Australian Government
Australian Security Intelligence Organisation

ASIO submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure

No. 17 2017–18

www.asio.gov.au

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. 17 provides a detailed account of ASIO's administration and budgetary activities during the financial year 2017–18. The submission addresses specific information requests from the PJCIS, including on the following:

- strategic direction and priorities;
- corporate governance and organisational performance;
- legislative changes that have impacted on the administration of the agency;
- 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 strategies and outcomes, and workplace diversity statistics and initiatives;
- training and development, and individual performance management;
- staff feedback, complaints and investigations;
- accommodation and distribution of staff;
- security issues;
- information and communications technology initiatives; and
- public relations and public reporting.

This submission also provides the committee with information requested on ASIO's overall financial position, the impact of funding increases and budget measures, budget constraints, efficiencies and savings measures, financial controls, notable capital expenditure projects, and significant changes in recurrent expenditure.

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

ASIO'S ROLE AND FUNCTIONS

ASIO's purpose is to protect Australia, its people and its interests from threats to security, through intelligence collection and assessment and the provision of advice to the Australian Government, government agencies and business. In 2017–18 we pursued our purpose through four key activities:

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

ASIO's statutory functions are set out in the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), with 'security' defined as the protection of Australia and its citizens from:

- espionage;
- sabotage;
- politically motivated violence;
- the promotion of communal violence;
- attacks on Australia's defence systems;
- acts of foreign interference; and
- serious threats to Australia's territorial and border integrity.

This definition also includes the carrying out of Australia's obligations to any foreign country in relation to the above matters.

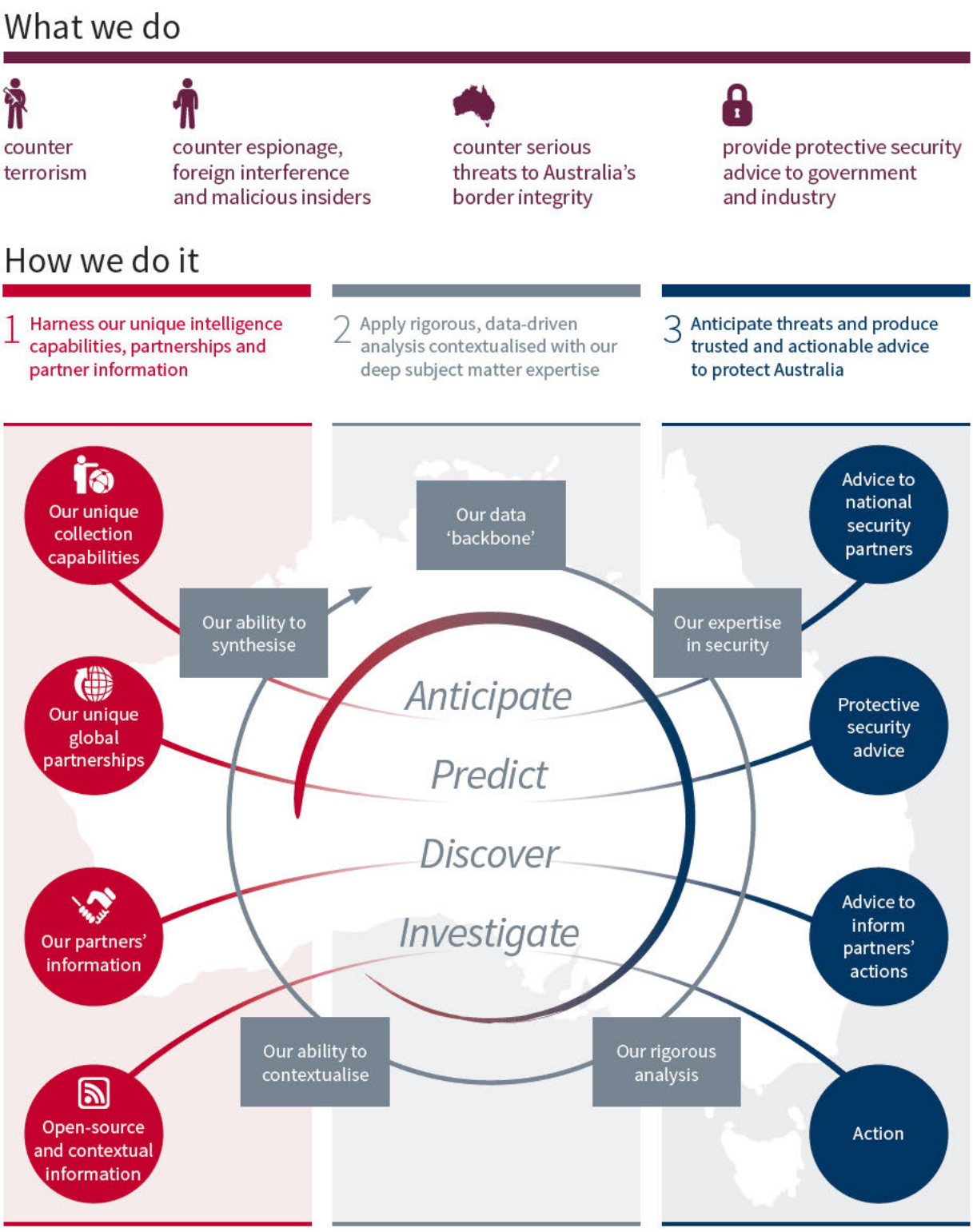
The ASIO Act authorises ASIO to provide security advice in the form of a security assessment to government agencies to inform their decision-making about prescribed administrative action in regard to:

- people seeking entry to Australia;
- people seeking access to classified material and designated security-controlled areas; and
- people seeking access to hazardous chemical substances regulated by licence.

Section 17(1)(e) of the ASIO Act authorises ASIO to obtain foreign intelligence within Australia, including under warrant, on matters related to national security, at the request of the Minister for Defence or the Minister for Foreign Affairs.

In responding to and investigating matters of national security, ASIO works closely with a range of stakeholders, including members of the National Intelligence Community, law enforcement agencies, government departments, industry and members of the public. This engagement includes providing protective security advice to industry and communicating and cooperating with relevant authorities of foreign countries, as approved by the Attorney-General.

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



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. Since September 2014, when the national terrorism threat level was raised, there have been 15 major disruption operations of imminent attack planning and seven terrorist attacks targeting people in Australia.

The principal source of the terrorist threat to Australia remains Sunni Islamist extremism; it primarily emanates from individuals and small groups who are directed, inspired or encouraged by overseas terrorist groups. All but one of the seven onshore terrorist attacks and disruptions have been related to Islamist extremism.

However, the threat of terrorist attacks is not isolated to Islamist extremists. Individuals motivated by other ideologies—such as an extreme left-wing or right-wing ideology—may consider conducting an act of terrorism.

The trend in the West has been towards targeting people over other targeting options, including infrastructure. Directly targeting people in crowded places can lower the level of complexity required for an attack to be successful, and it has the potential to achieve a number of key terrorist objectives, including multiple casualties, the generation of fear, and media attention.

The most likely form of terrorism in Australia remains an attack by an individual or small group using simple attack methodologies: of the seven successful terrorist attacks Australia has experienced, three involved the use of knives, three involved firearms, and one was a mixed-mode attack involving the use of a knife and a vehicle containing gas cylinders. However, the possibility of more complex attacks cannot be ruled out. Disrupted attack plans during the reporting period demonstrate that extremists have also considered unconventional weapons and more advanced terrorist tactics, such as using poison and large-scale, mixed-mode attacks.

A range of online extremist information provides weapons and tactics advice on how to conduct an attack and increase its lethality. This literature includes simple instructions on how to use readily available materials to make weapons, such as homemade explosives. Publicity about terrorist incidents is likely to provide further guidance and inspiration to terrorists.

Islamist extremist propaganda continues to be produced and disseminated by supporters and extremist groups offshore. This propaganda calls for attacks in Western countries, and we continue to expect that, for years to come, this propaganda will remain accessible and will seek to justify the use of violence.

Dispersal of foreign fighters

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

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

Australian returnees

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

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

All overseas Australian terrorism suspects, including those seeking to return to Australia, are handled in accordance with Australian Government frameworks. These frameworks support whole-of-government coordination in handling such cases and ensure that each individual is managed in light of the threat they pose, the nature and potential criminality of their activities, and the level of their engagement with extremist groups. ASIO works closely with other Australian agencies to identify the threat each of these individuals might pose and ensure appropriate treatment plans are in place.

Assistance to whole-of-government counter-terrorism activity

ASIO supports various whole-of-government disruption and mitigation activities short of prosecution. These include citizenship loss and passport cancellation processes, as well as 'declared area' processes and the proscription of extremist groups.

In addition to its investigative role, ASIO supports Joint Counter-Terrorism Teams through contributions to briefs of evidence, thus assisting the prosecution of individuals for terrorism and related offences.

Violent protest and communal violence

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

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

Australia continues to experience low levels of communal violence, although incidents in response to specific local or international events that resonate with expatriate communities do occur occasionally.

Espionage and foreign interference

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

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

We focus on influence activities that accord with the ASIO Act definition of 'acts of foreign interference'—that is, activities relating to Australia that are conducted by or on behalf of a foreign power and are clandestine or deceptive and are for intelligence purposes or to affect political or governmental processes or are otherwise detrimental to the interests of Australia; or involve a threat to any person. Covert influence activities and acts of foreign interference represent a threat to Australia's sovereignty and the integrity of Australia's national institutions and impinge on community and individual freedoms.

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

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

Cyber threats continue to evolve with changes in technology, and we regularly observe cyber espionage activity targeting Australia. Foreign state-sponsored adversaries target the networks of the Australian Government, industry and individuals to gain access to information and progress other intelligence objectives. The number of countries pursuing cyber espionage programs is expected to increase, as these programs can offer significant intelligence returns with relatively low cost and plausible deniability.

The blurring of traditional lines between the cyber activities of state actors and those of non-state actors means that attributing cyber intrusions to a source can be a difficult and lengthy process. It is therefore vital that we continue to develop our capabilities to ensure we can assist government to respond quickly and proportionally to any cyber intrusions.

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

A focus for us during this reporting period was supporting the development of a suite of policy and legislative measures to counter the espionage and foreign interference threat to Australia, and working with key stakeholders—primarily the Australian Federal Police—to start implementing these measures. We provided advice and assessments that:

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

These legislative measures were subsequently enacted by parliament in the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* and the *Foreign Influence Transparency Scheme Act 2018*. These laws provide valuable new tools to help combat espionage and foreign interference, offer a significant public deterrent and make it more difficult for our adversaries to conduct interference or espionage in Australia. In our view, the new espionage and foreign interference offences and the Foreign Influence Transparency Scheme regime will impose appropriate restrictions on foreign and Australian entities seeking to act contrary to Australia's sovereignty, security and prosperity, while including important protections for Australia's democracy.

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

Border integrity

Australia remains an attractive target for terrorist groups, and Australia's border integrity and security form a critical part of Australia's defences against the terrorist threat. The collapse of ISIL's so-called caliphate has created an increased movement of potential terrorists across the globe. In 2017–18, ASIO continued to mitigate these threats to Australia's security by ensuring that individuals posing a security risk were denied entry to Australia.

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

In 2017–18 we completed 5454 visa security assessments, and we met all service-level agreements with Home Affairs on visa security assessments. In 2016–17, we finalised 14 358 visa security assessments. The decrease in the number of finalisations this financial year is due to changes to the security assessment referral criteria, which resulted in a decrease in Home Affairs referrals to ASIO for assessment. We continue to refine our processes and procedures to ensure our focus is on the highest priority caseloads.

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

Accreditations

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

Disruptions

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

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

Table 1: Visa security assessments

Type of entry	2015–16	2016–17	2017–18
Temporary visas	3515	3782	1746
Permanent residence and citizenship	985	2248	294
Onshore protection (air)	75	212	66
Offshore refugee/humanitarian	1772	2265	919
Illegal maritime arrivals	864	546	95
Other referred caseloads	4751	5305	2334
TOTAL	11 962	14 358	5454

Notes:
1. Excludes assessments undertaken to resolve potential matches to national security border alerts

Figure 2: ASIO at a glance 2017–18

STRATEGIC DIRECTION, PERFORMANCE AND CORPORATE GOVERNANCE

Strategic direction

ASIO is operating at a time of unprecedented change. The security environment is more complex than it has ever been, with overlapping peaks in both our counter-terrorism and our counter-espionage programs. At the same time, rapid technological change has disrupted our operating environment, and we need to adapt to that change to ingest and make sense of increasing volumes of data. We are entering a new phase in ASIO's history—one characterised by significantly shifting government and community expectations and evolving views on privacy and security.

