASIO candidates and applying this insight when targeting recruitment campaigns and determining selection methodologies;
- continually analysing the effectiveness of our sourcing strategies and applying this analysis to better target recruitment activities; and
- increasing the use of merit lists as a significant recruitment lever.

Throughout the reporting period, our recruitment activities for the graduate and training programs—including our Intelligence Officer, Intelligence Analyst and Surveillance Officer training programs—attracted strong candidate interest. We continue to refine our approach to difficult-to-fill information technology roles, including through the Technologist graduate program, through targeted marketing and attraction campaigns.

Recruitment and retention strategies

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.

We continue to work with universities in science, technology, engineering and mathematics (STEM)–related fields to increase our technical capability through our 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.

We expended $1 517 000 on marketing and advertising and related recruitment activities and campaigns in 2018–19. These included greater attendance at career fairs, and increased outreach with advertising for high priority skill specific roles, including a renewed focus on technical streams, surveillance and NPP related recruitment.

Training and development

During the reporting period, we continued to provide an extensive range of personal and professional development opportunities to effectively meet the diverse needs of our staff and to build the capabilities needed to deliver organisational outcomes. In 2018–19 we focused on delivering leadership training to support leadership behaviours and capabilities, to drive and support a transforming organisation. We are also engaged in a number of community-wide learning and development opportunities.

By adopting the 70–20–10 learning model—that is, 70 per cent on-the-job learning, 20 per cent learning from others, and 10 per cent structured training—we equip our employees with the foundational, core job role and advanced competencies they need to successfully operate in the workplace across a diversity of generic and specialist skill sets. These skill sets include management and leadership, personal safety, collection and analysis, language, basic and advanced technical competency, and surveillance capability.

We continuously improve and ensure alignment of training with ASIO's objectives by conducting training-needs analysis, followed by review and evaluation. Training programs are delivered through a mix of in-house learning and development and training by subject matter experts and external training providers.

In 2018–19:

- We approved or conducted 136 training courses, including 3941 face-to-face training activities attended by 1370 staff.
- Our staff completed 3384 mandatory and 638 non-mandatory e-learning courses across seven mandatory and 31 non-mandatory online programs.
- We allocated $260 174 to 129 staff attending over 119 ASIO-supported study programs.
- ASIO's Senior Executive Service (SES) 360 Degree Feedback and Executive Coaching program, in which 49 SES members participated, concluded. The final coaching session for each SES member focused on leading through change in support of ASIO's Enterprise Transformation.

Face-to-face training offered has remained consistent with the previous financial year. The number of mandatory e-learning modules completed by staff increased by 830 from the previous year, and the completion of non-mandatory e-learning decreased by 146. Although use of non-mandatory online programs decreased, staff use of an external learning platform providing contemporary, relevant and 'just in time' modular online learning expanded.

Intelligence training

ASIO's Intelligence Officer Development Program (IODP) and Intelligence Analyst Development Program (IADP)—collectively known as the Intelligence Development Program (IDP)—trains and assesses employees for operational and analytical intelligence roles in ASIO. We conduct two IDPs per year, selecting participants from diverse academic, professional and personal backgrounds through a rigorous recruitment process.

All IDP participants must demonstrate workplace competence in their respective discipline to graduate as Intelligence Professionals. Graduates are posted to roles in ASIO's analytical or human intelligence functions. Participants who do not meet this standard are typically offered alternative roles in ASIO.

We also provide Intelligence Professionals with a range of further intelligence training opportunities to develop specific analytical and operational skills. These opportunities support ASIO's ongoing intelligence capability development.

Technical workforce

ASIO relies on several recruitment programs to sustain and develop the depth and breadth of its specialist technical workforce. These include the Technologist Graduate Program and the Information and Communications Technology (ICT) Traineeship.

For the Technologist Graduate program, we conduct a twice-yearly intake of university graduates with relevant science, technology, engineering and/or mathematics qualifications. This is a 12-month structured work placement and development program which sees our Technical Graduates deployed across a variety of technical areas and disciplines–both at the operational and enterprise level. Graduates are provided with a technical mentor and access to a range of online and offline training opportunities throughout the program. An underlying focus of the program involves teamwork, the application of continual learning practices and the progression of technical innovation methodologies.

Upon successful completion of the program, graduates are permanently placed into a technical team. Existing ASIO staff with applicable backgrounds may transfer into the program, subject to an assessment of their abilities.

ICT trainees are currently recruited every two years and enter a two-year traineeship comprising on-the-job workplace support for Certificate IV-level tertiary studies in an ICT discipline. ICT trainees complete four rotations to build their experience across software development, networking, server and desktop hardware, and ICT customer service. On graduation, trainees are appointed to technical enterprise positions in ASIO.

We also provide select in-house courses for elements of the technical workforce undertaking the technical collection of intelligence. No commercial equivalents exist for this skill-specific training and, where possible, efficiencies are gained by working with domestic or international partners to share the burden of developing and running these courses.

Other training programs

Other ASIO training programs include the Surveillance Officer Traineeship Program and the Graduate Lawyer Program. These programs support critical capabilities in ASIO and are developing the workforce of the future.

The Surveillance Officer Traineeship Program, conducted approximately every two years, equips officers with the skills, knowledge and experience to perform operational surveillance duties. It is a means of ensuring regular maintenance of ASIO's overall surveillance capability. After demonstrating initial suitability to be a surveillance officer, and successfully completing the program over approximately six months, staff are employed at the AE5 classification level and deployed across the Organisation. The most recent intake began in 2019.

The Graduate Lawyer Program enables participants to develop the legal competencies of a junior ASIO lawyer, with opportunities for supervised legal work across all areas of law practised in ASIO's Legal Services (LS) division. In parallel with the program, financial and study leave support is provided to participants who have not yet completed the external practical legal training course requirements for admission to legal practice. Upon successful completion of the program, participants are placed in an AE6 position in one of the LS branches, with LS placement expected for a minimum of two years. The program includes relevant internal and external training and development opportunities.

Language skills

In 2018–19 ASIO allocated $178 719 to 38 employees under the Language Skills Development Program. The overall allocation of funds was reduced owing to ongoing budgetary constraints. ASIO continued to apply extra rigour to the selection process and greater expectations of applicants to research cost-effective options and articulate Organisational benefits.

Table 8: Language Skills Development Program

	2016–17	2017–18	2018–19
Allocation	$291 661	$271 361	$178 719
Staff	34	32	38

National Intelligence Community training

In mid-2019, the National Centre for Intelligence Training and Education moved from ASIO to the Office of National Intelligence.

Ethics and conduct

ASIO strives to provide a positive working environment, where Organisational culture, leadership styles and workplace relationships support staff to effectively and efficiently undertake their roles and meet Organisational objectives. To achieve this, ASIO provides a consistent and robust response to bullying, harassment or other forms of inappropriate behaviour. This approach is supported by policies on employee ethics and conduct as well as ASIO's defined values and code of conduct, which help to inform decision-making and employee behaviour. The policies on ethics and conduct provide information on when to seek advice and report incidents to help ensure the effective management of employee conduct and behaviour.

