Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure

No.16 2016–2017

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 into Administration and Expenditure No. 16 provides a detailed account of ASIO's administration and budgetary activities during the financial year 2016–17. The submission addresses specific topics requested by the PJCIS, including the following:

- strategic direction and priorities;
- corporate governance;
- 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 and retention strategies and outcomes, workplace diversity statistics and initiatives;
- training and development, and individual performance management;
- staff feedback, complaints and investigations;
- changes to the distribution of staff across different areas of the organisation;
- matters relating to security;
- information and communications technology initiatives; and
- public relations and public reporting.

In particular, the submission provides the PJCIS with information on the overall financial position of the agency, the impact of funding increases and budget measures, budget constraints, efficiencies and savings measures, financial controls, and any significant changes in recurrent expenditure.

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

ASIO'S ROLE AND FUNCTIONS

ASIO is responsible for protecting Australia, its people and its interests from threats to security, through intelligence collection and assessment, and for providing advice to the Australian Government, government agencies, business and other approved entities.

In 2016–17 ASIO pursued our purpose through five key activities:

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

Our statutory functions are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). Importantly, 'security' is 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 in relation to 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 Australian 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.

SECURITY ENVIRONMENT

Terrorism

The threat from terrorism in Australia remains elevated. Three recent disrupted attack plots—in December 2016 and November 2017 in Melbourne, and July 2017 in Sydney—provide a stark reminder of the threat Australia faces and the need to be prepared for attacks spanning a range of tactics and capabilities. The most likely form of terrorism in Australia remains an attack by an individual or small group.

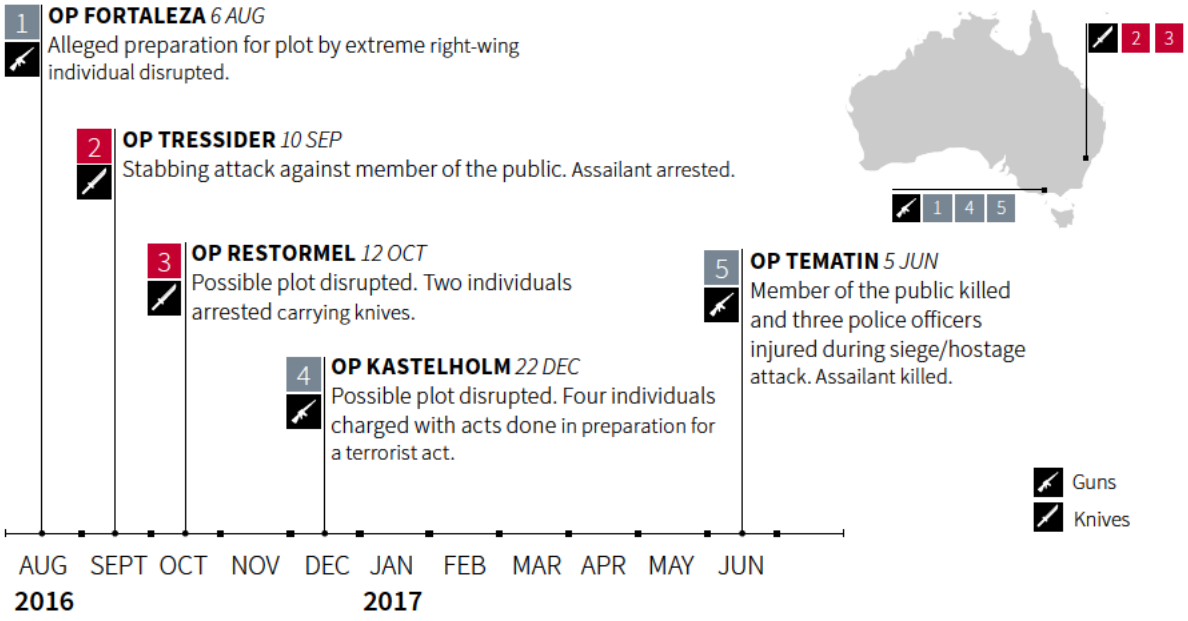
In 2016–17, the national terrorism threat level remained at PROBABLE—credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to conduct a terrorist attack in Australia. Since the national terrorism threat level was raised on 12 September 2014, there have been 14[1] major disruption operations in relation to imminent attack planning, and five terrorist attacks targeting people in Australia. All but one were linked to or inspired by Islamist extremists, particularly the Islamic State of Iraq and the Levant (ISIL).

Globally in 2016–17, terrorist attacks emerged with little or no forewarning, many using basic weapons and targeting the public in readily accessible locations. Such attacks are highly challenging to identify and prevent. ISIL was the main driver of terrorist attacks in many countries, including the United States, Europe, Bangladesh, Turkey and the Philippines. The attack in Nice, France, in July 2016—where an individual drove a truck through a crowd, killing over 80 people—showed the extreme lethality of an attack using 'simple' tactics. The reporting period also saw the first instances of ISIL affiliates being involved in successful attacks in Western countries.