In 2017–18, in response to these change imperatives, the Director-General of Security commissioned Mr David Thodey AO to conduct a review of ASIO's technology state and provide recommendations on the systems, processes, governance and resources to support ASIO in the future. Mr Thodey's report, *A digital transformation of the Australian Security Intelligence Organisation*, recommended that ASIO fundamentally overhaul its technology and operating model and develop one that is more able to thrive in the contemporary security and technology environment.

To drive this program of major transformational change, in January 2018 ASIO established the Enterprise Transformation Office (ETO), based in the significant work driven by the ASIO2020 program and the Enterprise Technology Strategy of the previous reporting period. During 2018, the ETO built the foundations needed to begin and sustain ASIO's transformation, including the development of the ASIO Strategy 2018–23.

Future transformation efforts will require significant new financial investment, primarily in technology, and the adoption of a new operating model. The model will focus on driving four key 'shifts' in ASIO:

1. becoming a data-driven enterprise;
2. adopting contemporary ways of working;
3. ensuring ASIO is adaptive; and
4. instituting a culture of strategic partnering.

Movement into the Home Affairs portfolio

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

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

Corporate plan

ASIO published its corporate plan 2017–18 on 31 August 2017, in line with the requirements of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The 2017–18 corporate plan built on the 2016–17 corporate plan, reinforcing ASIO's commitment to protecting Australia, its people and its interests from threats to security by providing effective security intelligence advice and services to the Australian Government, national security partner agencies and industry. The four key activities identified in the plan were:

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

Foreign intelligence collection—the fifth key activity in the 2016–17 corporate plan—is now managed as a subset of the 'Countering espionage, foreign interference and malicious insiders' activity.

ASIO's corporate plan 2018–19 was finalised after the conclusion of the 2017–18 reporting period and published in July 2018. The 2017–18 and 2018–19 plans are available online at www.asio.gov.au.

2017 Independent Intelligence Review

In 2016–17, the Prime Minister commissioned Professor Michael L'Estrange AO and Mr Stephen Merchant PSM to undertake an independent review of the Australian Intelligence Community (AIC). The Prime Minister released the review's report in July 2017.

The review found that Australia's intelligence agencies are highly capable and staffed by skilled officers of great integrity. The review made 23 recommendations to strengthen the AIC's structural, resourcing, capability, legislative and oversight arrangements. ASIO supported the recommendations of the review and has contributed to whole-of-government work to implement the review's recommendations.

Organisational performance

Each year ASIO sets out its performance objectives for the forthcoming year in its corporate plan, in line with the requirements of the PGPA Act. The Organisation monitors its performance against those objectives throughout the year and at the end of the year prepares an annual performance statement setting out whether those objectives were achieved. The performance statement is informed by a range of information sources, with ASIO's annual stakeholder survey playing an important role in capturing our stakeholders' independent evaluations of ASIO's performance. The annual performance statement is published in ASIO's annual report.

The *ASIO annual report 2017–18* was tabled in parliament on 18 October 2018 and is available on the ASIO website, www.asio.gov.au. The report highlights ASIO's key performance outcomes for the reporting period, which include:

- working with Australian Government policymakers and providing advice to support parliament's consideration of legislative measures to strengthen Australia's efforts to counter harmful espionage and foreign interference affecting Australia's national interests, culminating in the passage of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* and the *Foreign Influence Transparency Scheme Act 2018*;
- our significant contributions to the disruption of, and subsequent government and industry responses to, planned terrorist attacks in Australia (Operation Silves and Operation San Jose);
- providing support to the security planning and accreditation for special events held in Australia, including the Gold Coast 2018 Commonwealth Games (GC18) and the ASEAN–Australia Summit—as part of this work we conducted over 71 000 assessments of individuals requiring accreditation for the events;
- publishing more than 1400 intelligence reports, threat assessments and analytical reports on terrorism, espionage and foreign interference and border security issues, to support the work of the Australian Government and our national security partners in responding to security threats; and
- providing highly sought-after protective security advice to government and industry security managers, including through the Business and Government Liaison Unit (BGLU) website, BGLU's tailored industry briefing days and ASIO-T4's physical security advice.

The effectiveness of our performance was confirmed by stakeholder responses in our 2018 annual stakeholder survey, which was conducted by an independent senior reviewer and involved interviews with 74 senior stakeholders from 66 federal, state and territory government bodies, industry and academia. The reviewer found that ASIO continues to be highly regarded as an effective partner, offering high-quality and largely unique services, and that we are perceived as a very credible organisation, with officers that are customer-focused, well trained and professional. Findings included the following:

- Stakeholders in federal and state governments and law enforcement regarded our counter-terrorism advice as timely, of high quality and very influential in informing their efforts to disrupt and defend against terrorism.
- Stakeholders said we had worked effectively with security and law enforcement agencies to ensure the success of protective security aspects of GC18. They viewed the GC18 effort as being characterised by close cooperation and unprecedented information-sharing.

- Government and industry stakeholders said that reporting and assessments disseminated by the BGLU and sectoral briefing days were valuable, influential and essential in informing the measures they implement to defend against terrorism.
- Stakeholders said that our advice informing policy development and responses to espionage, foreign interference and malicious insiders was trusted and respected. They noted, in particular, that our advice had been influential in informing the Australian Government's response to the Sergei Skripal poisoning.
- Stakeholders also commented favourably on the increasing quality and range of ASIO reports. Foreign Investment Review Board representatives noted the high quality and continuing improvement of our advice and briefings on the foreign investment threat.
- Stakeholders said the quality of our briefings for politicians, senior office holders and officials was of a very high standard. Our tailored briefings on foreign states of concern and the management of electronic devices during travel were particularly sought after and highly regarded by those about to travel.
- Home Affairs said our contribution to border security policy development during the year—as well as our security assessments and intelligence assessments on people-smuggling and our advice on emerging potential threats—had been influential. They said our extensive reporting and assessments on aviation security threats, in particular, had made an important contribution to their development of new measures to further strengthen security at Australia's ports of entry. Our ability to draw on our extensive range of international liaison partners, who often provide unique perspectives on border security issues, was also considered valuable.
- Stakeholders said ASIO-T4's expertise and contribution to national protective security arrangements during this reporting period were highly regarded. They noted the ASIO-T4 series of security manager and critical infrastructure guides as an impressive body of work.
- While acknowledging that our personnel security assessments are only one part of the vetting process, many stakeholders reiterated their concerns about the time taken to issue them.

Organisational structure

ASIO's structure evolved further in 2017–18 to reflect our focus on enterprise transformation through technology and the strategic use of resourcing. In addition, executive functions were restructured to provide an increased focus on the essential areas of accountability and oversight, as well as on strategy and reform.

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

Performance challenges in 2017–18

While ASIO achieved the majority of the performance objectives set out in its 2017–18 corporate plan, the scale and seriousness of the terrorism, espionage and foreign interference threats facing Australia have continued to put significant pressure on the Organisation's work programs.

The heightened espionage and insider threat has increased demand for assurance about staff with access to Australia's most sensitive information and capabilities. This is reflected in the significant increase in demand for ASIO security assessments for Top Secret Positive Vetting (PV) clearance holders. Our assessment that we have *substantially* achieved our performance objectives for corporate plan measure 2(b)—'National security partner agencies use our advice to disrupt and defend against harmful espionage, foreign interference and malicious insiders'— acknowledges that, while we have performed well in most of the activities that contribute to this measure, including in completing security assessments for non-PV clearances, there is more work to be done to meet agreed time frames for PV clearances.

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

Figure 3: Organisation structure

as at 30 June 2018

Duncan Lewis

DIRECTOR-GENERAL OF SECURITY

- Chief Transformation Officer
- Chief Digital Advisor

Deputy Director-General
STRATEGIC ENTERPRISE MANAGEMENT GROUP

- New policy implementation

First Assistant Director-General

- State Manager NSW North
- Executive
- State Manager Vic. South
- Corporate and Security
- Office of Legal Counsel

Assistant Director-General

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

Deputy Director-General
OPERATIONAL SUPPORT AND CAPABILITIES GROUP

First Assistant Director-General

- Technical Capabilities
- Operational Capabilities
- Information

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

- Operations and Assessments Capability and Strategy

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 Coordination	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			

Corporate governance

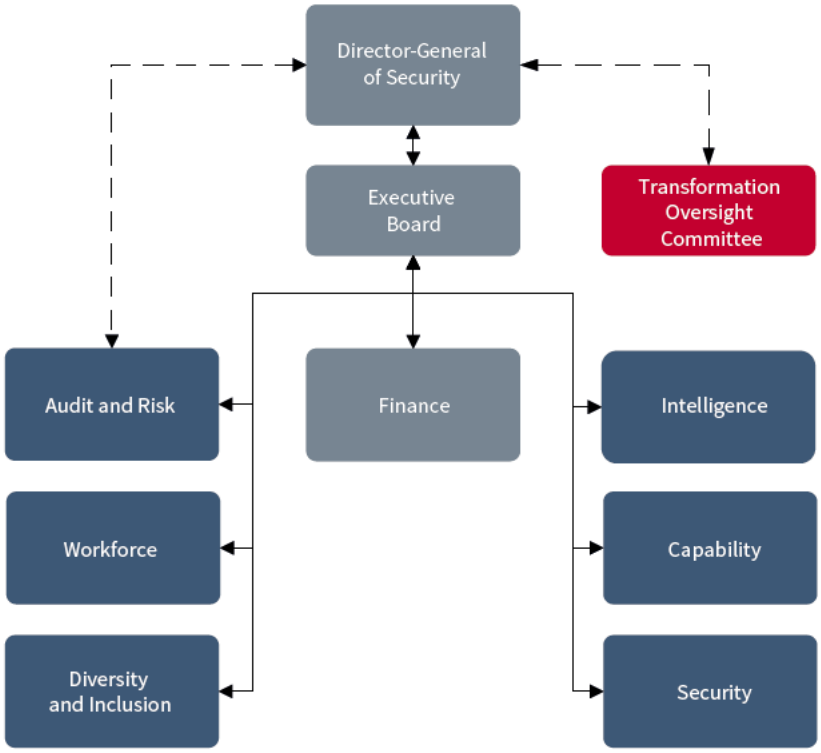
The Director-General of Security is the accountable authority for ASIO under the PGPA Act. Our Executive Board and corporate governance committees support the Director-General to fulfil his responsibilities under the PGPA Act. Their roles are to provide strategic direction, manage risk, coordinate effort and evaluate performance in support of ASIO's purpose and corporate governance arrangements for our work programs.

New governance arrangements were implemented during this reporting period to strengthen our oversight of performance and risk management. In addition to our existing corporate governance committees, the Executive Board established three new standing committees and commenced a new performance- and risk-reporting regime.

One of the three new committees included the Transformation Oversight Committee, which was established in February 2018. Its establishment reflects a recommendation from the Thodey Review that there be governance arrangements to support ASIO's transformation.

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

Figure 4: Governance standing committees 2017–18



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 ASIO's peak advisory committee, assisting the Director-General to govern ASIO. Its membership comprises the Director-General, the Deputy Directors-General, the Chief Transformation Officer and an external member.

The board met every two months during this reporting period, setting ASIO's overall strategic direction and overseeing the management of its resources. The board received regular reporting from ASIO's 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 enterprise transformation and diversity and inclusion goals.

Intelligence Committee

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

Workforce Committee

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

Security Committee

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

Finance Committee

The Finance Committee oversaw the governance arrangements and decision-making for ASIO's financial management program. The committee met monthly during this reporting period and conducted triannual reviews of performance and risk. Financial governance has now been taken up by the Executive Board under the direct supervision of the Director-General.

ASIO Diversity and Inclusion Committee

The ASIO Diversity and Inclusion Committee oversaw governance arrangements and decision-making for ASIO's diversity and inclusion program. The committee met monthly during this reporting period and conducted triannual reviews of performance and risk.

Capability Committee

The Capability Committee oversaw governance arrangements and decision-making for ASIO's capability program. The committee met bimonthly during this reporting period and conducted triannual reviews of performance and risk. The Capability Committee ceased in June 2018, and its governance functions were assumed by the Executive Board.

Transformation Oversight Committee

The Transformation Oversight Committee was established to provide strategic oversight of, monitor the progress of and measure benefits realised from the transformation process.

Audit and Risk Committee

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

The committee comprises seven members—four external members, including an external chair; and three ASIO members—as well as 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 Audit and Risk Committee.

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

The ASIO Fraud Control Framework 2016–18, available online from www.asio.gov.au, outlines our fraud control and management arrangements.