The Ethics and Conduct team, within ASIO's Human Resources Branch, oversees employee harassment and discrimination complaints and allegations of misconduct. Public interest disclosures, allegations of fraud and security breaches are investigated through separate mechanisms and attract separate reporting obligations.

ASIO uses several systems and processes to identify, manage and respond to allegations of inappropriate behaviour and misconduct, including:

- early intervention;
- dispute resolution;
- coaching;
- conflict management and management of complaints; and
- misconduct investigations.

Promotion of ethics

In 2018–19 we provided staff with mandatory training that clarifies expectations of employee conduct, which must be legal, ethical and respectful of human rights. The training included the following subjects:

- ASIO's values and code of conduct requirements;
- mechanisms available to make a public interest disclosure;
- managing workplace discrimination, harassment and bullying; and
- work health and safety obligations.

Training on conduct and behaviour was also provided through our induction training and management training programs.

Misconduct

Human Resources Branch ensures impartiality by using external engaged investigators to conduct independent and impartial misconduct investigations.

Harassment and Discrimination Adviser network

Our network of Harassment and Discrimination Advisers (HaDA) is an Organisational resource designed to provide staff with information and impartial support on issues of discrimination, harassment, bullying and other forms of inappropriate behaviour. The HaDAs also provide referral advice and clarification on policies and complaint procedures. The role of a HaDA is voluntary, and the appointment is for two years.

At the end of 2018–19, there were 33 HaDAs across ASIO. HaDA network meetings were held in the reporting period to provide support to the HaDAs and to help ensure a consistent approach across the network in response to employee queries. In addition, health reviews of work areas were conducted as a proactive way to understand functioning within work areas and to partner with senior leadership to influence and educate employees on expectations and behaviour consistent with ASIO's values and Leadership Charter.

Public interest disclosures

Disclosure under the *Public Interest Disclosure Act 2013* (the PID Act) is an avenue open to employees who wish to raise issues involving potential wrongdoing at work and to have those issues investigated by management. The PID Act:

- provides a framework for public officials to make public interest disclosures;
- ensures that public interest disclosures are properly investigated and dealt with; and
- ensures that public officials are supported and protected from adverse consequences relating to disclosures.

The protection given to eligible disclosers is a significant feature that distinguishes the PID legislative framework from other courses of action open to concerned staff members. ASIO's experience in allocating and investigating public interest disclosures has been that the scheme provides appropriate protection of intelligence information, as well as protection for individuals making a disclosure.

In the past three financial years, four disclosures have been investigated and reported on, or allocated for investigation by another authority. A decision not to investigate, in accordance with section 48 of the PID Act, was made for one disclosure. During 2018–19, no disclosures were received.

Table 9: Public interest disclosures received by ASIO

Financial year	Public interest disclosures received by ASIO	Outcomes / findings
2016–17	4	▶ One report found nil findings of maladministration. ▶ One report identified disclosable conduct and was passed to Human Resources Branch to consider. ▶ Two disclosure reports were allocated to the Human Resources Branch for investigation under another authority.
2017–18	1	▶ One disclosure report was received; a decision was made not to investigate and a determination was made to refer the matter to ASIO's Human Resources Branch.
2018–19	0	N/A

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. During 2018–19 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 ASIO's human resources policy.

The ASIO Ombudsman provides valuable support and advice to employees and line managers. During 2018–19 the Ombudsman:

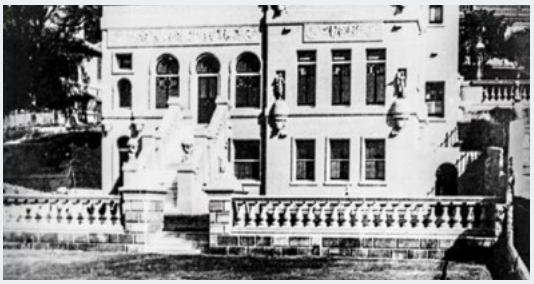
- provided advice and guidance in response to four formal contacts from staff;
- conducted one preliminary review of investigative matters;
- responded to Human Resources on four policy matter queries;
- conducted two health checks of business areas; and
- carried out two investigations relating to the Code of Conduct.

The Ombudsman met weekly with the Assistant Director-General of Human Resources; fortnightly 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.

Accommodation and facilities

In 2018–19 ASIO continued to manage a large and complex property portfolio, ensuring the working environments were secure and fit for purpose to meet our operational requirements. The property portfolio includes the Ben Chifley Building in Canberra, which continued to support the evolving business and capability needs of ASIO and our 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.

Figure 18: ASIO accommodation over time



Potts Point, Sydney (1949–51)

Queens Road, South Melbourne (1951–68)

469 St Kilda Rd, Melbourne (1968–86)

Russell Offices, Canberra (1986–2014)

SECURITY

Security of ASIO

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

Security policies and governance

In 2018–19 ASIO continued to foster a positive protective security culture, whereby security is considered in all decision-making and is perceived as a shared responsibility. This included supporting ongoing security management and training to ensure that 'promoting a security culture' is treated as a core capability requirement for all staff.

Protective Security Policy Framework

Reforms to the Australian Government's PSPF, led by the Attorney-General's Department, came into effect on 1 October 2018. The transition to the new classification system has an extended implementation period until October 2020.

ASIO Security Committee

During the reporting period, ASIO's leaders continued to promote a culture of security through the ASIO Security Committee, a senior-level committee that oversees ASIO's security policies and practices and ensures that security risk management best practice is incorporated into all aspects of our business.

e-security

Our ICT systems are subject to stringent security requirements, owing to both the large volumes of classified information processed on these systems and the sensitivity of ASIO's work. We continually work to manage and mitigate identified security risks to ASIO information and our ICT systems. This work includes strengthening ASIO systems against both trusted insider threats and external threats.

All activities on ASIO systems are audited to provide an appropriate level of assurance that ASIO systems protect information in accordance with Australian Government and partner agencies' expectations.

Safety and security training

In the current heightened threat environment, ASIO continued to direct significant resources towards ensuring the safety of our operational activities, enhancing our building security and providing safety training for staff. This involves a layered approach to personal safety and security training that begins at induction training for staff and is supplemented by a suite of courses and refresher training consistent with the nature of each officer's work.

Security assessments

Overview

ASIO's security assessment function is an important component of Australia's national security defences. It provides a mechanism for security (as defined in the *Australian Security Intelligence Organisation Act 1979*) to be considered in certain government decision-making processes.

Part IV of the ASIO Act provides the legislative basis for ASIO to furnish security assessments to a Commonwealth agency, state, or authority of a state in providing advice informing whether or not prescribed administrative action should be taken in respect of a person.[1]

Security assessments may be provided to inform decisions relating to:

- applications for employment in a Commonwealth department or agency;
- applications for security clearances under the Protective Security Policy Framework (PSPF);
- applications for access to security-restricted sites or material;
- applications for the grant of, or suitability to continue to hold, a visa;
- applications for the grant of Australian citizenship;
- applications for the grant of an Australian passport;
- requests for the cancellation of an Australian passport; and
- consideration of cessation of Australian citizenship.