Islamist extremist English-language propaganda, particularly from ISIL, continued to call for terrorist attacks in Western countries, including Australia. As ISIL lost territory in Syria and Iraq, the tone of its propaganda changed from superiority to reframing success, with supporters encouraged to fight the West in their home countries rather than travel to ISIL-held territory.

Al-Qa'ida continues to be an ongoing threat to the West. During 2016–17, al-Qa'ida continued to rebuild, and by the end of the reporting period it was stronger than it had been for over a decade. Through its network of affiliates, al-Qa'ida increased its support and influence in the Middle East, Africa and South Asia.

Figure 1: Onshore terrorist attacks and disruptions 2016–17



1 As at 5 December 2017

Violent protest and communal violence

In 2016–17, most protests in Australia complied with regulations and concluded without significant incident. Ongoing hostility between extreme left-wing and anti-Islam/extreme right-wing proponents occasionally resulted in confrontational behaviour, but violence was minimal.

High-level international visits provoked some small-scale violence from elements in some Australia-based diaspora communities. However, generally Australia continues to experience low levels of communal violence.

Espionage and foreign interference

The threat from espionage and foreign interference to Australian interests is extensive, unrelenting and increasingly sophisticated. In addition to traditional espionage efforts to penetrate Australian governments, foreign intelligence services are clandestinely targeting a range of other Australian interests, including our intellectual property, science and technology, and commercially sensitive information. Foreign intelligence services are also using a wider range of techniques to obtain intelligence and clandestinely interfere in Australia's affairs. There has been a greater focus on covert influence operations, in addition to the traditional methods of human-enabled collection, technical collection and exploitation of the internet and information technology.

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

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

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

Border integrity

During 2016–17, Operation Sovereign Borders and offshore regional processing continued to deter people-smuggling operations to Australia. However, while demand from potential illegal immigrants has fallen, it is not universally or permanently suppressed.

In the reporting period, illegal maritime ventures to Australia continued to be organised mainly from Sri Lanka and Indonesia, and potential illegal immigrants from Sri Lanka, Bangladesh, Afghanistan, Myanmar and Vietnam showed the greatest interest in illegal travel. Planned and actual illegal maritime ventures to Australia will remain an enduring challenge over the next decade.

ASIO continued to support the Australian Government's efforts to counter people-smuggling, identifying individuals involved and assisting partners' disruption activities.

In 2016–17, ASIO continued to collaborate closely with the Department of Immigration and Border Protection (DIBP) and other national security partners to meet whole-of-government priorities in relation to visa, citizenship and other border-related security assessments. Among other activities, ASIO provided assessments and advice to support government initiatives such as the additional Syrian–Iraqi refugee intake and the agreement with the United States Government to resettle detainees from Manus Island and Nauru.

STRATEGIC DIRECTION, PERFORMANCE AND CORPORATE GOVERNANCE

Strategic direction

ASIO's purpose is to protect the nation, its people and its interests from threats to security. The environment in which we work provides opportunities but also a series of significant challenges. The variety of threat actors has expanded, threats develop more rapidly and society's use of online technologies, including encryption, has risen exponentially. The requirement to understand and exploit cutting-edge technology platforms is more acute now than ever before.

Other challenges include recruiting and retaining skilled knowledge workers, especially those with technical skills, and the need for big data analytics to manage an increasing variety, velocity and volume of data. We are committed to meeting these challenges by encouraging diversity and innovation in our workforce and our work practices, while also enhancing our strategic capability.

During the 2016–17 reporting period, we continued to address these challenges. Highlights from the year include the introduction of an innovation strategy to foster a culture of innovation within ASIO, information technology initiatives, an ASIO-wide promotion of diversity and inclusion, and a continued recruitment drive for workers with technical skills.

We also implemented a tailored approach to risk management across all levels of our business, in three categories: preventable risks, strategy risks and external risks.

ASIO2020

ASIO2020 provided the key mechanism for our strategic direction and reform program during the reporting period. Commenced on 1 July 2016, the ASIO2020 program set out to address the most significant challenges to ASIO's future success. ASIO2020 has four strands of work that set our strategic capability agenda:

- Context—our authorising and task environments;
- Culture—the backbone to our success;
- People—our most important asset; and
- Systems—how we work (our practices, tools and mindsets).

In the 'Context' strand, we aim to maximise our contribution to society, ensuring our value is understood by our society, government and partners. In the 'Culture' strand, we focus on ensuring we have a positive work culture that drives productivity, enabling a culture of diversity and innovation. In the 'People' strand, we focus on how to obtain maximum benefit from our people and how to recruit and retain the people we need in the future. In the 'Systems' strand, we focus on how we work and we support a 'data discovery' approach that enables us to learn and manage tomorrow's security challenges.