EXPENDITURE

Budget

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

In 2017–18, ASIO received revenue from government totalling $505.3 million, comprising $421.8 million in operating funding and for capital activities, $68.6 million in Departmental Capital Budget and $14.9 million in equity injection.

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

Two of the Additional Estimates measures related to recommendations from the Independent Review of Australia's Intelligence Community. The measures were:

- assistance with the establishment of a 24/7 capability in the Australian Cyber Security Centre; and
- a temporary secondment of nine ASIO personnel to the Australian Government Security Vetting Agency (AGSVA) to help with the agency's remediation program for the vetting of Top Secret Positive Vetting (PV) security clearances.

The temporary duration of the secondment reflects the anticipated completion of the AGSVA PV remediation program.

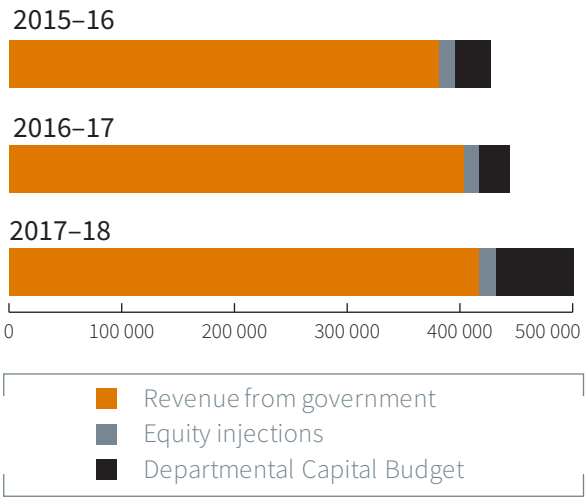
In addition, a measure classified as a decision taken but not yet announced resulted in ASIO receiving $2.3 million in 2017–18. ASIO's funding for 2017–18 also included operating funds for sustainability, which has been extended for 2018–19 only. Without ongoing sustainability funding, there will be significant resourcing pressures.

During 2017–18, ASIO returned approximately $25.4 million to the government through the efficiency dividend and other savings measures ($17.7 million in the efficiency dividend; $2.5 million through the Home Affairs savings measures, which is part of $25.5 million over 10 years; and $5.2 million in other measures).

We will continue to contribute to Australian Government savings measures, including the efficiency dividend, which will have a significant impact on ASIO's Departmental Capital Budget (DCB), the 2018–19 operating budget, and across the forward estimates.

We will continue to identify and implement efficiencies and rigorously prioritise our activities to ensure we operate within future budget allocations. However, further consideration will be given during 2018–19 to the sustainability of our current operations in light of our projected DCB and operating budget, and our current and anticipated future operating environment.

Figure 5: Revenue from government (000)



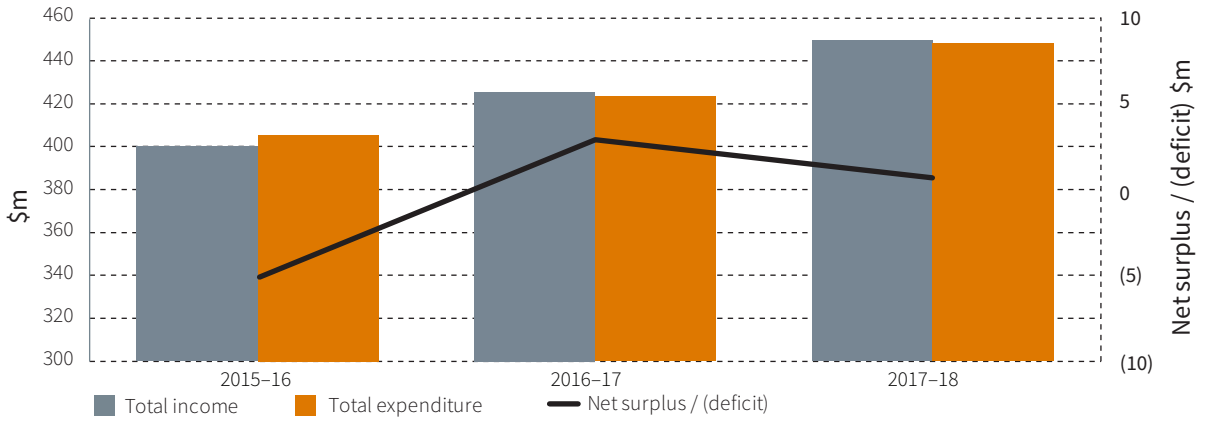
Financial performance

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

In relation to financial performance, ASIO achieved a small surplus of $0.972 million (excluding depreciation), which represents 0.2 per cent of our budget.

However, our DCB remains under pressure as we work to replace assets that provide the capability needed to operate effectively in a rapidly changing security and technological environment. These rapid changes contributed to a capital expenditure increase in 2017–18, a trend that we expect to continue over the forward estimates. While our DCB will increase from $68.6 million in 2017–18 to $85.6 million next financial year as a result of the previous year's appropriation re-phasing, from 2019–20 it will stabilise at a lower figure of approximately $44 million annually.

Figure 6: Financial performance



Resource allocation and capital items

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

In line with the previous reporting period, ASIO's expenditure continued to be predominantly operationally related (78 per cent). During the reporting period, ASIO's expenditure split between operational and non-operational moved by approximately 3 per cent, resulting in an overall increase in non-operational spending, from 19 per cent to 22 per cent of ASIO's budget. While ASIO has actively rationalised its non-operational component, pressures have still resulted in the increased non-operational split. The reasons for the shift include the following:

- External factors led to an increased operating cost. For example, in 2017–18 ASIO's Corporate and Security supplier costs increased by 8 per cent, which included a 4 per cent increase in property operating expenditure. Additionally, ASIO's Information Division supplier costs increased by 18 per cent, which included a 5 per cent increase in information and communication technology costs and a 19 per cent increase in materials.
- As a direct outcome of the Thodey Review, in 2017–18 ASIO established the Enterprise Transformation Office (ETO), which spent $9.3 million in the reporting period. The ETO did not exist before this and therefore did not affect previous expenditure.

The expenditure on capital items increased during the reporting period. This increase relates to ASIO's asset replacement program. ASIO's DCB from 2018–19 will not be sufficient to fund assets that are required to be replaced.

Figure 7: Resource allocation

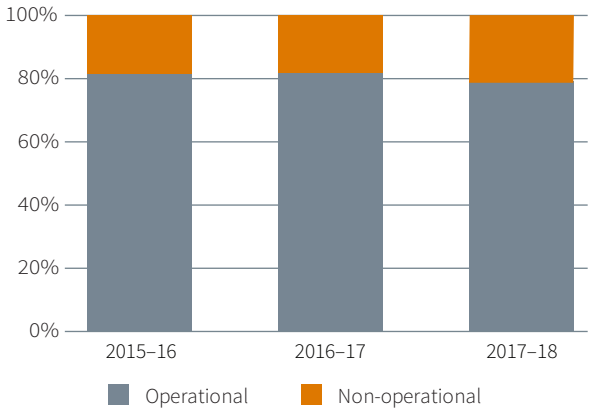
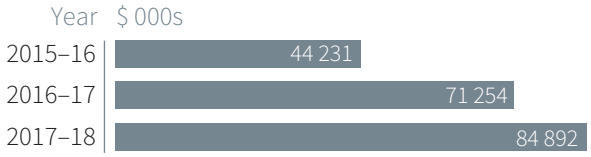


Figure 8: Purchase of capital items



Procurement

Throughout 2017–18 we adhered to the Commonwealth Procurement Rules and associated policy and guidelines. Our compliance was monitored through our Audit and Risk Committee and Finance Committee. No significant issues were identified, and overall compliance was acceptable.

Consultants

During 2017–18, we entered into 35 new consultancy contracts, involving total actual expenditure of $10.6 million. In addition, nine ongoing consultancy contracts were active, involving total actual expenditure of $0.24 million.

We applied the Commonwealth Procurement Rules and Department of Finance guidance when selecting and engaging consultants. We also followed internal policy and associated procedures that provide guidance on identifying and determining the nature of a contract. We engaged consultants when we needed professional, independent and expert advice or services that were not available from within ASIO.

In line with authorised exemptions to avoid prejudice to our national security activities, ASIO is not required to publish information on the AusTender website, which holds information on the value of contracts and consultancies. However, a list of our consultancy contracts to the value of $10 000 or more during this reporting period, and the total value of each of those contracts over the life of each contract, can be made available to the PJCIS.

Contracts

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

Financial management and internal 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 2017–18, ASIO did not receive any adverse audit qualifications from the ANAO as part of its independent audit reporting to parliament.

Within ASIO, the Chief Finance Officer reports monthly to the Finance Committee. 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 Chief Financial Officer also provides quarterly briefings to ASIO's Audit and Risk Committee to support the committee's role of providing independent assurance about ASIO's internal governance, risk and control framework.

Internal audit

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 Audit and Risk Committee. The annual Assurance Work Program is endorsed by the Audit and Risk Committee and is based on an annual assessment of business risks and internal controls.

The work program includes compliance audits—some mandatory, as required by either legislation or agreements—and performance reviews.

The Audit and Risk Committee provides independent advice to the Director-General and the Executive Board on our financial and performance reporting responsibilities, risk oversight and system of internal control (refer to 'Audit and Risk Committee', above). During 2017–18 the Chief Financial Officer reported quarterly on ASIO's financial performance to the Audit and Risk Committee.

During the 2017–18 reporting period, we began a review of our compliance framework. This work is ongoing, and detail on the outcome of the review will be presented in ASIO's submission to the 2018–19 PJCIS Administration and Expenditure Review.

HUMAN RESOURCE MANAGEMENT

During the reporting period, ASIO continued to invest heavily in attracting, managing, developing and retaining a highly capable workforce, which operates in a challenging and high-tempo security and operating environment.

The report from the Thodey Review, *A digital transformation of the Australian Security Intelligence Organisation*, emphasised the importance of cultural and people management reform in achieving enterprise transformation. In particular, it identified the need for ASIO to:

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

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

Over a period of change, we provided staff with extensive training and development opportunities to build their skills and attain a broader understanding of the priorities and direction of the Organisation, particularly in the context of enterprise transformation.

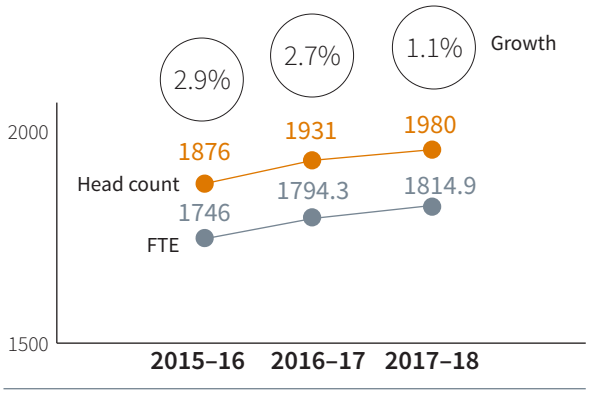
In addition, ASIO continued to improve the workforce's digital literacy through TechX, our key strategy for the communication of information about ASIO's technical capabilities to internal and external stakeholders. TechX was established as an initiative under the ASIO2020 program and the Enterprise Technology Strategy to increase awareness of technical capabilities and to promote a greater, more innovative use of technology.

Workforce statistics

At the end of 2017–18, ASIO employed 1815 full-time equivalent staff, an increase of 1.1 per cent from 2016–17. Through concerted investment in our recruitment and vetting capability, we are currently on track to welcome up to 100 new employees during 2018–19, more than doubling the 49 new employees who commenced with the Organisation in 2017–18.

The reporting period saw an increase in the number of ASIO employees accessing flexible work arrangements through part-time employment. This is assessed 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 and the establishment of Diversity and Inclusion networks.