Security assessments are not character checks, and factors such as criminal history, dishonesty and deceit are only relevant to ASIO's advice if they have a bearing on security.

ASIO is limited in the manner in which it may communicate with agencies seeking security assessment advice to inform the taking (or not taking) of prescribed administrative action. It may communicate in only one of three forms of assessment: non-prejudicial, qualified or adverse:

- A non-prejudicial assessment indicates that ASIO does not hold security concerns about the action being taken (or not taken) in relation to the person. This type of assessment should not, however, be construed as positive endorsement by ASIO for the person; other non-security related concerns may exist, but it is the responsibility of the agency seeking the assessment to satisfy itself on matters other than security.
- A qualified security assessment contains advice or information that is or could be prejudicial to the interests of the person but does not contain a prejudicial recommendation regarding the prescribed administrative action considered in the assessment.
- An adverse security assessment contains advice or information that is prejudicial to the interests of the person; and contains a prejudicial recommendation regarding the prescribed administrative action considered in the assessment.

Most ASIO security assessments are made at the request of another department or agency; however, it is open to ASIO to furnish an assessment as a consequence of an ASIO intelligence investigation. This happens when ASIO receives information, often via lead or liaison reporting, reaching a threshold which may cause ASIO to furnish a security assessment, or to reconsider a previously furnished assessment for an individual. Where this occurs, any new security assessment furnished by ASIO will supersede the previous assessment.

ASIO security assessments are undertaken in two key areas: personnel security assessments; and assessments related to travel, immigration and access to security-controlled areas.

ASIO acknowledges the gravity of our work—our security assessments directly affect people's lives. The assessments may affect the ability to travel, obtain employment or see loved ones. On this basis, ASIO welcomes oversight of the work we do, with oversight provided through the Inspector-General of Intelligence and Security (IGIS), the PJCIS and the Independent Reviewer of Adverse Security Assessments.

1 Prescribed administrative action is defined in the ASIO Act and includes action relating to access by a person to security-controlled locations, occupancy of a position in the Commonwealth or state, or the exercise of any power under the *Migration Act 1958*, the *Australian Citizenship Act 2007* or the *Australian Passports Act 2005*, or under specific provisions of the *Telecommunications Act 1997* or the *Security of Critical Infrastructure Act 2018*.

Personnel security assessments

Security assessments to government agencies

ASIO provides security assessments to Australian Government agencies to inform their assessment of an individual's suitability to access national security-classified information and/or areas. As stipulated in the PSPF, ASIO's personnel security assessments are a mandatory requirement of the security clearance process for Negative Vetting Level 1 (NV1) and 2 (NV2) and Positive Vetting (PV) security clearances, and Baseline clearances where national security concerns are identified. The ASIO security assessment process plays a critical role in helping partner agencies protect classified and sensitive government information, areas and resources from the threat of espionage and foreign interference, and terrorism. Further, ASIO contributes to whole-of-government development and reform of personnel security policy.

ASIO security assessments are used by the relevant department or agency to inform its deliberations on whether or not to issue or revalidate a security clearance for an individual, or to consider whether an individual should continue to hold a security clearance. The security assessment advice and/or recommendations are considered alongside other information collected through the security clearance process, and the relevant vetting department or agency makes an assessment of the individual's suitability to hold a security clearance as stipulated in the *Australian Government Protective Security Policy Framework—Personnel security adjudicative guidelines*.

When ASIO issues an adverse or qualified assessment, apart from those exemptions under Part IV of the ASIO Act, individuals are provided with a copy of the statement of grounds, which contains the information that has been relied upon in making the assessment. Subject to exemptions under Part IV of the ASIO Act (including Intelligence Community employees and non-Australian residents), where clearance subjects wish to appeal the assessment made by ASIO they may apply within 28 days to the Administrative Appeals Tribunal for a review of an adverse or qualified security assessment.

Each year ASIO completes a small number of adverse and qualified personnel security assessments containing advice and recommendations on an individual's suitability to be granted or to continue to hold a clearance. While the overall number of prejudicial assessments may be small, this does not diminish the value of the security assessment function, as history shows that a single person can be responsible for significant damage to Australia's, or our foreign partners', national security. As a result of prejudicial assessments informing decision-making, the risk to sensitive government information and/or areas has been mitigated.

Table 10: Personnel security assessments completed (2009–19)

Year	Total PSAs completed
2009–10	22 343 (2431 PV)
2010–11	31 099 (3100 PV)
2011–12	27 801 (2172 PV)
2012–13	27 586 (1789 PV)
2013–14	23 522 (1367 PV)
2014–15	23 073 (428 PV)
2015–16	31 066 (1359 PV)
2016–17	27 182 (1780 PV)
2017–18	32 153 (2759 PV)
2018–19	32 887 (4091 PV)

Notes:
PSA: personnel security assessment
PV: Positive Vetting
QSA: qualified security assessment
ASA: adverse security assessment

In 2018–19 we completed 32 887 personnel security assessments—a small increase from the previous financial year. Of these, 4091 were PV security assessments, an increase of nearly 50 per cent compared with the previous financial year.

AGSVA feedback acknowledges that the PV caseload has significantly reduced, and ASIO has succeeded, in the main, in meeting time frames agreed for PV, NV1 and NV2 security assessments in 2018–19. The increase in timeliness enabled AGSVA to meet its performance benchmarks and enabled sponsoring entities to onboard staff in a timely manner. Furthermore, the contribution provided by ASIO secondees to AGSVA—in line with the recommendations of the Independent Intelligence Review of June 2017—has reinforced the cooperation between the two agencies and enabled a greater sharing of knowledge and expertise.

Case study 3:
Adverse security assessment advises of unacceptable risk of espionage or act of foreign interference

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.

We 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 the clearance holder's 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.

Outreach

During the reporting period, 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 aimed to increase understanding of 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.

Security assessments related to immigration and access

We produce security assessments to assist the Department of Home Affairs (Home Affairs), the Department of Foreign Affairs and Trade (DFAT) and other agencies to manage security risks relating to immigration matters, such as the suitability to obtain or continue to hold an Australian visa, passport or citizenship; or access to security controlled places or things, such as sensitive air or maritime port areas, security-sensitive chemicals, biological agents and nuclear sites; and special events accreditation.

Table 11: Immigration and access-related security assessments completed (2009–19)[2]

Year	Visa and citizenship assessments completed	Access assessments completed
2009–10	38 438	98 096
2010–11	34 396	109 166
2011–12	24 097	153 644
2012–13	29 449	130 045
2013–14	27 149	159 288
2014–15	17 628	171 203
2015–16	11 962	141 820
2016–17	14 358	141 784
2017–18	5454	225 846
2018–19	4314	145 114

2 All visa and citizenship figures exclude national security border alert numbers.

As part of the immigration and access security assessment process, we work closely with internal and external partners to obtain information to inform our assessments. We have mature triaging and prioritisation processes, driven by risk considerations. Assessment officers require a breadth of subject knowledge, as each case is unique in the nature of security concern and complexity. Assessment officers apply analytical rigour to their assessments and have the full suite of ASIO's investigative tools available to them to inform their assessments. Our work requires close engagement with ASIO's Legal Services division to ensure our security assessments are in accordance with accepted legal principles and practice.