Technology initiatives

ASIO is facing unprecedented disruptions in our operating environment that continue to challenge our capacity to protect Australia and its people from serious threats to their security. To ensure ASIO can fulfil its mission and remain accountable and effective, we have to address rapid advances in technology and the exponential rise in the volume and variety of data we need to access and interpret.

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* (the PGPA Act). The plan is available online from www.asio.gov.au.

The 2017–18 Corporate Plan builds on the 2016–17 Corporate Plan and reinforces ASIO's commitment to protecting Australia, our people and our 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—ASIO's areas of strategic focus for 2017–18—are:

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 our previous corporate plan—will be managed in 2017–18 as a subset of the 'Countering espionage, foreign interference and malicious insiders' activity.

The 2017–18 Corporate Plan recognises the vital role our federal, state and territory, and industry partners play in managing security risks and disrupting activities that threaten Australia's security, as well as ASIO's role in providing security intelligence assessments and advice to support that work.

As required by the PGPA Act, at the end of 2017–18 we will prepare annual performance statements that provide an assessment of how we have performed in relation to our 2017–18 Corporate Plan key activities. An unclassified version of the performance statement will be included in our 2017–18 annual report to parliament.

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

The Prime Minister released the review's report in July 2017. The review found that Australia's intelligence agencies were highly capable and staffed by skilled officers of great integrity. It 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

Our annual performance statements for 2016–17, contained within the *ASIO annual report 2016–17*, highlight our key performance outcomes during the reporting period. These achievements include:

- working with law enforcement partners to disrupt three planned terrorist attacks targeting people in Australia and to disrupt other terrorism-related activities;
- providing assessments that prevented travel by extremists to the conflict zone in Syria and Iraq;
- supporting terrorism-related prosecutions in New South Wales, Victoria and Queensland;
- continuing the identification and investigation of harmful espionage and foreign interference directed against Australia;
- identifying new leads into potential foreign intelligence activity through our management of the Contact Reporting Scheme;
- issuing 27 182 personnel security assessments to support decision-making on the granting of security clearances;
- providing 265 assessments to support the Foreign Investment Review Board process;
- providing 14 358 visa security assessments and 141 784 access security assessments to support the decision-making of DIBP and other national security partners in relation to the granting of visas, citizenship or access to security-controlled areas and substances;
- supporting Australian Government policy-making and responses in relation to a wide range of terrorism, espionage and foreign interference, and border security issues;
- publishing 1 433 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, particularly through ASIO's Business and Government Liaison Unit website and industry briefing days and through physical security advice from ASIO's Protective Security Directorate (ASIO-T4).

The annual report was tabled in parliament on 17 October 2017 and is available from ASIO's website.

Organisational structure

ASIO is structured into three groups: Strategy, Counter-Espionage and Interference & Capabilities, and Counter-Terrorism. This functional arrangement reflects the resources and governance required for our dominant and high-risk activities. Since its launch in August 2015, the structure has proven to be an effective and agile mechanism to utilise ASIO's resources efficiently. It is important that we continue to review our structure on a regular basis to ensure ongoing fitness for purpose in the face of emerging threats and challenges. The structure is shown in Figure 2.

Corporate governance

The Director-General of Security is the accountable authority for ASIO under the PGPA Act. Our corporate governance structure supports the Director-General to fulfil his responsibilities.

Following a review of our governance arrangements, in June 2017 ASIO launched a new corporate governance structure in which ASIO's Executive Board is supported by six standing committees: the Intelligence Committee, the Capability Committee, the Workforce Committee, the Security Committee, the Finance Committee, and the ASIO Diversity and Inclusion Committee. These standing committees are chaired at the Deputy Director-General level and are responsible for program-based performance and risk evaluation and reporting to the Director-General and the Executive Board. Alongside these, the Audit and Risk Committee continues in its role as a source of independent advice and assurance to the Director-General.

The new committee structure and the introduction of program-based evaluation and risk reporting arrangements will strengthen our oversight of performance and risk management. Reporting to the Executive Board will focus on performance outcomes for key activities and enabling programs, as well as any associated risks. The new arrangements will be implemented during the 2017–18 reporting period.

Corporate governance committees

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

ASIO Executive Board

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

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

In 2017–18, following the changes to the governance structure, the Executive Board's work program will focus on the program-based evaluation of performance and the management of program-based risks across all lines of effort.