Figure 9: Staffing growth (full-time equivalent actual and head count)



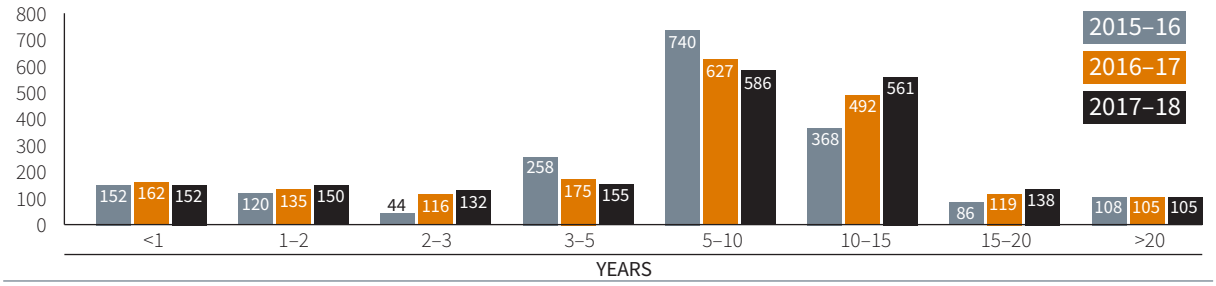
Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff

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

	2015–16			2016–17			2017–18		
Status	Ongoing	Non-ongoing	Total	Ongoing	Non-ongoing	Total	Ongoing	Non-ongoing	Total
Full-time	1567	10	**1577**	1611	12	**1623**	1640	10	**1650**
Part-time	225	15	**240**	240	18	**258**	260	21	**281**
Casual	-	59	**59**	-	50	**50**	-	49	**49**
Total	1792	84	**1876**	1851	80	**1931**	1900	80	**1980**

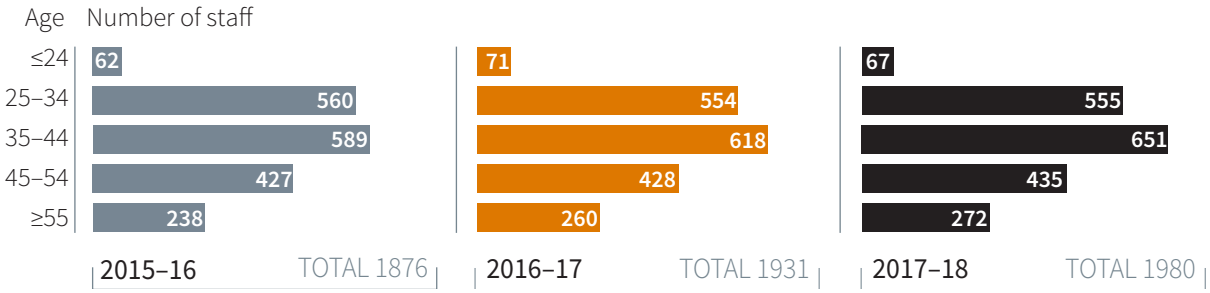
Notes:
1. Data includes the Director-General.
2. Non-ongoing employees do not include locally engaged staff and secondees.

Figure 10: Length of service



Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff

Figure 11: Age profile



Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff

Table 3: Head count of staff by gender and employment status

	2015–16				2016–17				2017–18			
Gender	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Female	812	8	14	**834**	844	10	14	**868**	882	8	12	**902**
Male	980	17	45	**1042**	1007	20	36	**1063**	1018	23	37	**1078**
Total	1792	25	59	**1876**	1851	30	50	**1931**	1900	31	49	**1980**

Notes:
1 Data includes the Director-General.
2. Non-ongoing employees do not include locally engaged staff and secondees.

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

		2015–16				2016–17				2017–18			
		Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Director-General	DG	1	-	-	**1**	1	-	-	**1**	1	0	0	**1**
Senior Executive Service	SES Band 3	2	-	-	**2**	2	-	-	**2**	4	0	0	**4**
	SES Band 2	12	1	-	**13**	11	-	2	**13**	12	0	3	**15**
	SES Band 1	34	2	1	**37**	34	2	1	**37**	37	2	1	**40**
Senior officers	AEE2–3	156	3	1	**160**	175	3	1	**179**	187	5	1	**193**
	AEE1	373	3	4	**380**	365	3	3	**371**	407	5	3	**415**
Employees	AE1–6, ITE1–2, Grade 1–2	1214	16	53	**1283**	1263	22	43	**1328**	1252	19	41	**1312**
Total		1792	25	59	**1876**	1851	30	50	**1931**	1900	31	49	**1980**

Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff
2. Data is derived from the Nominal establishment.
3. 'Employees' includes IT employees and engineers.

Table 5: Head count of employees by location and employment status

	2015–16				2016–17				2017–18			
	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Canberra-based	1259	18	48	**1325**	1312	17	37	**1366**	1358	23	36	**1417**
Other locations	533	7	11	**551**	539	13	13	**565**	542	8	13	**563**
Total	1792	25	59	**1876**	1851	30	50	**1931**	1900	31	49	**1980**

Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff

Table 6: Workplace diversity

Classification	Total staff	Women	Non–English speaking background	Aboriginal and Torres Strait Islander	People with a disability	Available EEO data*
			2015–16			
Senior Executive Service (incl DG)	53	18	3	-	-	48
Senior officers (AEE1–3)	540	196	72	1	6	496
Employees	1283	620	212	9	12	1206
Total	1876	834	287	10	18	1750
Percentage	100%	44%	16%	1%	1%	93%
			2016–17			
Senior Executive Service (incl DG)	53	21	3	-	-	47
Senior officers (AEE1–3)	550	194	76	2	5	506
Employees	1328	653	245	10	14	1252
Total	1931	868	324	12	19	1805
Percentage	100%	45%	18%	1%	1%	93%
			2017–18			
Senior Executive Service (incl DG)	60	25	5	-	1	54
Senior officers (AEE1–3)	608	231	90	1	5	565
Employees	1312	646	238	9	14	1243
Total	1980	902	333	10	20	1862
Percentage	100%	46%	18%	1%	1%	94%

Notes:

1. Percentage of women and percentage of available EEO data calculated using the total head count
2. Percentages of employees identifying as Aboriginal and Torres Strait Islander, a person with a disability or being from a non–English speaking background calculated using the head count of available data
3. Data includes the Director-General and excludes secondees into ASIO, locally engaged staff and contractors.
4. 'Employees' includes IT employees and engineers.
5. Provision of EEO data is voluntary. Data is considered 'available' if a staff member has provided information on at least one diversity category.
6. Data is derived from the Nominal establishment.

* EEO stands for Equal Employment Opportunity

Commencements and separations

ASIO's effort to grow in order to support our capability and meet our transformation objectives is ongoing. In 2017–18, we achieved a net growth of 49 ongoing staff.

As at 30 June 2018, we employed 1815 full-time equivalent staff. Our separation rate at that time was 5.05 per cent, compared with the 2016–17 financial year separation rate of 5.26 per cent.

Table 7: Commencements by classification

		2015–16	2016–17	2017–18
Director-General	DG	-	-	-
Senior Executive Service	SES Band 3	1	-	-
	SES Band 2	2	2	1
	SES Band 1	1	1	1
Senior officers	AEE2–3	4	4	10
	AEE1	26	22	17
Employees	AE1–6, ITE1–2, Grade 1–2	126	136	123
Total		160	165	152

Notes:
1. Includes the Director-General and ongoing, non-ongoing and casual employees.
2. Excludes secondees into ASIO and locally engaged staff.
   - A total of 51 secondees into ASIO and locally engaged staff commenced with ASIO in FY2015–16.
   - A total of 34 secondees into ASIO and locally engaged staff commenced with ASIO in FY2016–17.
   - A total of 29 secondees into ASIO and locally engaged staff commenced with ASIO in FY2017–18.
3. 'Employees' includes IT employees and engineers.

Table 8: Separations by classification

		2015–16	2016–17	2017–18
Director-General	DG	-	-	-
Senior Executive Service	SES Band 3	1	-	-
	SES Band 2	2	2	3
	SES Band 1	4	3	5
Senior officers	AEE2–3	9	11	8
	AEE1	23	27	21
Employees	AE1–6, ITE1–2, Grade 1–2	59	67	67
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.
   - A total of 42 secondees into ASIO and locally engaged staff separated from ASIO in FY2015–16.
   - A total of 48 secondees into ASIO and locally engaged staff separated from ASIO in FY2016–17.
   - A total of 38 secondees into ASIO and locally engaged staff separated from ASIO in FY2017–18.
3. 'Employees' includes IT employees and engineers.

Table 9: Separations by reason

	2015–16		2016–17		2017–18	
Reason	Total	% of head count	Total	% of head count	Total	% of head count
Resignation	68	4%	80	4%	67	3%
Age retirement	10	1%	10	1%	18	1%
Retirement: invalidity	-	0%	1	0%	1	0%
Other	62	3%	67	3%	56	3%
Total	140	8%	158	8%	142	7%

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

In the reporting period, the average tenure for all ASIO separating employees, including contractors, was four years. The average tenure at separation for ongoing employees only is 11 years.

Of the 104 ongoing, non-ongoing and casual employees who separated, the highest percentages came from the following cohorts:

- ASIO officers with a tenure of 5–9 years (31 per cent), closely followed by ASIO officers with a tenure of 10–14 years (30 per cent)—these separations are commensurate with the percentage of employees within these cohorts (30 and 28 per cent respectively);
- AE6 officers and equivalents (34 per cent), which is commensurate with the percentage of employees within this cohort (39 per cent); and
- ASIO officers 55 years of age and over (36 per cent), followed by ASIO officers aged between 35 and 44 years of age (30 per cent).

These separations are proportionate to the percentage of employees within their respective cohorts, except for ASIO officers 55 years of age and over (36 per cent of separations), which comprise only 14 per cent of ASIO's workforce. Retirement comprised 49 per cent of separations within this age group.

Of the separating ongoing ASIO Officers, 33 per cent resigned and commenced employment with Australian Public Service agencies, and 15 per cent accepted employment within the private sector.

Table 10: Separations by tenure

	2015–16				2016–17				2017–18			
	Number		Percentage		Number		Percentage		Number		Percentage	
Tenure	Separations	Tenure for all employees	Separations	Tenure for all employees	Separations	Tenure for all employees	Separations	Tenure for all employees	Separations	Tenure for all employees	Separations	Tenure for all employees
Less than 2 years	-	272	62%	10%	20	297	67%	15%	13	303	13%	15%
2–4 years	20	302	8%	22%	16	291	6%	15%	8	287	8%	14%
5–9 years	32	740	12%	42%	34	627	12%	32%	32	586	31%	30%
10–14 years	34	368	13%	15%	24	492	9%	25%	31	561	30%	28%
15 years or more	12	194	5%	10%	16	224	6%	12%	20	243	19%	12%
Total	**98**	**1876**	**100%**	**100%**	**110**	**1931**	**100%**	**100%**	**104**	**1980**	**100%**	**100%**

Notes:
1. Includes the Director-General, ongoing, non-ongoing and casual employees
2. Does not include secondees, contractors or locally engaged staff
3. Any discrepancies in the percentage figures are due to rounding.

Table 11: Separations by classification

	2015–16				2016–17				2017–18			
	Number		Percentage		Number		Percentage		Number		Percentage	
Classification	Separations	ASIO workforce by classification	Separations	ASIO workforce by classification	Separations	ASIO workforce by classification	Separations	ASIO workforce by classification	Separations	ASIO workforce by classification	Separations	ASIO workforce by classification
AE5 & equivalents	13	402	10%	21%	14	404	31%	21%	16	369	15%	19%
AE6 & equivalents	37	716	46%	40%	40	748	25%	39%	35	771	34%	39%
AEE1 & equivalents	23	380	19%	19%	27	371	18%	19%	21	415	20%	21%
AEE2 & equivalents	9	138	5%	8%	9	150	5%	8%	6	169	6%	9%
Other	16	240	20%	13%	20	258	21%	13%	26	256	25%	13%
Total	**98**	**1876**	**100%**	**100%**	**110**	**1931**	**100%**	**100%**	**104**	**1980**	**100%**	**100%**

Notes:
1. Includes the Director-General, ongoing, non-ongoing and casual employees
2. Does not include secondees, contractors or locally engaged staff
3. Any discrepancies in the percentage figures are due to rounding.

Table 12: Separations by age group

	2015–16				2016–17				2017–18			
	Number		Percentage		Number		Percentage		Number		Percentage	
Age group	Separations	ASIO workforce by age	Separations	ASIO workforce by age	Separations	ASIO workforce by age	Separations	ASIO workforce by age	Separations	ASIO workforce by age	Separations	ASIO workforce by age
24 years and under	-	62	0%	3%	-	71	0%	4%	-	67	0%	3%
25–34 years	14	560	14%	31%	24	554	21%	29%	17	555	16%	28%
35–44 years	30	589	31%	32%	32	618	28%	32%	31	651	30%	33%
45–54 years	23	427	23%	21%	24	428	23%	22%	19	435	18%	22%
55 years and over	31	238	32%	12%	30	260	27%	13%	37	272	36%	14%
Total	98	1876	100%	100%	110	1931	100%	100%	104	1980	100%	100%

Notes:
1. Includes the Director-General, ongoing, non-ongoing and casual employees
2. Does not include secondees, contractors or locally engaged staff
3. Any discrepancies in the percentage figures are due to rounding.

Recruitment and retention strategies

Attracting high-quality candidates to meet future capability and growth requirements continues to be a high priority for the Organisation. 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, ASIO continued to receive positive interest from applicants seeking to work with the Organisation over the reporting period.