While the number of international travellers to Australia grows, without a commensurate increase in resources, the number of referrals that we can assess remains the same.[3] This means we prioritise visa and citizenship security assessment referrals to mitigate the risk of missing potential threats. Since a 2014 evidence-based internal review, we have continued to evolve our visa assessment model, moving away from reliance on the profiling of visa and citizenship applicants to a greater emphasis on watchlisting. The shift has enabled us to focus our investigative and assessment resources on resolving security indicators in relation to individuals of potential security concern, rather than diffusing resources across large caseloads of individuals who are of limited, if any, security relevance.

In addition to watchlisted referrals, we work closely with Home Affairs to identify criteria to determine which visa or citizenship applicants should be referred to ASIO for assessment. These criteria are recorded in the regularly updated Security Checking Handbook, used by Home Affairs and DFAT staff who process visa and citizenship applications.

The consequences of an immigration- or access-related security assessment depend on the purpose for which it is made and the associated legislation, regulation or policy. In some cases, decision-makers are obliged to take (or are prevented from taking) actions because of an ASIO security assessment—for immigration-related assessments, this may affect an individual's ability to travel to or remain in Australia due to a visa refusal or cancellation; while, for assessments for access to security-controlled places, a recommendation to refuse the granting of an Aviation Security Identification Card (ASIC) may affect an individual's ability to gain employment at an airport.

Appeal rights for recipients of adverse or qualified security assessments vary based on the individual's circumstances at the time the assessment was furnished, and the type of assessment furnished. Judicial review—a review of the administrative decision-making processes—is available to all security assessment recipients. For most categories of security assessment, merits review is available through the Security Division of the Administrative Appeals Tribunal (AAT). The AAT may inform itself on any matter in such a manner as it considers appropriate and can remit an assessment for reconsideration, or substitute its own decision.[4]

The recipient of an adverse or qualified security assessment may raise the matter with the Office of the IGIS. The IGIS maintains a close interest in ASIO's security assessment function. It is not a function of the IGIS to review the merits of an adverse assessment, but the IGIS may review the legality and propriety of the assessment, and adherence to associated ASIO policies and procedures.

A small number of individuals are eligible to request review of their adverse visa security assessment by the Independent Reviewer of Adverse Security Assessments (the Reviewer). The role of the Reviewer is to conduct an independent advisory review of ASIO adverse security assessments furnished to Home Affairs in relation to individuals who remain in immigration detention, having been found by Home Affairs to be owed protection obligations under international law and to be ineligible for a permanent protection visa or who have had their permanent protection visa cancelled because they are the subject of an adverse security assessment. The Reviewer examines all material ASIO relied upon in making the security assessment, provides an opinion to the Director-General of Security on whether the assessment is an appropriate outcome based on the material ASIO relied on, and makes recommendations for the Director-General's consideration.

3 The Department of Home Affairs received a record 9.6 million visa and 160 000 citizenship applications in 2018–19. Only a small subset (see table at the end of this section) of these applications were referred to ASIO for a security assessment.

4 For information on Litigation matters, please refer to Section 7.

Case study 4:
Adverse security assessment of offshore individual in relation to politically motivated violence

The loss of territory by the Islamic State of Iraq and the Levant (ISIL) has not diminished its appeal to extremists, nor its ability to inspire attacks globally. During the reporting period, an investigation into an offshore individual was initiated after the watchlisted individual applied for a visa. The individual was the subject of reporting that he intended to conduct an offshore attack in support of ISIL. The individual was identified to be in contact with members of ISIL, one of whom provided assistance and direction to carry out an attack.

We assessed that the individual was supportive of the use of politically motivated violence, and issued an adverse security assessment resulting in refusal of the visa. Investigations resulting in prejudicial assessments such as this are tangible examples of actions directly contributing to the safety of Australia and its interests.

Immigration-related security assessments

Visa and citizenship[5]

In 2018–19 ASIO provided 11 699 security assessments to Home Affairs to support its decision-making on the issuing of a range of visas and actions in relation to movements at and beyond the border. These assessments included a relatively small number of adverse security assessments in relation to individuals whom ASIO 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 terrorism grounds. These assessments informed the taking of prescribed administrative action by 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, ASIO met all current service-level agreements with the department on visa security assessments.

Throughout the reporting period, we worked closely with 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 all caseloads. We contributed to the training of Home Affairs staff in the Australia-wide visa processing network to ensure referrals made to ASIO optimally reflect those cases which could pose the greatest risk to national security. We engaged regularly with Home Affairs to ensure that systems and policies in relation to border alerts were appropriate and fit for purpose and provided training and advice to Home Affairs staff to facilitate appropriate resolution of border alerts.

5 This section discusses security assessments informing an application for citizenship, as opposed to assessments for citizenship loss, which are discussed separately (see subsection on Citizenship cessation).

Passport cancellations

ASIO furnishes security assessments to inform ministerial decision-making in relation to passport cancellation and refusal in order to prevent security-relevant travel (for example, travel to conflict regions) or to prevent travel to third countries once overseas.

Case study 5:
Adverse security assessment of onshore individual in relation to politically motivated violence

During the reporting period, an investigation into an individual who had previously attempted to travel offshore to join the Islamic State of Iraq and the Levant (ISIL) and engage in politically motivated violence identified that the individual still maintained an extremist ideology supportive of ISIL and had intent to engage in offshore politically motivated violence (PMV) or acts in support of PMV.

We assessed that, if the individual were permitted to travel overseas using an Australian travel document, they would be likely to engage in conduct that might prejudice the security of Australia or a foreign country. Following careful consideration of the consequences of depriving the individual of a personal travel document, we furnished an adverse security assessment recommending that the Minister for Foreign Affairs cancel the individual's travel document to prevent the individual from engaging in the conduct.

Citizenship cessation

Our advice to the Minister for Home Affairs in relation to citizenship cessation must be provided in the form of a security assessment because it relates to prescribed administrative action under the ASIO Act. In operation-of-law cases, we provide advice to the minister in the form of a qualified security assessment.

ASIO's security assessment relates specifically to the intelligence case as relevant to sections 33AA and/or 35 of the *Australian Citizenship Act 2007* (Citizenship Act). ASIO does not assess whether an individual is a dual national as this is a matter for Home Affairs.

Access to security-controlled places or things, and event accreditation

ASIO conducts security assessments at the request of AusCheck (an agency within the Department of Home Affairs) and the Australian Federal Police (AFP) for applicants requiring access to security-sensitive places or things. This process is mirrored in referrals received for designated special events.

In 2018–19 we provided 135 005 access security assessments to AusCheck, including in relation to individuals seeking ASICs and Maritime Security Identification Cards (MSIC). 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, in which over 99 per cent of referrals were finalised within three months of receipt. No events accreditation assessments were completed during the reporting period.

During the reporting period, we provided input into a holistic review of the ASIC/MSIC schemes conducted by the Aviation Maritime Security (AMS) division within the Department of Home Affairs. We continue to work closely with AMS to help identify improvements to the schemes.