Figure 2: Organisational structure

as at 30 June 2017

Duncan Lewis

DIRECTOR-GENERAL OF SECURITY

Deputy Director-General *STRATEGY*

First Assistant Director-General

State Manager NSW North	Executive	State Manager VIC South	Corporate and Security	Office of Legal Counsel
Assistant Director-General				
	Office of the Senior Executive		Internal Security	Assessments, Corporate Law and Capability Protection
	Strategic Partnerships and Production	State and Territory Managers	Financial Management	Operations Law
	ASIO2020		Human Resources	Litigation
			Property	

Deputy Director-General *COUNTER-ESPIONAGE AND INTERFERENCE & CAPABILITIES*

Technical Capabilities	Operational Capabilities and Training	Information	Counter-Espionage and Interference
Data and Technical Analysis	Physical Surveillance	IT Infrastructure Services	CEI Operations
Tele-communications Operations	Operations Services	Business Information Systems	CEI Investigations 1
Computer Operations	Training	Information Services	CEI Investigations 2
Close Access Operations		ICT New Policy Proposals	CEI Assessments
Strategy and Performance			Defence and Engagement

Deputy Director-General *COUNTER-TERRORISM*

Counter-Terrorism	Security Advice and Assessments	Centre for Counter-Terrorism Coordination
Counter-Terrorism Coordination	National Threat Assessment Centre	Centre for Counter-Terrorism Coordination
Counter-Terrorism Investigations 1	Border Investigations and Assessments	
Counter-Terrorism Investigations 2	Intelligence Discovery, Investigations and Assessments	

Intelligence Coordination Committee

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

Workforce Capability Committee

The Workforce Capability Committee's focus during the reporting period was ensuring our workforce was sufficiently sized, skilled, equipped and accommodated to meet the current and future needs of our Organisation. The Work Health and Safety Committee was a subcommittee responsible for ensuring better health and safety policies and practices across ASIO. The committee was chaired by the Deputy Director-General, Strategy.

Security Committee

The Security Committee provided advice to the Executive Board on the evolving security environment and matters relating to the security of our operational activities, people, property and information technology. It also approved revised security policies and procedures and reviewed our compliance with Australian Government security standards. The committee was chaired by the Deputy Director-General, Strategy.

Finance Committee

The Finance Committee provided advice to the Executive Board on financial strategy, resource allocation within ASIO, accommodation and assets. The committee was chaired by the Deputy Director-General, Strategy.

Audit and Risk Committee

In line with the requirements of section 45 of the PGPA Act, the Director-General established the Audit and Risk Committee in 2015. During the reporting period, the committee provided independent assurance and advice to the Director-General and the Executive Board on our financial and performance reporting responsibilities, risk oversight and management, and system of internal control.

The committee had four external members—including an external chair—and three internal members. Observers from the Australian National Audit Office also attended committee meetings.

Fraud control and management

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

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

The ASIO Fraud Control Framework 2016–18, which is available from ASIO's website, 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 to parliament. 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 post-Budget.

In 2016–17, ASIO received revenue from government totalling $445.2 million, comprising $403.0 million in operating funding and for capital activities, $28.1 million in Departmental Capital Budget and $14.1 million in equity injection.

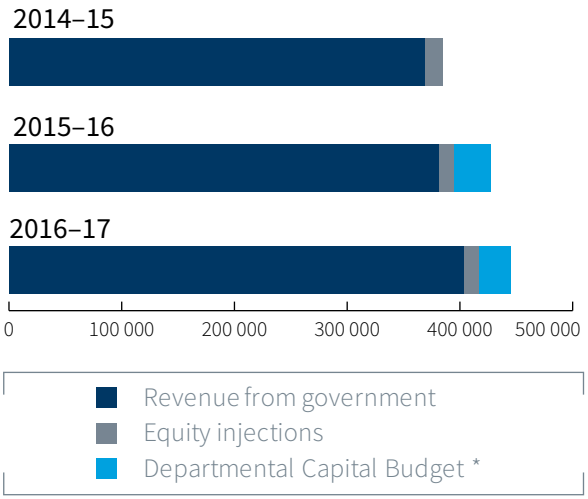
The 2016–17 financial year was the third year of the new policy proposal 'Enhancing security intelligence capabilities to counter the Islamist terrorism threat'. During the financial year, this measure received $45.3 million in operating funding and an equity injection of $14.1 million for capital activities.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

The 2016–17 financial year was the second year of funding under the 'Syrian and Iraqi humanitarian crises' new policy proposal. During the reporting period, we received operating funding of $0.6 million for this measure.

There are significant resourcing pressures in other areas of our work that will be exacerbated by changes to our budget over the forward estimates.

During 2016–17, ASIO returned approximately $24.1 million to the government through the efficiency dividend and other savings measures ($21.4 million in the efficiency dividend and $2.7 million in savings 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) and the 2017–18 operating budget, and across the forward estimates ($65.5 million).

Figure 3 : Revenue from government ($'000's)



* Departmental Capital Budget was rephased from 2012–13 to 2015–16 into the 2017–18 and 2018–19 forward estimates. Adjustments relating to 2012–13 and 2013–14 were made against the 2014–15 Departmental Capital Budget.