As a direct outcome from the Thodey Review, there has been considerable investment of resources into analysing the future system enhancements required to streamline processes and create greater efficiencies across all domains of the recruitment pipeline, including recruitment, vetting, cognitive assessments and onboarding. It is anticipated that this work will culminate in a single recruitment system that will deliver greater speed and efficiency in the recruitment and onboarding process, ensuring that we remain responsive to organisational needs and competitive labour market demands.

Additionally, the new ASIO job family model continues to mature. It will increase the flexibility of ASIO's future workforce by enabling ASIO to source and recruit candidates with the skills, capabilities and experience to fill a range of roles, rather than sourcing and recruiting to a specific job. The aim of this is to provide greater depth in candidate pools so that future capability needs across ASIO can be met at any time. The job family model will also enable ASIO employees to identify other roles in ASIO that they would be suitable for, improving career pathways, retention and organisational flexibility.

Other significant reforms underway within Recruitment 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;
- conducting ongoing analysis of the effectiveness of our sourcing strategies and applying this to better target recruitment activities;
- increasing the use of merit lists as a significant recruitment lever; and
- commencing a functional review of the Organisation to determine which elements could be decentralised to our regional offices, to provide greater opportunity to recruit from new or emerging talent pools while also providing greater career options for our current and future workforces.

Throughout the reporting period, recruitment activities for the graduate and training programs, including our Intelligence Officer, Intelligence Analyst and Surveillance Officer training programs, attracted strong candidate interest.

ASIO continues to refine its approach to difficult-to-fill information technology roles, including through the Future Technologist graduate program and through targeted marketing and attraction campaigns. ASIO's approach to attracting technical candidates is continuously refined and includes attendance at career fairs and partnering with key universities with a strong technical focus.

Recruitment outcomes

In 2017–18, ASIO conducted 80 recruitment activities, including career fairs, larger bulk rounds and role-specific campaigns.

Table 13: Recruitment outcomes

Financial year	Number of applications received	Applicants found suitable at interview / Assessment Centre	Percentage of total applicants found suitable
2015–16	12 997	278	2%
2016–17	10 211	605	6%
2017–18	9643	602	6%

* Suitable to be appointed, progressed to vetting or placed in a merit pool

Table 14: Attendance at career fairs

	2015–16	2016–17	2017–18
Number of fairs attended	9	12	16
Cost*	$163 546	$109 233	$141 152

* Includes a security component

Secondments

To enhance collaboration across all areas of our mission and purpose, ASIO pursues and provides opportunities for secondment to and from a wide range of federal, state and territory government agencies, international counterparts, and other bodies. As at 30 June 2018, ASIO had 33 secondees to the Organisation and 28 secondees from the Organisation in relation to Australian Government agencies.

Workplace agreement

ASIO continued to operate under its 10th Workplace Agreement, which was agreed in 2016 and notionally expires in March 2019. The agreement meets our requirement under the ASIO Act to adopt the employment principles of the Australian Public Service where they are consistent with the effective performance of the Organisation.

The consultation and negotiation for our 11th Workplace Agreement has commenced, ahead of the nominal expiry of the existing agreement in March 2019.

ASIO Consultative Council

The ASIO Consultative Council (ACC) was 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 council is a deliberative and advisory forum, not a determining body, and is recognised by the Attorney-General.

The council continues to strengthen the lines of 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, ASIO developed a Leadership Charter during 2017–18. Centred on four overarching principles—mission focused, inclusive, committed to building people, and enterprise minded—the charter articulates the behaviours expected of all leaders in ASIO, regardless of level.

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

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

Figure 12: ASIO Leadership Charter

Leadership Charter

Every successful organisation or enterprise exhibits a strong leadership culture. This culture presents at all levels of management – leadership is not the only prerequisite for organisational success but it is the bedrock upon which other necessary qualities and characteristics are founded. This axiom of organisational behaviour has particular relevance for ASIO. As an organisation, we are as sound and effective as our leadership culture.

You, as a core member of our leadership team, carry the direct responsibility to create the right atmosphere for a leadership culture to develop and flourish in all those officers around you. I expect you to lead your respective teams in such a way that your people are challenged but achieve the mission; are inspired but feel their interests are being defended; and feel valued but know that in turn they must lead and look after their people.

ASIO's mission is too important to trust to anything less than the best leadership culture we can create. I look to you to assist me directly with this work and focus every day on your leadership and the creation of leadership qualities and practices in your people.

Finally, I want to comment on awareness. I expect leaders in ASIO to have a continuous horizon scan going. Good leaders can see outside their 'lane'. They can take something of a helicopter view and see opportunities for, and threats to, their work units. You need to get 'above the ruck' for at least part of each working day.

I wish you every success as we work together to use this charter to develop a stronger ASIO Leadership Culture.

Duncan Lewis
Director-General of Security

Australian Government
Australian Security Intelligence Organisation

Mission Focused

Reinforcing our core purpose and focus

I am leading when I:

- Anchor my teams work to the Organisation's mission and whole-of-government outcomes
- Communicate priorities, make the hard decisions and follow my commitments with action
- Own the risk delegated to me and take responsibility for decisions I make
- Translate the Organisation's strategy to my team

We are leading when we:

- Inspire others through a clear, consistent and shared communication of our mission
- Show collective ownership of our purpose and strategy
- Work together to get the job done
- Engage with risk and support each other to do so
- Ensure our people understand what we do and why, our objectives and how we can measure our performance effectively

Committed to Building People

Prioritising people and culture

I am leading when I:

- Know my team so that I can draw on their experiences and strengths
- Trust and empower others, including delegating effectively
- Am visible and accessible
- Create an environment where my team can achieve their potential
- Know the professional aspirations of everyone in my team and am invested in professional development
- Lead with empathy, authenticity and courage

We are leading when we:

- Prioritise people development as core business
- Share credit when things go well and take responsibility when they don't
- Call out inappropriate behaviour, including from our peers
- Create a safe environment so our people can learn from trying
- Nurture talent for succession; pave the way for the next generation

Inclusive

Committing to diversity and inclusion

I am leading when I:

- Lead by modelling diversity and inclusion
- Understand and account for my biases
- Have no shame in saying "I don't know" and asking for input
- Create an environment where my whole team is supported and represented
- Make and explain considered, fair and transparent decisions
- Innovate and challenge the status quo

We are leading when we:

- Value everyone's contribution, skills and talents
- Work together, across divisions, as an ASIO team
- Recognise, communicate and model the benefits of diversity and inclusion
- Act to eliminate non-inclusive behaviour – see something, say something, do something
- Stamp out 'us' and 'them' mindsets and behaviours

Enterprise Minded

Leading on behalf of the whole Organisation

I am leading when I:

- Understand and communicate the impact of my decisions on other areas
- Support, value and communicate the pressures and priorities of other teams
- Contribute to whole-of-Organisation decision making and support the outcomes
- Put organisational outcomes ahead of individual ambition
- Scan the horizon for signals of change, and position the organisation to respond

We are leading when we:

- Collectively own the Organisation's wins and losses
- Share experiences, information, good practices and lessons
- Collaborate with and help each other, our partners and stakeholders
- Share resources for the good of the Organisation
- Trust each other's contribution and expertise

Performance management processes

Performance management policy and processes continued to be refined during 2017–18. Building on reforms undertaken in the 2015–16 and 2016–17 reporting periods, we achieved 100 per cent rate of compliance for employee participation in the performance cycle.

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

Staff survey

ASIO conducts a comprehensive staff survey approximately every two years. The most recent survey was held in June 2017. Survey results showed that ASIO's workforce is engaged and committed, job satisfaction is high (91 per cent), and there have been improvements in key areas since the last survey was held (2014). The overall participation rate was 62 per cent, a slight increase on the rate for the 2014 staff survey.

The survey indicated that some areas—such as career management processes—could be improved, and substantial progress was made during the reporting period to address these areas. Further information is provided under 'Training and development', below.

Ethics and conduct

ASIO strives to provide a positive working environment where the organisational culture, leadership styles and workplace relationships support staff to effectively and efficiently undertake their roles and meet organisational objectives. To achieve this, ASIO maintains ethics and conduct policies which promote an organisational culture based on the ASIO Values and which guide the decision-making and behaviour of employees. These policies assist individuals and the broader Organisation to seek advice, report incidents and effectively manage conduct and behaviour.

ASIO's Human Resources Branch manages ethics and conduct for the Organisation through a range of mechanisms that provide oversight on matters such as complaints and allegations of misconduct, and harassment and discrimination. Public interest disclosures, allegations of fraud and security breaches are investigated through separate mechanisms and attract separate reporting obligations.

A number of initiatives were trialled in 2017–18 to enhance ASIO's systems and processes for identifying and responding to allegations of inappropriate behaviour and misconduct, including:

- engagement of external investigators to undertake independent and impartial misconduct investigations;
- engagement with the Department of Defence Dispute Resolution team to provide mediation services; and
- the introduction of workplace health reviews aimed at identifying factors that may be inhibiting work areas from becoming high-achieving teams.

Promotion of ethics

In 2017–18, ASIO initiatives conveying to staff our expectations of individual conduct which is legal, ethical and respectful of human rights included mandatory training for all staff on:

- 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.

In addition, ASIO provided training on conduct and behaviour through ASIO's induction training, management training and SES-led sessions on ethical decision-making in ASIO.

Figure 13: ASIO Values and Code of Conduct

Harassment and Discrimination Adviser network

ASIO's network of Harassment and Discrimination Advisers (HaDAs) is an organisational resource to provide staff members 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.

There are currently 31 HaDAs across ASIO. The role of a HaDA is voluntary, and appointment is for two years. An annual HaDA refresher training event was held in June 2018.

In 2017–18, ASIO commenced a review of the HaDA Network and its functions to ensure the HaDA program is visible and accessible to staff and effectively supports and contributes to ASIO's conduct and behaviour strategy. To support the review, an all-staff survey has been developed to inform strategies to improve awareness of the network and the value provided by its members.

There were fewer HaDA reports this year than in the two previous reporting periods. However, during 2017–18 three health reviews of work areas were undertaken, with the opportunity for individuals to talk through experiences in the workplace. This was a proactive way to understand functioning within work areas and to work with senior leadership to influence and educate employees about expectations and behaviour, consistent with ASIO's Values and the Leadership Charter.

Public interest disclosures

Disclosure under the *Public Interest Disclosure Act 2013* (the PID Act) is one 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.

Since 30 June 2015, five disclosures have been investigated and reported on, or allocated for investigation by another authority. During 2017–18, one disclosure was received. The decision was made not to investigate, and the disclosure was passed to ASIO's Human Resources Branch (HR) to consider. The employee ceased employment with ASIO prior to HR finalising its investigation.

Table 15: Public interest disclosures received by ASIO

Financial year	Public interest disclosures received by ASIO	Outcomes / findings
2015–16	0	N/A
2016–17	4	▸ 1 report found nil findings of maladministration. ▸ 1 report identified disclosable conduct and was passed to Human Resources Branch to consider. ▸ 2 disclosure reports were allocated to the Human Resources Branch for investigation under another authority.
2017–18	1	▸ 1 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.

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 the reporting period, the ASIO Ombudsman met regularly with our senior management and Staff Association representatives to discuss the health of the workplace. The Ombudsman provided valuable support and advice to employees and line managers, including:

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

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

In 2017–18 the ASIO Ombudsman was not involved in work matters related to public interest disclosures.

Work health and safety

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

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

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

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

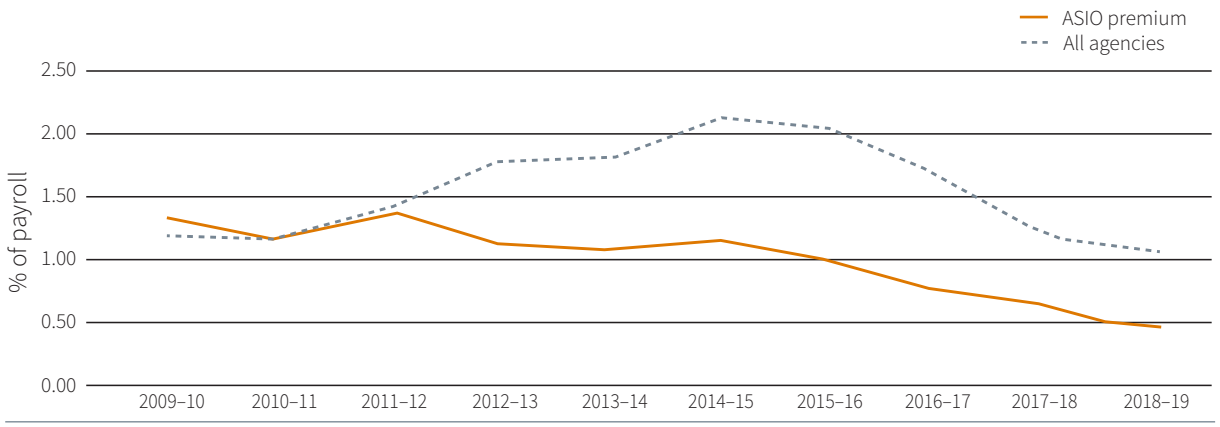
In the current heightened threat environment, we continued to direct significant resources towards ensuring the safety of our operational activities, enhancing our building security and providing safety training for staff. This involves a layered approach to personal safety and security training that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

This safety and security training complements the foundational security training provided to all new employees and as a refresher to all continuing employees.