Table 12: Access to security-controlled places (2016–19)[6]

Type of assessment	2016–17	2017–18	2018–19
Access security (ASICs, MSICs, Flight Crew etc)	132 088	144 629	135 005
Security-sensitive substances and nuclear sites	9696	9963	10 109
Events accreditation	Nil	71 254	Nil
Total	**141 784**	**225 846**	**145 114**

6 Note: The total shown in 'Event accreditation' 2017–18 comprises 68 341 assessments for the Gold Coast Commonwealth Games in April 2018, and 2913 assessments for the Association of South East Asian Nations meeting held in Sydney in March 2018.

LEGISLATION AND LITIGATION

Role of legal officers and the need for specialist staff

ASIO in-house lawyers, with their specific skill sets, continue to provide specialised legal services to the Organisation to support ASIO's operational and corporate functions. This includes advising on ASIO's mandate and functions, legislative interpretation and reform, use of special powers and operations. The Legal Services division also manages ASIO's involvement in criminal and civil litigation. The longer term trend of expanded operational remit—including border security—and expansion of external demands, including parliamentary and statutorily appointed reviewers and official inquiries, continues to create increasing demand for legal services and expertise, often within short time frames.

ASIO in-house lawyers and other specialist warrants, capability protection and legal support staff, advise and support the Organisation on:

- the execution of ASIO's special powers and other operational activity (both before and during the execution of special powers and other operational activity);
- warrants;
- security assessments;
- protection of ASIO's capabilities from compromise;
- employment, commercial, internal security, and Freedom of Information;
- management of legal proceedings involving ASIO;
- existing and proposed legislation; and
- responding to external accountability and oversight bodies, including executive and parliamentary inquiries.

Training implications

Legal Services works with client areas and ASIO's Training Branch to identify requirements for training on legislative developments and other requirements as they arise. Resources are committed to developing tailored training packages or modifying current training practices to include legislation changes.

Legal Services holds two in-house training events per year to ensure that lawyers comply with relevant compulsory professional development requirements and that all staff have relevant, targeted and accessible training. This is in addition to ad hoc training sessions and events throughout the year. Training events in 2018–19 focused on warrants, countering foreign interference, Transformation, operational planning, ethics, document management, statutory interpretation, and ASIO Act and Telecommunications (Interception and Access) Act communications powers.

Relationships with other agencies

As with all legislative changes, ASIO has ongoing interaction with agencies such as the Department of Home Affairs, the Australian Federal Police (AFP), the Attorney-General's Department and other National Intelligence Community agencies.

Legislative changes that have impacted on ASIO's administration

Significant legislation affecting ASIO and its operations was passed during the reporting period, including:

- *Counter-Terrorism Legislation Amendment Act (No. 1) 2018; and*
- the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

Further information about each of these Acts is provided below.

Counter-Terrorism Legislation Amendment Act (No. 1) 2018

The *Counter-Terrorism Legislation Amendment Act (No. 1) 2018* was passed on 16 August 2018 and began on 25 August 2018. The Act extended the provisions relating to control orders, preventative detention orders and the declared area offence, and terrorism-related stop, search and seizure powers, for a further three years. The Act also extended the provisions relating to ASIO questioning warrants and questioning and detention warrants for a further 12 months (until 7 September 2019).

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA legislation) was passed on 6 December 2018, with substantive provisions beginning on 9 December 2018. The Act was an important response to ASIO's technological challenges. It 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.

There has been a significant body of work in implementing the TOLA legislation, including developing internal training materials, presentations and templates, and consulting extensively with the Department of Home Affairs and the Office of the Inspector-General of Intelligence and Security (IGIS).

During the reporting period, ASIO used a number of the powers available under TOLA.

Implementation of specific legislation

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

In June 2018 the Australian Parliament passed the National Security Legislation Amendment (Espionage and Foreign Interference) Bill. This was a significant development that criminalised acts of foreign interference for the first time in Australia. The Act also strengthens espionage, secrecy, sabotage and related criminal offences through amendments to the *Criminal Code Act 1995* (Criminal Code), the *Crimes Act 1914* and the *Telecommunications (Interception and Access) Act 1979*. Most of the Act began on 30 June 2018, with its secrecy provisions beginning on 29 December 2018.

The Act:

- strengthens existing espionage offences and introduces a new 'theft of trade secrets' offence to protect Australia from economic espionage;
- introduces new foreign interference offences targeting covert, deceptive or threatening actions by foreign actors who intend to influence Australia's democratic or government processes or to harm Australia;
- reforms Commonwealth secrecy offences, ensuring they appropriately criminalise unauthorised disclosures of harmful information while also protecting freedom of speech;
- introduces comprehensive new sabotage offences that effectively protect critical infrastructure in the modern environment;
- modernises and reforms offences against government, including treason, to better protect Australia's defence and democracy; and
- introduces a new aggravated offence for providing false and misleading information in the context of security clearance processes.

ASIO has not yet been involved in any prosecutions under the National Security Legislation Amendment (Espionage and Foreign Interference) Act, but anticipates such prosecutions will be resource-intensive and test information protection mechanisms.

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

Foreign Influence Transparency Scheme Act 2018

The *Foreign Influence Transparency Scheme Act 2018* (the FITS Act) received royal assent on 29 June 2018. The FITS Act introduced the Foreign Influence Transparency Scheme, which is administered by the Attorney-General's Department (AGD) and began in December 2018. The scheme requires individuals and entities who undertake 'registrable activities' on behalf of foreign principals in Australia to register. 'Registrable activities' include parliamentary/political lobbying and activities for the purpose of political or governmental influence, including communications activity and disbursement activity.

Registrants are required to report any material changes affecting their registration, or disbursement activity over particular thresholds, and any registrable activities undertaken during voting periods for federal elections where the activity relates to the federal election. They are also required to make disclosures when undertaking communications activity on behalf of foreign principals.

There are various exemptions to registration under the scheme. These include activities undertaken by members of parliament, diplomatic or consular activities, and activities undertaken by an officer or employee of a foreign government under the name of the foreign principal.

Litigation matters

During the reporting period, ASIO 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, civil lawsuits and inquiries.

The Administrative Appeals Tribunal (AAT) reviewed a number of administrative decisions, including prejudicial ASIO security assessments. While the assessments primarily related to politically motivated violence, there was growth in the number of reviews of personnel security assessments. As well, current and former ASIO employees brought review proceedings challenging Comcare decisions, requiring ASIO to contribute and ensure protection of sensitive information. AAT decisions are reported on the Australasian Legal Information Institute website, Austlii (www.austlii.edu.au).

Security assessment reviews—Administrative Appeals Tribunal

Over the reporting period, ASIO was involved in 15 adverse security assessment reviews before the AAT, relating to cancelled passports, visas and security clearances.

- Four were pending at the end of the reporting period.
- Three assessments were remitted to ASIO for new assessments to be prepared, resulting in the issuing of three non-prejudicial assessments.
- Five were dismissed.
- Two were heard, with both decisions remaining reserved at the end of the reporting period.
- One affirmation was handed down.

Security assessment reviews—Federal Court and High Court reviews

Over the reporting period, 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.