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

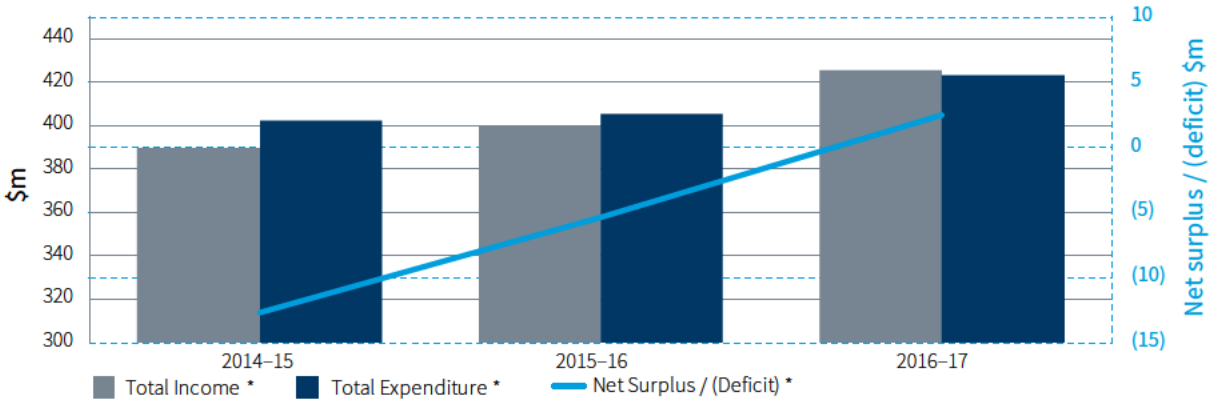
We will continue to identify and implement efficiencies and rigorously prioritise our activities to ensure we operate within future budget allocations. However, further consideration will be given during 2017–18 to the sustainability of our current operations in light of our projected DCB and operating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

Financial performance

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

We achieved a small surplus of $2.5 million (excluding depreciation), which represents 0.6 per cent of budget. This result would have broken even except for favorable interest rate movements, which had a positive impact on the accounting required for employee leave provisions.

Figure 4: Financial performance



Resource allocation and capital items

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

In line with the previous reporting period, ASIO's expenditure continued to be predominantly operationally related (81 per cent).

The expenditure on capital items increased during the reporting period. This increase relates to assets whose replacement was delayed while ASIO's new central headquarters were commissioned.

Figure 5: Resource allocation

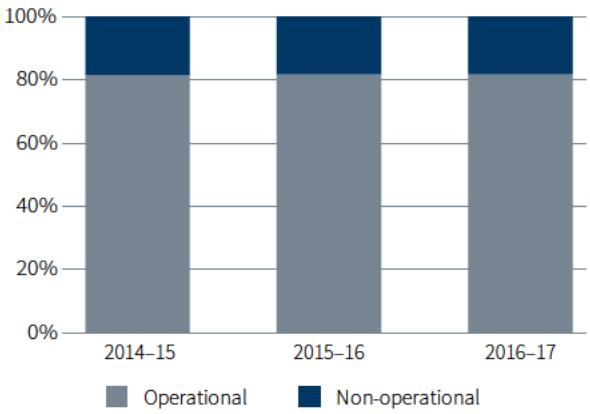
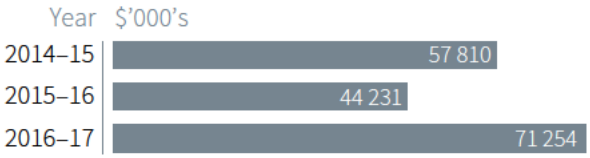


Figure 6: Purchase of capital items



Financial management and internal controls

ASIO prepares annual financial statements in accordance with the provisions in subsection 42(2) of the *Public Governance, Performance and Accountability Act 2013* (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 2016–17, 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 and the Executive Board. Reporting includes current and future organisational financial performance matters and strategic financial management planning. ASIO's financial management practices are underpinned by a financial management information system with integrated internal controls aligned to the Organisation's financial framework. The Chief Finance 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 mandatory compliance audits, required by either legislation or agreements, and performance reviews.

HUMAN RESOURCE MANAGEMENT

During the 2016–17 reporting period, ASIO continued to effectively manage and develop a highly capable workforce in a challenging security and operating environment. We further strengthened our recruitment arrangements to ensure that we continue to attract and effectively develop the people required for ASIO to continue to meet its objectives. We provided staff with extensive training and development opportunities, which were consistently highly rated by participants. We also assessed our workforce at all levels through a performance management framework that evaluated capability and performance and provided pathways to further develop staff capabilities.

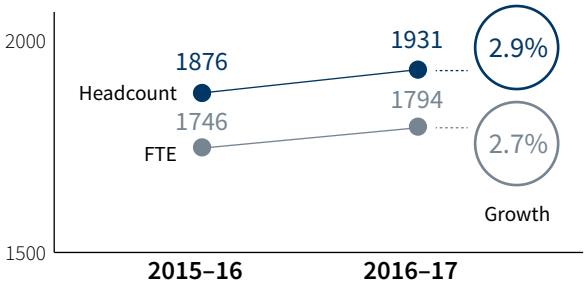
At the end of 2016–17, ASIO employed 1794.3 full-time equivalent (FTE) staff, an increase of 2.7 per cent from 2015–16.