In line with legislated notification obligations, we reported two incidents to Comcare in 2017–18. Comcare did not initiate any investigations into the notifiable incidents, nor were any notices issued to ASIO under the *Work Health and Safety Act 2011*.

ASIO's Comcare premium rate has been consistently and significantly lower than the Commonwealth average since the 2011–12 financial year. A number of factors have contributed to this trend, including our performance on medium-term and long-term claims, and our comparatively low claim frequency. While the number of claims by ASIO employees increased in 2015, largely as a result of the introduction of personal safety and security training, these injuries were generally minor and quickly resolved. Their impact on our Comcare premium was also partially cushioned by the removal in 2017–18 of the additional margin charged by Comcare to repair past underfunding.

Figure 14: Comparison of Comcare premium rates 2009–10 to 2018–19



Note: 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.

Diversity and inclusion

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

Under the direction of a corporate committee established in 2016–17, during the reporting period ASIO undertook a range of initiatives in support of diversity and inclusion, including:

- releasing ASIO's Diversity and Inclusion Strategy 2018–20, which articulates our diversity and inclusion goals and paves the way for us to broaden our staffing profile and harness the diversity of our existing workforce;
- strengthening our employee engagement program for staff on long-term leave, and establishing family room facilities to provide support for staff members with caring responsibilities;
- rolling out the ASIO-wide 'if not, why not' approach to flexible working arrangements;
- establishing staff-initiated and -led diversity networks, which form an essential part of creating a diverse and inclusive culture where all staff feel valued, respected, included and safe;
- creating a community of support for Aboriginal and Torres Strait Islander employees;
- delivering a number of cultural awareness initiatives, including a cross-cultural communication week and training packages;
- continuing our commitment to the Male Champions of Change program, including the establishment of a dedicated AEE1 position to support this 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.

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

Accommodation and facilities

In 2017–18, 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.

TRAINING AND DEVELOPMENT

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

In 2017–18:

- We approved or conducted 135 training courses, including 4057 face-to-face training activities attended by 1367 staff.
- Our staff completed 2554 mandatory and 784 non-mandatory e-learning courses across seven mandatory and 31 non-mandatory online programs.
- We allocated $316 413 to 137 staff attending over 90 ASIO-supported study programs.
- We allocated $159 050 to 13 domestic and two international development opportunities, attended by 15 members of our Senior Executive Service. In 2018–19, this budget will be allocated to adaptive leadership training across ASIO, in line with our transformation requirements.
- We allocated $212 982 to 49 members of our Senior Executive Service for the 360-degree survey and feedback executive coaching program.

Due to budget constraints, there has been a reduction in face-to-face training offered, from 146 face-to-face courses last year to 135 offered this financial year. The number of e-learning modules undertaken by staff has also decreased; this is due to outdated modules being deleted from the system.

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 required to successfully operate in the workplace across a diverse range 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 undertake training-needs analysis to understand training requirements, followed by reviews and evaluation to update the programs for continuous improvement and alignment of training with ASIO's objectives. We deliver our training programs through a mix of in-house learning and development and training by subject matter experts and external training providers. We provide a tailored ASIO-specific training course to in-house trainers to ensure the best learning outcomes—this has resulted in consistently positive feedback from both course participants and line managers, indicating that ASIO has continued to deliver the capability development requirements to support its employees' diverse roles.

Intelligence training

ASIO's year-long Intelligence Development Program (IDP)—comprising the Intelligence Officer Development Program (IODP) and the Intelligence Analyst Development Program (IADP)—trains and assesses employees recruited to perform operational and analytical roles in ASIO. These roles are responsible for ASIO's threat, strategic, investigative and operational analysis functions, as well as our operational intelligence collection capabilities. Intelligence officers perform both analytical and operational roles, while intelligence analysts specialise in the analytical function.

After a pilot in late 2016, the IADP was introduced in 2017 to provide dedicated training and career progression for individuals seeking to specialise in intelligence analysis. The year-long IADP also offers a career pathway for IODP participants who complete the foundational analytical training but either voluntarily withdraw from the IODP or are removed due to underperformance during the operational training. Upon successful completion of the IADP, participants graduate as AE6.0 intelligence analysts and are posted to one of ASIO's intelligence analysis business areas.

Technical workforce

ASIO relies on several recruitment programs to sustain and develop the depth and breadth of its specialist technical workforce. These include the Future Technologists graduate program and the Information and Communications Technology (ICT) traineeship.

For the Future Technologists graduate program, ASIO conducts a twice-yearly intake of university graduates with science, technology, engineering or mathematics qualifications. The program occurs over a 12-month period and involves group education, the allocation of a technical mentor, multiple placements in various work units in technical teams, and access to a range of online and offline training platforms. Upon successful completion of the program, graduates are placed in one of these units on an ongoing basis. Existing ASIO staff with relevant backgrounds may transfer into the program—subject to assessment of their abilities—as a precursor to embarking on a career in technology in ASIO.

The ICT traineeship is conducted over a two-year period, and comprises on-the-job workplace support for Certificate IV-level tertiary studies in an ICT discipline. 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 positions in ASIO.

Management and leadership development

Grounded in the four key objectives outlined in the Leadership Charter, ASIO's Management and Leadership Strategy supports leaders in ASIO to reinforce our core purpose and focus, prioritise people and culture, commit to diversity and inclusion and lead on behalf of the Organisation. Launched in 2017, the strategy supports the 70–20–10 model and enables self-driven learning, providing a broad and tailored range of structured and targeted leadership development opportunities to support leaders in managing organisational growth and change, while increasing capability and productivity to meet new and emerging challenges.

Mentoring is a key overarching pillar in the strategy. In this context, mentoring aims to continue the development of ASIO's current and future management and leadership capability by providing exposure to the learning needed to excel in prospective new roles. Two current mentoring initiatives are the Executive Digital Leadership program and our formalised shadowing program:

- During 2017–18, ASIO developed the Executive Digital Leadership program to enhance the senior executive's understanding of digital concepts, key technologies and associated issues so they can effectively respond to challenges and harness opportunities in this age of accelerated technology. Under the program each senior executive is matched with a digital mentor, and as a pair they explore topics of strategic importance to ASIO. Launched in November 2018, the program provides mentors and mentees with the opportunity to ask questions about each other's work programs and priorities and exchange perspectives, enabling two-way mentoring.
- The opportunity to shadow a more senior manager is offered as part of our foundational leadership program, enabling staff to learn one on one about a different area of the Organisation and to see the behaviours and competencies required at a higher level. Shadowing is included in the program as a critical talent development and retention tool, as well as an important element of strategic succession planning. Participants in shadowing opportunities have spoken highly of the benefits.

Other training programs

Two additional significant ASIO training programs are 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, run 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.

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

Language skills

In 2017–18, ASIO allocated $180 000 to 40 employees under the Language Skills Development Program. While there has been an increase in the number of staff receiving funds, the overall allocation was reduced due to significant budgetary constraints. There was also a deliberate strategy to apply extra rigour to the process and greater expectations of applicants to research cost-effective options and articulate organisational benefits.

Table 16: Language Skills Development Program

	2015–16	2016–17	2017–18
Allocation	$370 281	$291 661	$180 000
Staff	69	34	40

In addition to this training, ASIO delivered a wide range of courses and seminars for a broad audience internally and in the AIC on a range of languages.

National Intelligence Community training

ASIO continues to host the National Centre for Intelligence Training and Education (NCITE) on behalf of the National Intelligence Community (NIC). NCITE identifies and implements shared learning and development opportunities across the NIC to support and encourage enhanced networking, interoperability and understanding across the community. NCITE is communally funded by the NIC agencies on a full cost-recovery basis.

ASIO supports NCITE's role in providing a broad range of intelligence training and related programs for ASIO staff and the broader NIC. ASIO also values the benefits NCITE brings to the community through coordination and consolidation of training content and resources.

Because of NCITE's focus across the NIC, ASIO is working with the Office of National Assessments to move NCITE into what will become the new Office of National Intelligence.

SECURITY ISSUES

Security of ASIO

Throughout this reporting period, we managed the security of our people, information and assets in line with the requirements of the Protective Security Policy Framework, and we reviewed and updated our policies and procedures to reflect changes in broader government policy and our risk environment. In addition to our safety training (refer to 'Training and development'), we provided staff with security awareness training at their 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.

In response to the heightened terrorist threat to law enforcement and security agency staff, we continued to supplement the physical security arrangements for our headquarters building (the Ben Chifley Building) with armed officers from the AFP.

Security policies and governance

In 2017–18, ASIO continued to foster a positive protective security culture where security is considered in all decision-making and is perceived as a shared responsibility. This included supporting ongoing security management and training and ensuring that 'promoting a security culture' is treated as a core capability requirement for all staff.

ASIO contributed to the update of the Protective Security Policy Framework (PSPF), led by the Attorney-General's Department, during 2018.

ASIO Security Committee

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

e-security

ASIO's ICT systems are subject to stringent security requirements due to both the large volumes of classified information processed on these systems, and the sensitivity of ASIO's work. ASIO continually works 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.

Security clearances and vetting

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

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

We continue to work closely with AGSVA to improve the efficiency of the security assessment process while maintaining an appropriate level of assurance for vetting candidates.

Table 17: Personnel security requests and assessments

	2015–16	2016–17	2017–18
Personnel security assessments completed	31 411	27 182	32 153
Number of requests for PV clearances	975	2227	3128
Number of PV security assessments completed	1359	1780	2759
Percentage increase in PV requests	N/A	129%	40%

Current procedures

ASIO's security clearance vetting procedures continue to be consistent with the requirements of the Protective Security Policy Framework, including the *Personnel security guidelines: vetting practices*.

OVERSIGHT AND ACCOUNTABILITY

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

ASIO's ministerial accountability changed during this reporting period. In May 2018 our ministerial accountability moved from the Attorney-General to the Minister for Home Affairs. The 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 Attorney-General and to the Minister for Home Affairs on a range of investigative, operational and administrative issues, which were communicated primarily through more than 230 formal submissions. The Director-General also briefed other ministers on security issues and matters relevant to their portfolios, when required.

We conduct our security intelligence activities in accordance with 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. The department is currently reviewing the guidelines following a recommendation by the PJCIS, and we contributed to the departmental review during this reporting period.

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

Engagement with parliament

Annual report to parliament

ASIO's annual report to parliament for 2017–18 was tabled in both Houses of parliament on 18 October 2018. ASIO's key performance outcomes for the reporting period are described in 'Organisational performance', above.

A short classified appendix was produced to meet ASIO's reporting requirements under section 94 of the ASIO Act. This classified appendix contains statistics on:

- special intelligence operation authorisations;
- authorisations for telecommunications data access; and
- our use of special powers warrants.

Leader of the Opposition

The Director-General of Security is a statutory position, with a responsibility to provide impartial advice. The ASIO Act requires the Director-General to regularly brief the Leader of the Opposition on matters relating to security and to provide them with a copy of ASIO's annual report. Throughout 2017–18, classified briefings on specific security cases were provided for shadow ministers.

Parliamentary Joint Committee on Intelligence and Security

The PJCIS plays a significant role in our oversight and accountability framework. Its annual review of administration and expenditure scrutinises the non-operational aspects of our work, particularly the effectiveness of policies, governance and expenditure. ASIO appeared before the PJCIS in closed and public hearings for its Review of Administration and Expenditure No. 16 (2016–17), providing both oral and written submissions.

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

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

Senate Legal and Constitutional Affairs Committee

ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate Estimates process on 24 October 2017, 27 February 2018 and 24 May 2018. Our evidence to the committee can be found in the Estimates *Hansard* for those days (refer to www.aph.gov.au.

Other parliamentary involvement

ASIO appeared before the Standing Committee on Privileges during this reporting period in relation to its inquiry into parliamentary privilege and the use of intrusive powers. We also contributed to a number of portfolio submissions to other committee inquiries.