Criminal prosecutions

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

REPORTING, OUTREACH AND PUBLIC ACCESS

Intelligence reporting

During 2018–19 we published 1252 intelligence and security reports for Australian partner agencies covering a range of terrorism, espionage, foreign interference and border security issues. Reporting was distributed to more than 90 federal, state and territory government organisations.

Countering espionage and foreign interference

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; and
- 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 also 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 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 work.

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.

The annual survey of stakeholders showed high regard for our assessments and advice on counter-espionage intelligence and investigations with stakeholders characterising them as being 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.

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 Five-Eyes counterpart agencies, to inform our advice was 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.

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, directly impacting on policy decisions.

We provided in-depth analysis and briefings on matters such as risks arising from the aggregation of foreign ownership in critical infrastructure, threats to the telecommunications sector, and the circumvention of foreign investment scrutiny processes. This advice informed 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.

Defence industry

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 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.

We also 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 reporting 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 ASIO's Business and Government Liaison Unit (BGLU) website for new members of the DISP. This has improved our ability to provide advice directly to defence industry.

Innovation sector

In 2018–19 we continued to develop our innovation sector outreach program in concert with other government agencies, such as the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the office of CFIC, the Department of Home Affairs and the Department of Education.

ASIO was one of the key participants in developing the Guidelines to Counter Foreign Interference in the Australian University Sector. The objective was to provide additional guidance on which universities can draw to assess risk in their global engagements, and to safeguard their people and data.

During the reporting period, we expanded the depth of our engagement with universities, research institutes and think tanks. We focused on enhancing the sector's resilience to the threats posed from espionage and foreign interference, without undermining the invaluable asset of their openness. This engagement enabled us to enhance the threat awareness of executives and boards as well as key staff engaged in research of value to foreign intelligence services.

We also provided advice to help the sector identify espionage and foreign interference risks to their people, assets, intellectual property, international partnering and business, including attempted and actual compromises of their infrastructure.

Countering terrorism

Our assessments of the terrorism threat environment continued to be in high demand among our federal, state and territory policy, security and law enforcement partners during 2018–19. 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 Islamic State in Iraq and the Levant 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.

Our annual survey of stakeholders 2018–19 indicated that our advice on counter-terrorism policy and responses played a crucial role in informing ministerial-level decisions. A significant number of our stakeholders—particularly at the state and territory-level and in the business and tertiary education sectors—regard our reports and assessments as indispensable in informing their terrorism defences. Stakeholders also commented positively on the increasing number of joint reports prepared with other agencies as being indicative of the level of collaboration between ASIO and partner agencies, and our ability to draw on the expertise of others.

In the survey, federal and state government and law enforcement stakeholders commented favourably on the manner in which ASIO engages with counter-terrorism partners; and a number of key stakeholders advised they believed the operational success of disruption operations was achieved mainly through ASIO's close collaboration efforts. Our membership of and active involvement in the multi-agency Joint Counter Terrorism Teams contributed to successful counter-terrorism disruptions and prosecutions during the reporting period.

During the reporting period, we contributed to the security awareness of the Australian and 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. In addition, we were actively involved in developing and conducting ANZCTC exercises and contributed in a similar way to Maritime Border Command's counter-terrorism exercises. We also developed specialist content for ANZCTC courses and provided expert instructors for specific courses

Border integrity

Our annual stakeholders survey showed that our analytical capability, advice and reporting are viewed 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.

Stakeholders continued to view our foreign fighter profiles as significantly contributing to enhancing border security, while our willingness to draw on our extensive range of liaison partners, often providing unique perspectives, was appreciated and valued.

Business and government

Throughout the reporting period, our protective security advice and services continued to assist government (at all levels) and businesses to manage their security risks by equipping them with credible, intelligence-backed reporting, enabling them effect positive and effective protective security practices, policies and procedures. As with previous years, our Business and Government Liaison Unit (BGLU) acted as a central conduit between ASIO and our government and industry stakeholders. BGLU coordinates and delivers information designed to enable business and federal, state and local government stakeholders with security or risk management responsibilities to recognise and respond to national security threats, develop mitigation strategies and provide informed briefings to executives and staff.

- This reporting period, the BGLU hosted fewer large briefings in ASIO Headquarters in favour of more tailored and specific briefings to discrete stakeholders. This was driven by an increase in requests for tailored information exchanges and the diminishing value of providing broad advice which has been accepted, used and acted on by many stakeholders.
- The BGLU continued to meet the ASIO commitment to provide advice to the more remote jurisdictions and hosted briefings in Western Australia (July 2018), the Northern Territory (March 2019) and South Australia (May 2019). The BGLU also used experts from outside ASIO (including from the Office of National Intelligence, ACSC, Defence and the office of the NCFIC) to complement and reinforce key messaging at these briefs.
- In conjunction with the ANZCTC Crowded Places Advisory Group (CPAG) and Business Advisory Group (BAG), the BGLU hosted the inaugural (now annual) ASIO Crowded Places brief and BAG Forum over two days (10–11 October 2018) in ASIO Headquarters.
- The BGLU continued to produce and disseminate domestic and international security information through its secure website. In 2018–19, we published 45 ASIO reports—including six ASIO-T4 Protective Security directorate (ASIO-T4) protective security managers guides—on the website, and subscriber numbers continue to grow as stakeholders are encouraged to subscribe when BGLU (and other ASIO) staff meet with them.

ASIO-T4 Protective Security

The role of the ASIO-T4 Protective Security (ASIO-T4) section 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. In 2018–19 we continued to provide high-quality, comprehensive and timely intelligence-led protective security advice and services to our national security partners. 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 jurisdictional 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 other ASIO-T4 courses, remains oversubscribed, and feedback from attendees continued to be very positive.
- ASIO-T4's Technical Surveillance Counter Measures (TSCM) team provided security assurance to Australian Government domestic customers, while also deploying overseas to assist partner agencies in the Americas, Asia and Pacific regions; further site-specific advice was given to improve customers' security posture. The TSCM team continued to provide support to investigations of suspected technical surveillance against Australian Government and industry partners.

Our annual stakeholder survey indicated that ASIO-T4's protective security advice and services—including briefings, reports and guides—are regarded highly favourably and of great use in managing security risks. Stakeholders continued to value the BGLU 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.

Public access to ASIO records

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 to facilitate access to ASIO records, while balancing various and sometimes competing priorities.

In 2018–19 we 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 13: 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%	60.0%

Public statements and the media

The Director-General and Deputy Directors-General are publicly identified ASIO officers and undertake public outreach through media responses, public speeches and appearances at various parliamentary forums. They also speak at select public seminars or conferences. ASIO's website has information on public speeches and statements made in 2018–19.

The media can contact ASIO directly through a publicly listed media contact number and email address. In 2018–19 ASIO continued to respond to media inquiries, without commenting on operations, investigations, individuals or operational capabilities.

OVERSIGHT AND SPECIAL POWERS

ASIO must operate in a manner that is consistent with our values of Excellence, Integrity, Respect, Cooperation and Accountability. These five values incorporate our firm commitment to operate lawfully, in proportion to threats we are investigating, and in line with the standards and expectations of the Australian community. A comprehensive oversight and accountability framework comprising legislation and ministerial, parliamentary and independent oversight provides assurance that we will continue to meet our commitment.