The reporting period saw an increase in the number of ASIO employees accessing flexible work arrangements through part-time employment. There was also a reduction in the number of casual employees.

Workforce statistics

ASIO conducted a review of its workforce metrics in financial year 2016–17 to align workforce reporting with guidance from the Department of Finance. The changes reflect the inclusion of the Director-General and the exclusion of secondees into ASIO and staff engaged locally at ASIO's overseas posts, or as indicated in the relevant notes under each data set. Data has been retrospectively amended for 2015–16 for comparative purposes.

Figure 7: Staffing growth



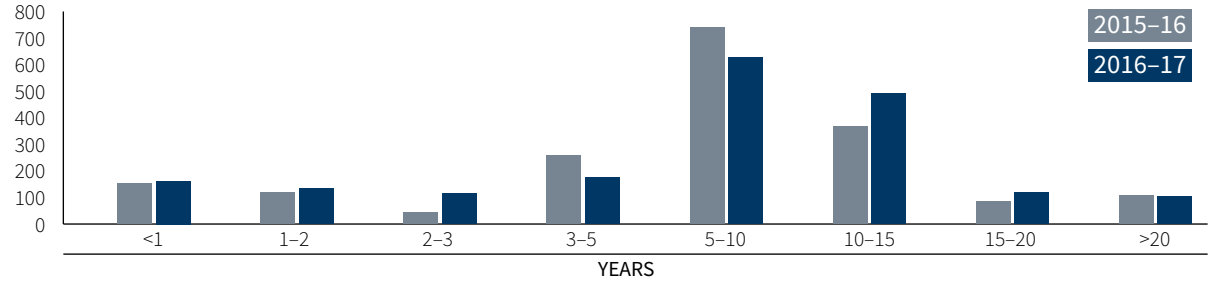
Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff overseas.

Table 1: Headcount of staff by load and employment status

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

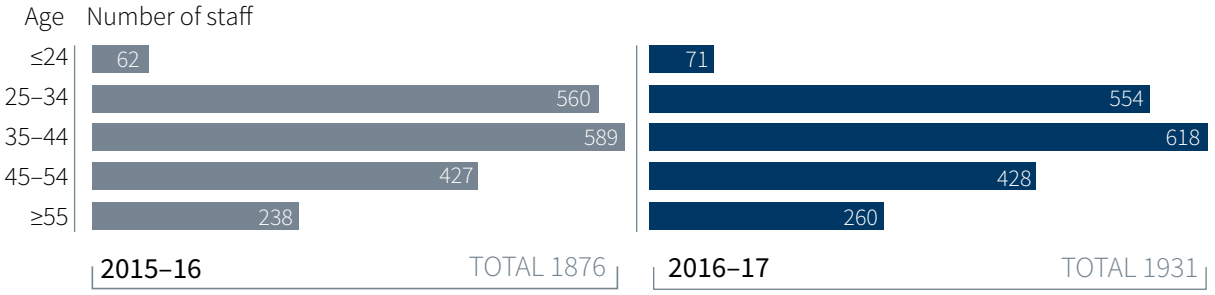
Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff overseas.

Figure 8: Length of service



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

Figure 9: Age profile



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

Table 2: Headcount of staff by gender and employment status

	2015–16				2016–17			
Gender	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Female	812	8	14	**834**	844	10	14	**868**
Male	980	17	45	**1042**	1007	20	36	**1063**
Total	1792	25	59	**1876**	1851	30	50	**1931**

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

Table 3: Workplace diversity

Classification	Total staff	Women	Non–English speaking background	Aboriginal and Torres Strait Islander	People with a disability	Available EEO data[2]
			2015–16			
Senior Executive Service (incl DG)	53	18	3	-	-	48
Senior Officers (AEE1–3)	540	196	72	1	6	496
Employees (AE1-AE6)	1153	599	195	7	9	1082
IT Employees (ITE1/2)	122	21	17	2	3	116
Engineers (Grade1/2)	8	-	-	-	-	8
Total	**1876**	**834**	**287**	**10**	**18**	**1750**
			2016–17			
Senior Executive Service (incl DG)	53	21	3	-	-	47
Senior Officers (AEE1-3)	550	194	76	2	5	506
Employees (AE1-AE6)	1191	631	220	9	10	1123
IT Employees (ITE1/2)	119	20	21	1	4	112
Engineers (Grade1/2)	18	2	4	-	-	17
Total	**1931**	**868**	**324**	**12**	**19**	**1805**

Notes:
1. Includes the Director-General and excludes secondees into ASIO and locally engaged staff overseas.
2. Provision of Equal Employment Opportunity (EEO) data is voluntary. Data is considered 'available' if a staff member has provided information on at least one diversity category (incl. first non-English language and parents' first language).