Independent oversight

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

Inspector-General of Intelligence and Security

The role of the Inspector-General of Intelligence and Security (IGIS) is to review the activities of the AIC and provide assurance that agencies operate with propriety, according to law, consistent with ministerial guidelines and directives, and with due regard for human rights. The IGIS retains statutory powers similar to those of a standing royal commission.

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

During 2017–18 the IGIS regularly inspected activities across our operational functions and investigated complaints received by her office. Details can be found in the IGIS annual report, available online at www.igis.gov.au. In February 2018, the IGIS commenced an inquiry into an ASIO matter under section 8(2) of the IGIS Act. The inquiry is continuing at the time of writing this report.

Consistent with our commitment to acting with legality and propriety, we are taking steps to address areas identified by the IGIS in 2017–18 as requiring improvement and further attention.

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

Independent National Security Legislation Monitor

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

On 13 February 2017, Dr James Renwick SC was appointed Independent National Security Legislation Monitor.

During this reporting period, the INSLM commenced a review of the prosecution and sentencing of children for Commonwealth terrorist offences. ASIO contributed to the review. Our unclassified submission to the INSLM and evidence provided at public hearings can be found on the relevant inquiry page on the INSLM's website, www.inslm.gov.au.

Independent Reviewer of Adverse Security Assessments

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

In performing this function, the Independent Reviewer examines all ASIO material that ASIO relied on in making the adverse assessment as well as other relevant material, which may include submissions or representations made by the eligible person. The Independent Reviewer closely considers the overall security environment, which is informed by ASIO's contemporary assessment of security threats, and any changes to the applicant's circumstances or ideology during their time in detention.

The Independent Reviewer's terms of reference are available at www.ag.gov.au/asareview. The terms of reference provide for an initial primary review of each adverse security assessment, and subsequent periodic reviews every 12 months for the duration of that assessment.

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

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

The Independent Reviewer for the reporting period was Mr Robert Cornall AO.[1]

1 In November 2018 Mr Cornall was reappointed as the Independent Reviewer for a further two years.

LEGISLATION AND LITIGATION

Legislative changes that have impacted on ASIO's administration

Significant legislation affecting ASIO and its operations was passed during the reporting period, including the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), the *Foreign Influence and Transparency Scheme Act 2018* (Cth), the *Security of Critical Infrastructure Act 2018* (Cth) and the *Telecommunications and Other Legislation Amendment Act 2017* (Cth). Further information about each of these Acts is provided below.

Staffing implications of legal changes

Role of legal officers and the need for specialist staff in relation to legislative advice

ASIO in-house lawyers, with their specific legal skill sets, continue to provide legal advice to the Organisation on existing and proposed legislation.

The demand for legal assistance has again increased substantially in direct response to ASIO's operational activities. It includes the provision of legal advice and support with regard to such activities, security assessments and the protection of ASIO's capabilities from compromise; the provision of corporate legal advice in areas such as employment, procurement, internal security and Freedom of Information; and the management of legal proceedings involving ASIO.

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, the Attorney-General's Department and other National Intelligence Community agencies.

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*, the *Crimes Act 1914* and the *Telecommunications (Interception and Access) Act 1979*. The majority of the Act commenced on 30 June 2018, with secrecy provisions to commence on 29 December 2018 or earlier if proclaimed.

In particular, the Act:

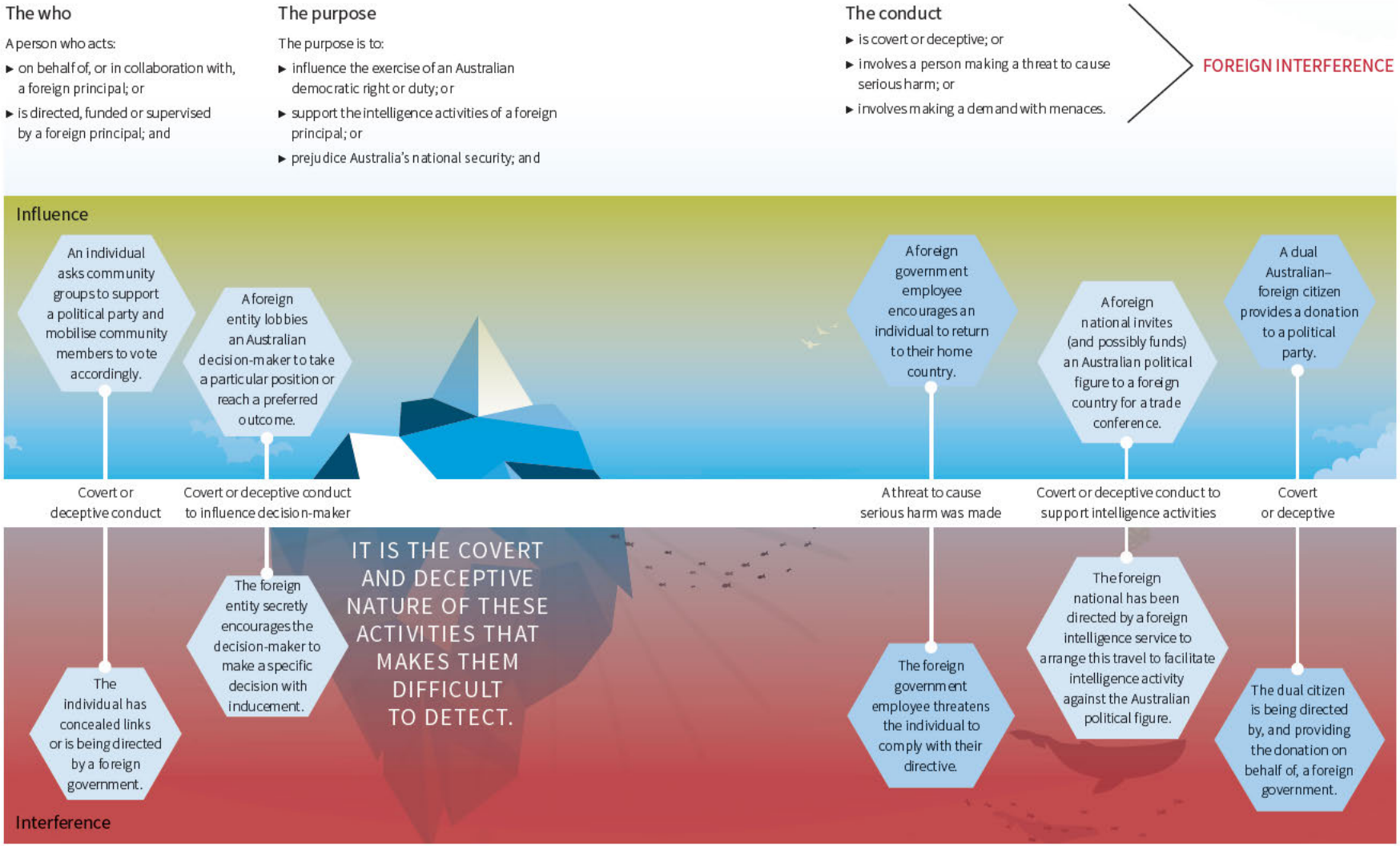
- strengthens existing espionage offences and introduces a new 'theft of trade secrets' offence to protect Australia from economic espionage;
- introduces new foreign interference offences targeting covert, deceptive or threatening actions by foreign actors who intend to influence Australia's democratic 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.

Resource, relationship and training implications

The Act has had substantial resource implications for ASIO officers across the Organisation. For legal officers, passage of the legislation has entailed effort in increasing awareness and knowledge of the new offences and in providing legal advice and support with regard to operational activities, the protection of ASIO's capabilities from unnecessary compromise and the management of legal proceedings.

ASIO will consult with other agencies, notably the office of the National Counter Foreign Interference Coordinator, where appropriate, in relation to the provisions of the Act.

Figure 15: The transition from influence to interference



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 introduces the Foreign Influence Transparency Scheme, which is administered by the Attorney-General's Department and will commence on 29 June 2019 or earlier if proclaimed. The scheme requires persons 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 exemptions 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.

Security of Critical Infrastructure Act 2018

The *Security of Critical Infrastructure Act 2018* (Cth) (the SOCI Act) and the *Security of Critical Infrastructure (Consequential and Transitional Provisions) Act 2018* (Cth) received royal assent on 11 April 2018. The key provisions of both Acts commenced on 12 July 2018.

The SOCI Act, along with the Consequential and Transitional Act (which amends Part IV of the ASIO Act dealing with security assessments), creates a framework for managing risks to national security arising from foreign investment in Australia's critical infrastructure assets. Such assets comprise key electricity, water, gas and port facilities either referred to in the SOCI Act or prescribed under the rules.

The SOCI Act introduces a ministerial directions power that allows the Minister for Home Affairs, having received an adverse security assessment from ASIO, to issue directions to certain relevant bodies requiring them to do, or refrain from doing, specified acts or things. The Act also establishes a non-public register of critical infrastructure assets and an information-gathering power for the minister to issue notices requiring reporting entities to provide certain information and documents.

Other assets can be privately declared by the Minister for Home Affairs, or publicly prescribed by rules, to be critical infrastructure assets and will then also be subject to the regulatory framework of the SOCI Act. ASIO may be asked to provide information to the minister to inform them on whether an asset should be prescribed or privately declared as a critical infrastructure asset.

The ASIO Act has been amended to include the directions power of the Minister for Home Affairs within the definition of 'prescribed administrative action' within Part IV. This requires any advice provided from ASIO to be in the form of a security assessment. ASIO anticipates furnishing security assessments in circumstances when there is a risk of an act or omission that would be prejudicial to security in connection with the operation of, or the delivery of a service by, a critical infrastructure asset.

Telecommunications and Other Legislation Amendment Act 2017

The *Telecommunications and Other Legislation Amendment Act 2017* (Cth) (the TOLA Act) introduces a regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities. The legislation received royal assent on 18 September 2017, and key provisions commenced on 18 September 2018.

The TOLA Act imposes a security obligation on carriers, carriage service providers and carriage service intermediaries (C/CSPs) that requires them to do their best to manage, for the purpose of security, the risk of unauthorised access and interference to networks and facilities they own, operate or use.

The TOLA Act also imposes a requirement on carriers and some carriage service providers to notify of planned changes to systems and services that are likely to make the network or facility vulnerable to unauthorised access and interference. It also provides for exemptions or partial exemptions from the requirement, and the option to submit a security capability plan to meet notification requirements.

Under the TOLA Act, the Attorney-General is granted the power to direct a C/CSP to do, or refrain from doing, a specified act or thing if there is a risk to security. Further, the Secretary of the Attorney-General's Department is granted a power to obtain information and documents from C/CSPs where that information is relevant to assessing compliance with the obligations imposed under the Act.

The ASIO Act has been amended to include the directions power of the Attorney-General within the definition of prescribed administrative action within Part IV.

This requires any advice provided from ASIO to be in the form of a security assessment. Following amendments to the *Telecommunications Act 1997* (Cth), the Attorney-General is required to obtain an adverse security assessment from ASIO before he or she can exercise the directions power.

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 a prescribed authority.[2] If ASIO judges that a warrant is required, the Director-General presents a warrant request to the Attorney-General.

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, issues 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 and the *Telecommunications (Interception and Access) Act 1979* to undertake the following methods of investigation:

- telecommunications interception and access;
- use of surveillance devices;
- entry to and search of premises;
- computer access; and
- the examination of postal and delivery service articles.

The ASIO Act also enables ASIO, with the Attorney-General's consent, to seek warrants from an issuing authority (a federal magistrate or judge) for the questioning, as well as the detention, of individuals in relation to investigations relating to terrorism offences.

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.

Involvement in litigation matters

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

Administrative Appeals Tribunal reviews

The Security Division of the Administrative Appeals Tribunal (AAT) reviewed a number of security assessments relating to the refusal or cancellation of passports, security clearances and visas.

2 'Prescribed authority' is defined as a person appointed under section 34B of the ASIO Act, usually a judge who has been in one or more superior courts for a period of five years and no longer holds a commission as a judge of a superior court.

Over the reporting period, ASIO managed 15 adverse security assessment reviews before the Administrative Appeals Tribunal:

- One application was filed but not continued.
- Four matters were pending at the end of the reporting period.
- Two assessments were remitted to ASIO by consent for new assessments to be prepared, which resulted in two non-prejudicial assessments being issued in the reporting period.
- Three applications were dismissed.
- Four matters were heard, with three adverse security assessments being affirmed or affirmed with minor variations and one decision remaining reserved at the end of this reporting period.
- One review was stayed.