Ministerial accountability

The Minister for Home Affairs exercises all the powers and functions under the ASIO Act except those that remain explicitly with the Attorney-General. These remaining powers reflect the Attorney-General's role as First Law Officer, with responsibility for integrity and oversight, and include issuing ASIO warrants and authorising special intelligence operations.

We keep our portfolio minister informed of significant national security developments, as well as other important issues affecting ASIO. During this reporting period, we provided advice to the Minister for Home Affairs and to the Attorney-General on a range of investigative, operational and administrative issues, which were communicated primarily through more than 240 formal submissions. The Director-General also briefed other ministers on security issues and matters relevant to their portfolios, when required.

We conduct our security intelligence activities in accordance with the Attorney-General's Guidelines, which are available online at www.asio.gov.au. The guidelines stipulate that we must conduct our activities in a lawful, timely and efficient manner, while applying the principle of proportionality—that is, the methods used to investigate a person must be proportional to the threat posed—to ensure the least intrusion necessary into an individual's privacy. Carriage of the guidelines has transferred to the Department of Home Affairs from the Attorney-General's Department (AGD). ASIO and Home Affairs are progressing the review of the guidelines.

The Attorney-General issues all warrants for ASIO to employ its special powers, except for questioning warrants, and questioning and detention warrants, which are issued by a 'prescribed authority'. If we judge that a warrant is required, the Director-General presents a warrant request to the Attorney-General. Most warrant requests are independently reviewed by the AGD before progressing to the Attorney-General. The Attorney-General considers the request and, if in agreement, issues the warrant. For every warrant issued, we must report to the Attorney-General on the extent to which the warrant helped us carry out our functions.

Engagement with parliament

Annual report to parliament

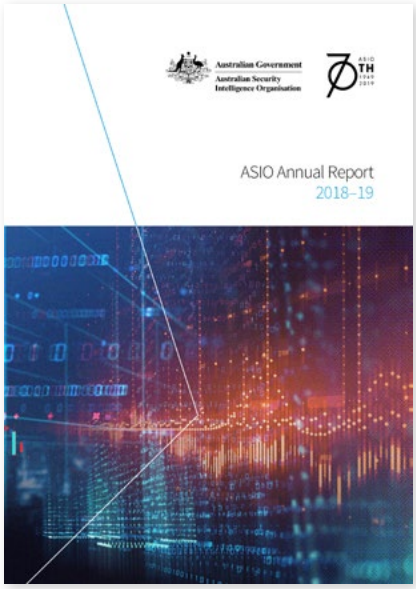
ASIO's annual report to parliament for 2018–19 was tabled on 16 October 2019. Our key performance outcomes for the reporting period detailed in the annual report are described in greater detail in 'Organisational performance', above.

Annual report classified appendix

We also produced a classified appendix to fulfil the scope of ASIO's reporting requirements under section 94 of the ASIO Act. This contains financial year statistics on:

- special intelligence operation authorisations;
- authorisations for telecommunications data access;
- use of technical assistance requests, technical assistance notices and technical capability notices; and
- use of special powers warrants.

To comply with the determination issued to ASIO by the Minister for Finance under Section 105D of the PGPA Act, these appendixes were withheld from the version of the annual report to parliament, to avoid prejudice to ASIO's activities.



Consistent with previous years' practice, a copy of the classified appendix in relation to telecommunications data access authorisations was provided to the Chair of the PJCIS to help the committee fulfil its role in assessing the overall operation and effectiveness of data retention legislation. This was provided to the PJCIS chair on 15 October 2019.

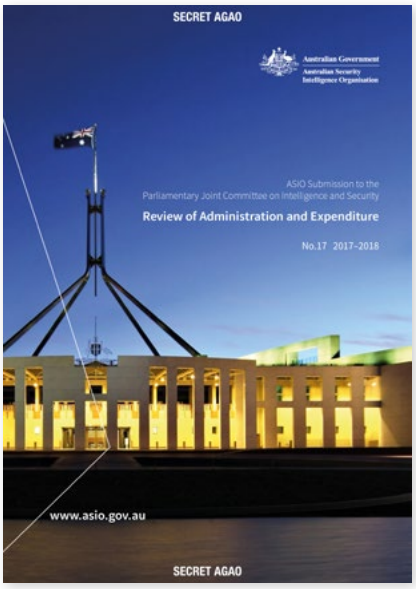
Leader of the Opposition

The Director-General of Security is a statutory position, with the responsibility to provide impartial advice. The ASIO Act requires the Director-General to regularly brief the Leader of the Opposition on security matters and to provide them with a copy of ASIO's annual report. Throughout 2018–19, classified briefings on specific security cases were provided for shadow ministers.

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. ASIO provided a classified and unclassified submission for the PJCIS Review of Administration and Expenditure No. 17 (2017–18) in December 2018.

The PJCIS also reviews the listing of terrorist organisations under the *Criminal Code Act 1995* and key national security legislation. During 2018–19 ASIO appeared at a number of hearings about the re-listing of terrorist organisations.



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 the Review of the Counter-Terrorism Legislation Amendment Bill, two inquiries 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.

Senate Legal and Constitutional Affairs Committee

ASIO 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)

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 ASIO fulfils its 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 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. ASIO is committed to acting with legality and propriety, and in 2018–19 we continued to take action to address areas that the IGIS had identified as needing improvement and further attention.

In 2018–19 the IGIS finalised and made recommendations on three inquiries related to ASIO. 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.

The Hon. Margaret Stone was appointed Inspector-General of Intelligence and Security in August 2015.

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.

During the reporting period, ASIO provided classified briefings and documentation in support of the INSLM's reviews of:

- the prosecution and sentencing of children for Commonwealth terrorism offences; and
- the operation, effectiveness and implications of terrorism-related citizenship loss provisions contained in the *Australian Citizenship Act 2007*.

The current INSLM, Dr James Renwick SC CSC, was appointed on 13 February 2017.

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 visa, or who have had their 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, examining all 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.

The Independent Reviewer's terms of reference and other relevant information are available at www.ag.gov.au/asareview.

In March 2019, Mr Robert Cornall AO was reappointed as the Independent Reviewer for a further term of two years, which expires on 26 March 2021. As at 30 June 2019, the Independent Reviewer had two adverse security assessments under consideration.

Use of ASIO special powers

The Attorney-General issues all warrants for ASIO to employ its special powers, other than questioning warrants and questioning and detention warrants, which are issued by an issuing authority.[7] If ASIO assesses a warrant is required, the Director-General requests the Attorney-General issue the warrant.

Warrant requests are usually independently reviewed by the Attorney-General's Department before progressing to the Attorney-General. The Attorney-General considers the warrant request and, if satisfied that the grounds on which the Director-General of Security requests the warrant are reasonable, the Attorney-General may issue the warrant.