Table 4: Headcount of employees by location and employment status

	2015–16				2016–17			
	Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Canberra-based	1259	18	48	**1325**	1312	17	37	**1366**
Other locations	533	7	11	**551**	539	13	13	**565**
Total	**1792**	**25**	**59**	**1876**	**1851**	**30**	**50**	**1931**

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

Table 5: Headcount of employees by classification and employment status

		2015–16				2016–17			
		Ongoing	Non-ongoing	Casual	Total	Ongoing	Non-ongoing	Casual	Total
Director-General	DG	1	-	-	**1**	1	-	-	**1**
Senior Executive Service	SES Band 3	2	-	-	**2**	2	-	-	**2**
	SES Band 2	12	1	-	**13**	11	-	2	**13**
	SES Band 1	34	2	1	**37**	34	2	1	**37**
Senior Officers	AEE2/3	156	3	1	**160**	175	3	1	**179**
	AEE1	373	3	4	**380**	365	3	3	**371**
Employees	AE1–AE6	1085	16	52	**1153**	1128	21	42	**1191**
IT Employees	ITE1/2	121	-	1	**122**	117	1	1	**119**
Engineers	Grade1/2	8	-	-	**8**	18	-	-	**18**
Total		1792	25	59	**1876**	1851	30	50	**1931**

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

Commencements and separation rates

ASIO continued to grow during the reporting period, in line with funding from the 'Enhancing security intelligence capabilities to counter the Islamist terrorism threat' new policy proposal. This additional funding made an important contribution to our recruitment efforts.

As at 30 June 2017, our separation rate was 5.26 per cent, a slight increase on the separation rate of 4.44 per cent in 2015–16. The main reasons given by employees separating from ASIO were transfer to another government department or the private sector as a means of broadening their career, and retirement.

Table 6: Separations 2016–17

	2016–17
Reason	Total
Resignation	80
Age retirement	10
Retirement: Invalidity	1
Other	67
Separations	158

Notes:
1. Includes the Director-General and ongoing, non-ongoing and casual employees.
2. 'Other' includes contract expired, contract terminated, deceased, dismissed, secondees into ASIO and locally engaged staff overseas.

Recruitment and retention strategies

After a review of selection and assessment methodologies for our graduate and trainee programs in the previous financial year, ASIO implemented the following changes in 2016–17:

- use of a more robust scoring and assessment matrix to meet best-practice standards;
- use of behaviourally anchored rating scales to more accurately assess candidates' core capabilities and to ensure standardisation;
- a focus on reducing unconscious bias;
- enhanced training of assessors and panels; and
- alignment of 'organisational fit' with the ASIO Values, and increased rigour in recording and assessing concerns about organisational fit.

ASIO's 2015–16 review of our advertising and marketing strategies resulted in the following enhancements during the reporting period:

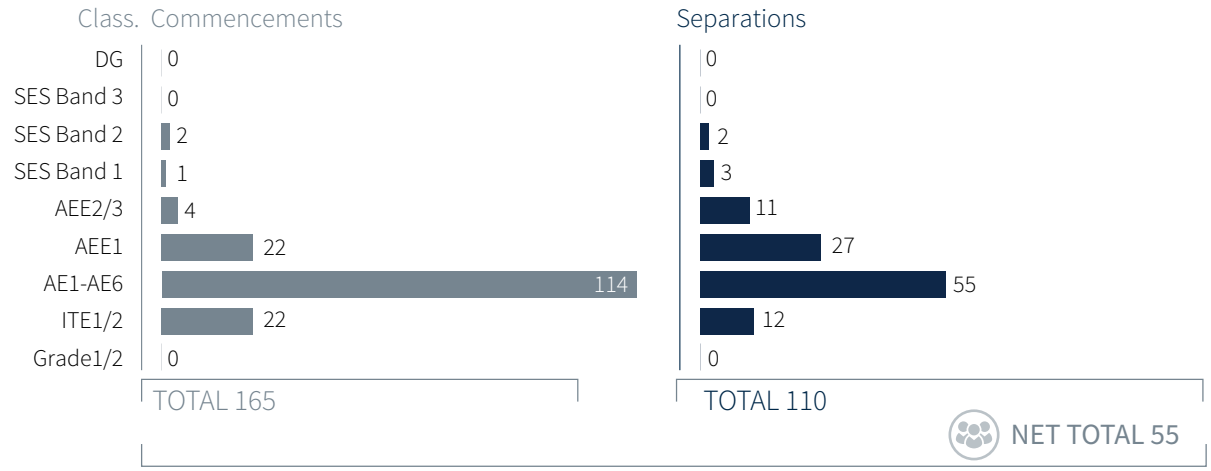
- further refinement of advertising concepts, including use of language and imagery;
- revised website content and navigation: and
- greater use of social media advertising.

In 2017–18, our marketing and advertising will continue based on these initiatives.