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

Most AAT Security Division open decisions are available on the website of the Australasian Legal Information Institute, Austlii, at www.austlii.gov.au.

Judicial reviews—security assessments

Two further security assessments were reviewed in the Federal Court of Australia and the High Court of Australia during this reporting period.

BSX15 v. Minister for Immigration and Border Protection and Director-General of Security (2016) FCA 1432

We assessed that BSX15, who had entered Australia as an irregular maritime arrival and claimed refugee status, was a member of Islamic State of Iraq and the Levant (ISIL) and posed a risk to Australia's security. The court (heard by Justice Markovic) held that the applicant was not denied procedural fairness at his security assessment interviews because the purpose of the interviews was clearly explained and he was given the opportunity to answer questions as comprehensively as he wished.

On 25 May 2017, the Full Federal Court heard an appeal by the applicant. On 11 July 2017, the court delivered its judgement, which accepted the appeal by BSX15 and set aside the assessment. The court found that ASIO should have questioned BSX15 further about his other names—in particular, its assessment that he was identical with 'Muthana Najim Abdullah'. The court found that BSX15 was not afforded sufficient procedural fairness, set aside the assessment and awarded BSX15's costs.

ASIO carefully considered this judgement.

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

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

The case is still before the High Court.

Terrorism and other criminal prosecutions

ASIO intelligence contributed to the prosecution of individuals in New South Wales, Victoria, South Australia and Queensland on terrorism offences. Our support ranged from the initial identification of activities of concern, the provision of unique insights and assessments, to the use of intelligence as evidence.

Working with our law enforcement partners and prosecuting authorities, our evidentiary contribution included telecommunications intercepts, physical surveillance, and listening and tracking devices. Sensitive capabilities were protected from disclosure through legal mechanisms such as public immunity claims and suppression orders.

OUTREACH AND ADVICE

Government, business and academia

Published reporting

During the reporting period, we published 1440 intelligence reports for Australian partner agencies covering a range of terrorism, espionage, foreign interference and border security issues. Reporting was distributed to more than 130 federal, state and territory government organisations.

Of these reports, we produced 1154 intelligence and security reports on a range of domestic and global terrorism-related topics, including threats to aviation and mass passenger transportation, and pathways to radicalisation; and we published 286 intelligence and security products on counter-espionage and foreign interference topics to inform policymakers' decisions. Key analytical products released during this period include assessments of the harm from espionage and a strategic overview of foreign interference—including to Australia's emerging technology industries, our media, diplomatic and trade missions, and Defence facilities and equities.

To support stakeholders and broaden the reach of our advice, where possible we produced versions of our highly classified reports at lower classification levels, including versions for industry stakeholders to inform their security arrangements. Wherever possible, ASIO has sought to include examples in order to demonstrate the reality of threats, particularly in relation to espionage and interference.

Business and Government Liaison Unit

The Business and Government Liaison Unit (BGLU) fulfils a central outreach function connecting ASIO with businesses and government agencies. BGLU information is 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.

The BGLU conducts its outreach and engagement function in several ways. A key mechanism is a dedicated secure website hosting intelligence-backed reporting and protective security advice relating to the domestic and international security environment. Hosted on the site are reports on terrorism, threats to critical infrastructure and crowded places, espionage and foreign interference threats, and reference material for security managers.

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

Counter-terrorism outreach—policymakers

Our advice and assessments informed policymakers' understanding of local and international terrorist threats. As well as our 1154 reports on terrorism-related issues, we provided briefings to stakeholders on a range of terrorism-related topics, including threats to aviation, and pathways to radicalisation. Of note, the National Threat Assessment Centre provided 31 briefing sessions for federal and state government agencies on terrorism indicators and extended these briefings to a range of foreign security and intelligence partners.

In 2017–18 we provided protective security advice and services to federal, state and territory governments and industry to enhance their understanding of and responses to security threats. As in previous years, ASIO provided the security environment context for the Australia – New Zealand Counter-Terrorism Committee. We also provided advice to the federal, state and territory governments in relation to potential counter-terrorism policy and legislative changes.

Countering espionage and foreign interference outreach—policymakers

During 2017–18, we continued our program of briefings and outreach to improve the understanding among federal and state governments and industry of techniques employed by foreign intelligence services, manifestations of espionage and foreign interference, and the associated risks of this interference, to protect our national institutions of government from foreign influence.

We have provided over 28 foreign intelligence service threat briefings for federal and state parliamentarians, ministerial staff and high office holders travelling overseas, which included advice on mitigation strategies to minimise possible threats.

In addition, our outreach team provided frequent security briefings (5–10 per week) to raise government agencies' awareness of espionage, foreign interference and malicious insider threats. These briefings also offered the opportunity to reiterate security clearance holder obligations, including responsibilities under the Contact Reporting Scheme.

Defence outreach

A major focus for ASIO in 2017–18 continued to be working in partnership with the Department of Defence.

During this reporting period, we:

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

We also contributed briefings to the Centre for Defence Industry Capability roadshow for small and medium-sized enterprises engaged in defence supply chain programs, and we engaged with defence industry companies such as BAE, Northrop Grumman and Thales. We have a comprehensive focus on working with Defence to deliver improved assurance for the supply chain, including support to companies that develop sovereign industrial capabilities.[3]

ASIO continues to develop our analytic and investigative effort focused on threats to the defence industry and acquisition programs, to prevent harm and to protect Australia's military information.

Academic outreach

During the reporting period, ASIO began an academic outreach program. We established engagement with universities, key academic peak bodies, key university committees, other research institutes and university internet connectivity suppliers. Our briefings provided advice on threats to university students, staff, intellectual property, information technology networks, and reputations, and supported university efforts to protect and commercialise innovative research.

Advice on foreign investment and critical infrastructure protection

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

During 2017–18:

- We completed 245 foreign investment assessments, which provided advice on the potential for a foreign power to conduct espionage, foreign interference or sabotage through its involvement in specific investments.
- Our advice on the lack of ownership diversity within certain infrastructure sectors supported the Australian Government's announcement in February 2018 that ownership diversity should be considered a key requirement for future sales; and supported the introduction of new foreign investment conditions for the electricity sector.

3 A sovereign industrial capability is where Australia assesses that a Defence capability is strategically critical and must therefore have access to, or control over, the essential skills, technology, intellectual property, financial resources and infrastructure underpinning the capability, as and when required.

- We identified security concerns about the implementation of the Business Exemption Certificate regime, particularly that applications did not include adequate specificity on the asset or company to be purchased and/or the location of the investment. We worked with the Treasury to ensure that national security concerns would be appropriately addressed under the exemption certification process.
- We also provided advice to the Australian Government on the national security implications of amendments to the Credit Reporting Scheme, highlighting discrepancies between the credit reporting bureaus and the banking sector in their regulation, oversight and security practices. Our advice contributed to legislative changes to require higher levels of data security assurance under the scheme.

Contact Reporting Scheme

The whole-of-government Contact Reporting Scheme (CRS), managed by ASIO, continued in 2017–18 to be a valuable tool in defending against harm from espionage, foreign interference and trusted insiders, providing leads on potential espionage and hostile foreign intelligence activity directed against Australia, including attempts to cultivate or recruit Australian Government employees. CRS reports have produced security intelligence leads that would not otherwise have been identified.

ASIO Protective Security Directorate (ASIO-T4)

ASIO-T4 provides expert protective security advice and technical surveillance countermeasures services to the Australian Government and other entities. Key clients of ASIO-T4 include owners and operators of national critical infrastructure, both government and privately owned. ASIO-T4 is also a significant contributor of protective security advice and guidance to the Australia – New Zealand Counter-Terrorism Committee.

During the reporting period, ASIO-T4 provided 71 security product evaluations, 89 Zone 5 (Top Secret) facility inspections, and a range of protective security publications to support industry and government, including entities considered ‘at risk’. These publications distil ASIO-T4 expertise into practical ‘how to’ guidance material, which security practitioners can apply to their own facilities. In 2017–18, we continued to add to the series of publications, including addressing topics of current interest to recipients, to ensure they have the information they need to take practical steps to better protect their staff, property and information, an initiative welcomed by recipient entities.

In addition, ASIO-T4 ran four protective security training courses for industry and government, and we partnered with federal, state and territory government security practitioners to develop and deliver protective security training courses and tailored advice. In 2017–18 ASIO-T4 also developed and delivered the ‘Introduction to Counter-Terrorism Protective Security Training’ course for government security practitioners and continued our capacity-building program to help stakeholders self-manage security risks.

Table 18: ASIO-T4 advice and services

Advice/service	2015–16	2016–17	2017–18
Protective security reports, including: ▸ ASIO Technical Notes ▸ circulars for government ▸ industry guides ▸ equipment guides	13	13	16
Zone 5 physical security site inspections	50	80	89
Zone 5 site certifications	24	39	60
SCEC-approved locksmith briefings	2	1	1
Security equipment guides	1	1	4
Courier evaluations	6	3	1
Safe maintainer courses	2	2	2
Lead agency gateway facility inspections	N/A	3	1
Lead agency gateway facility certifications	8	2	3
Security equipment evaluations	105	179	71
Protective security training courses	2	4	4
SCEC-approved consultant briefing	_	1	_
Destruction service approvals	3	9	_
Protective security review reports	4	1	1

Note

1. Zone 5 physical security site inspections—increase across 2016–18 driven by reporting requirements introduced by the Department of the Prime Minister and Cabinet; and increased construction of Zone 5 areas.

2. Zone 5 site certifications—delay between inspection and certification due to identified remediation works and time taken to rectify.

3. Courier evaluations—decreased evaluations due to phasing out of current evaluation scheme; new evaluation scheme will be introduced in 2018–19.

4. Security equipment evaluations—2016–17 increase driven by industry requests, in relation to testing program and prioritisation of testing within T4 works program.

5. Destruction service approvals—approval process was transitioned from T4 to the National Association for Information Destruction as a partnership arrangement developed under an ASIO-T4 terms of reference.

6. Protective security review reports—increased education of Agency Security Advisers and Industry Security Managers via BGLU and T4 Security Manager Guides has reduced the requirement to undertake security reviews.

ASIO's international relationships

ASIO's international partnerships reflect the nature of the international security environment. ASIO's legislated responsibilities extend to threats to Australia, Australians and Australian interests, wherever they are located. Our interests and reach must necessarily be global, and ASIO's network of international partnerships reflect this. We have relationships with over 350 intelligence services, in more than 130 countries.

ASIO is a trusted, professional and cooperative partner for these security and intelligence services. While the level of engagement with individual services necessarily differs, together our network of international partnerships provides access to unique and important lines of intelligence and assessment, as well as operational engagement, capability enhancement, training and benchmarking.

The primary role of our liaison posts is to develop, expand and enhance cooperation with foreign intelligence services on issues relevant to Australia's security. ASIO also hosts and manages a number of foreign service representatives in Australia and uses those relationships to complement our overseas engagement program.

In addition to our overseas representation, ASIO participates in a range of bilateral and multilateral forums covering strategic security issues, intelligence exchange, and operational and capability development matters. ASIO's engagement with foreign partners yields unique value and provides a very significant dividend against the resource investment. ASIO's overseas engagement and representation complement, but do not duplicate, those of our AIC partner agencies.

Enduring and profitable intelligence partnerships are two-way, even if the balance is more in one party's favour at any particular point in time. Productive partnerships with foreign services are built on shared interests, shared function and mandate, as well as trust and relationship—both institutional and personal.

Public outreach

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 parliamentary or Senate hearings. The Director-General and Deputy Directors-General also speak at select public seminars or conferences. ASIO's website has information on public speeches and statements made in 2017–18.

The media can contact ASIO directly through a publicly listed media contact number and email address. In 2017–18, ASIO continued to respond to media inquiries, without commenting on operations, investigations, individuals or operational capabilities.

Public access to ASIO records

ASIO is an exempt agency under the *Freedom of Information Act 1982* but is subject to release of records under the *Archives Act 1983* (the Archives Act), 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. The open period currently covers all records created before 1996. ASIO works closely with the National Archives in facilitating access to ASIO records while balancing various and sometimes competing priorities.

During the reporting period, 345 applications were made for access to records, and a total of 310 requests were completed.

'Internal reconsideration' cases are where a previous decision regarding the assessment of a record is reviewed under section 42 of the *Archives Act 1983*. In 2017–18, seven internal reconsiderations were processed, and the National Archives upheld the ASIO decisions.

Applicants may appeal exemptions to the Administrative Appeals Tribunal (AAT) and also appeal if their application is not completed within 90 days. There were no new applications to the AAT during the reporting period.

Table 19: Access to ASIO records

	2015–16	2016–17	2017–18
Applications for record access	473	484	345
Requests completed	650	478	310