There is no legislative requirement for the Attorney-General's Department to review warrants—this is general practice only. There are some instances where warrants are provided directly to the Attorney-General without being reviewed by the department. In these cases, the Attorney-General is informed that the department has not been involved in progressing the respective warrants. Warrants that are provided directly to the Attorney-General may involve sensitive counter-espionage matters or extremely compartmented collection methods. The decision to provide the warrant directly to the Attorney-General is made on a case-by-case basis.

To perform its functions, ASIO is authorised under the ASIO Act, the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997* to undertake the following methods of investigation:

- the use of telecommunications interception and access;
- the use of surveillance devices;
- entry to and search of premises;
- the use of computer access;
- the use of a range of conditionally approved ASIO Act powers in relation to an identified person (identified person warrants);
- the examination of postal and delivery service articles,
- the requiring the assistance of a relevant individual to access a computer, computer system; and
- the requiring or requesting assistance from communications providers.

In the case of a questioning or questioning and detention warrant, the ASIO Act also enables ASIO, with the Attorney-General's consent, to seek warrants from an issuing authority for investigations relating to terrorism offences.

In the case of identified person warrants (IPW), the initial (or parent) warrant is issued by the Attorney-General and provides conditional approval to exercise a range of ASIO Act powers to investigate the prejudicial activities of an identified person. The warrant, of itself, does not authorise investigative activity under the warrant. For operational activity to commence, a further authorisation (an IPW Authorisation) must be sought from the Attorney-General or the Director-General of Security in respect of each of the powers authorised in the parent warrant.

In seeking warrants, ASIO must comply with the Attorney-General's Guidelines. For every warrant issued, ASIO must report to the Attorney-General on the extent to which the warrant assisted ASIO in carrying out its functions.

7 'Issuing authority' is defined as a person who is appointed under section 34AB of the ASIO Act and who is a judge.

Warrants and authorisations 2018–19

Reporting in detail of ASIO warrants and authorisations is classified, apart from questioning warrants and questioning and detention warrants. Information on the latter is at table 14.

Details of the number of ASIO warrants issued and special powers exercised, as well as authorisations for telecommunications data under section 94 of the ASIO Act, were provided to the committee on 15 October 2019, after publication of ASIO's annual report (see above).

Table 14: Report on use of questioning warrants and questioning and detention warrants (2016–19)

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

Appendix A

Review of Administration and Expenditure No. 18 (2018–19)

Terms of Reference

In its evaluation of administration within the agencies, the Committee seeks a submission from each agency addressing the following matters:

- strategic direction and priorities;
- changes (if any) to the structure of the organisation;
- corporate governance, including information about compliance performance, risk assessment and risk management;
- legislative changes that have impacted on administration of the agency, including, as appropriate, the frequency and nature of use of any new powers, staffing implications, training, the role of legal officers and need for specialist staff, and the relationship with outside agencies such as police or the judiciary;
- involvement (if any) in litigation matters, including any administrative reviews in the Administrative Appeals Tribunal;
- human resource management, including;
  - staffing numbers and demographic information;
  - recruitment and retention strategies;
  - recruitment outcomes;
  - staff departures and separation rates;
  - workplace diversity statistics and initiatives;
  - training and development;
  - language skills;
  - individual performance management;
  - staff feedback, complaints and investigations (including public interest disclosures and any code of conduct, fraud, or bullying/harassment-related investigations); and
  - accommodation and facilities, including all locations within Australia where staff are present and any current or planned changes to accommodation arrangements;
  - changes to the distribution of staff across different areas of the organisation, including the ratio of field and operational staff to administrative staff, the ratio of executive to middle and lower level staff, and the ratio of central office to outlying staff;
- security issues, including policies, training, security breaches and e-security;
- initiatives implemented or underway to ensure compliance with the new Protective Security Policy Framework;
- security clearances, including clearance rates, number of revocations, current procedures, policy changes, average timeframes, delays and any associated outsourcing arrangements;
- information and communications technology initiatives;
- organisational performance evaluation and accountability, including any outcomes relevant to administration and expenditure for the financial year; and
- public relations and/or public reporting, including requests for public access to records.

Specific to the administration of individual agencies, submissions should address:

- in relation to the Australian Security Intelligence Organisation (ASIO):
  - the number of warrants issued and special powers exercised (in total and categorised by type);
  - the annual report on authorisations for telecommunications data pursuant to paragraphs 94(2A)(c)-(j) of the *Australian Security Intelligence Organisation Act 1979*;
  - the processes for producing security assessments of individuals for different purposes (such as visa, passport and citizenship applications), including:
    - triggers for assessments;
    - outcomes of assessments (such as adverse or qualified) and the implications for individuals;
    - consequences for assessments;
    - avenues of appeal open to different types of individuals;
    - number of different types of assessments issued during the last ten years and number of un/successful appeals;

- in relation to agencies operating under the *Intelligence Services Act 2001* (SA):
  - the number of ministerial authorisations issued (including class authorisations) and the number of activities undertaken under a ministerial authorisation, categorised by type;
- in relation to the Australian Secret Intelligence Service:
  - the number of activities undertaken in support of ASIO pursuant to section 13B of the ISA, and the number of these activities undertaken without notice from ASIO pursuant to subsection 13B(3) of the ISA;
  - an update on implementation of projects announced in the 2015-16 Budget to strengthen ASIS capabilities, including ICT system upgrades;
- in relation to the Defence Intelligence Agencies:
  - an update on the Australian Government Security Vetting Agency's efforts to reduce processing timeframes for positive vetting security clearances; and
  - an update on the *Pathway to Change – Evolving Defence Culture* initiative, including progress made to date and any impediments to progress.
- in relation to the Australian Signals Directorate:
  - an overview of the cyber security threat environment;
  - an overview of the activities of the computer emergency response team;
  - efforts to collaborate with the private and public sector to share information on threats and increase cyber resilience;
  - programs to increase governments, industry and community awareness of cyber security.
- In relation to the Office of National Intelligence:
  - a description of enterprise management initiatives planned or underway, for example:
    - recruitment and training programs;
    - planning and development of intelligence capabilities (including the Intelligence Capability Investment Plan and the administration of the Joint Capability Fund);
    - whole of NIC approaches to ICT interoperability and data;
    - programs aimed at facilitating integration, collaboration or innovation in the NIC.

In order to provide the Committee with a clear indication of trends, data from the previous two financial years should be included alongside data from the 2018-19 financial year where possible.

In relation to expenditure, the Committee will seek evidence as to each agency's ability to meet its objectives within budget parameters. The Committee requests that submissions include financial statements and address:

- the overall financial position of the agency;
- the impact any funding increases and budget measures;
- any budget constraints;
- the ongoing implications of the efficiency dividend (where applied) and other savings measures;
- efficiencies and savings measures implemented within the organisation;
- financial controls;
- the status and key deliverables of significant capital expenditure projects, including any changes to the budget, scope or timeframe for each project; and
- any significant changes in recurrent expenditure compared to previous years (both in total and in individual expenditure items), including the nature of and reasons for those changes.

In addition to the terms of reference, the committee requested information on the security environment and on the implementation of the *National Security Amendment (Espionage and Foreign Interference) Act 2018* and the *Foreign Influence Transparency Scheme Act 2018*.

19-11422