Significant recruitment changes in 2015–16, such as the continuous acceptance of applications for the role of Intelligence Officer (IO) and the introduction of the Intelligence Analyst Development Program (IADP) stream, had mixed effects. While continuous IO recruitment was trialled during the reporting period and candidate numbers were solid, the continuous model proved to be resource intensive and ceased in 2016–17. However, the new IADP stream has been well received, with all IADP places filled.

Graduate recruitment is an important part of ASIO's recruitment strategy, focusing on recruitment not only for IOs and IAs but also for technical graduates. Career fairs are an effective way to engage directly with graduating students, as well as initiating contact with students in their first and second years of study. The effectiveness of this approach was evidenced by reports from 'new starter' surveys in 2016–17.

Figure 10: Commencements and separations by classification 2016–17



Notes:
1. Includes the Director-General and ongoing, non-ongoing and casual employees.
2. Excludes secondees and locally engaged staff overseas.
   - A total of 48 secondees into ASIO and locally engaged staff overseas separated from ASIO in financial year 2016–17.
   - A total of 34 secondees into ASIO and locally engaged staff overseas commenced with ASIO in financial year 2016–17.

Recruitment

Recruitment outcomes

In 2016–17, ASIO conducted a total of 48 recruitment activities, including larger bulk rounds and campaigns. This focus reduced the need to run a larger number of smaller recruitment activities.

Table 7: Recruitment outcomes

Financial year	Number of applications received	Applicants found suitable at interview / Assessment Centre	Percentage of total applicants found suitable
2014–15	5462	355	6%
2015–16	12 997	278	2%
2016–17	10 211	605	6%

Employment Register

The Employment Register is a continuous vacancy advertised on the ASIO website, allowing candidates to apply online for employment with ASIO. A review of the Employment Register was undertaken in 2016–17 and revealed that the register provided small recruitment yields, through a considerable resource commitment and effort by a number of work areas. Following the review, targeted 'job family' listings for hard-to-fill roles were introduced and limited to the following job families: ICT roles, technical engineering and trade, and data analysts/ scientists.

Secondments

To enhance collaboration across all areas of our purpose, ASIO pursues and provides secondment opportunities to a wide range of federal, state and territory government agencies, international counterparts, and other bodies. As at 30 June 2017, ASIO had 37 secondees into the Organisation and 21 secondees from the Organisation in relation to Australian Government agencies.

Workforce management

Workplace agreement

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

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.

During the reporting period, the council continued 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 representatives from the Staff Association.

Individual performance management

Building on reforms implemented during 2015–16, we formalised the requirement for managers and employees to hold performance discussions and agree on performance expectations at the beginning of the performance cycle, falling on 1 July, with a compliance period to 31 August each year. These discussions provide the basis for developing staff and organisational capabilities by identifying capability requirements and establishing agreement on training or other development opportunities.

The focus throughout the 2016–17 performance cycle was on educating the broader Organisation on the performance process, particularly the importance of meeting cycle deadlines. This has been highly successful, with 100 per cent of eligible staff compliant with the Organisation's performance management obligations in 2016–17. Six staff members participated in formal underperformance management processes during the reporting period.

The emphasis for the 2017–18 cycle will be on the quality of the expectations discussions, educating and supporting managers and increasing proactive interaction with all employees regarding optimising performance.

In 2016–17 we refreshed our Career Management Framework and commenced a comprehensive review of the skills and capabilities required in our intelligence, technical, information and corporate roles. The objectives of this work were to:

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

We are working to finalise an update of our Career Management Framework and competency mapping by the end of 2017–18.

Staff survey

ASIO conducted a staff survey in June 2017. Results from the survey 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 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 could be improved, and the Director-General has made it a priority to address these. They include enhancing ASIO's Career Management Framework, improving recognition of individual and team achievement, and eliminating bullying.

The 2017 survey varied from that conducted in 2014. While the 2014 compliance and demographic questions remained intact, the remainder of the survey was amended to:

- provide simple and standardised measures to compare results across industry and government;
- streamline the survey process;
- reflect current best-practice engagement and measurement practices;
- enable collection of the underlying reasons for employee reactions; and
- reflect current strategic issues and topics of interest.

Ethics and conduct

ASIO's policies on ethics and conduct assist individuals and the broader Organisation in obtaining advice, reporting incidents and enabling reviews of reported incidents. These policies support an organisational culture based on ASIO's Values, which guide the decision-making and behaviour of employees.

ASIO's Human Resources Branch manages ethics and conduct matters 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.

Promotion of ethics

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

All staff, including our senior leaders, are required to complete mandatory training that:

- promotes our Values and Code of Conduct requirements;
- raises awareness of the mechanisms available to make a public interest disclosure;
- provides strategies for managing workplace discrimination, harassment and bullying; and
- explains work health and safety obligations.

Training on specific aspects relating to conduct and behaviour is also delivered through ASIO's management training programs and through presentations run by the Human Resources Branch. Both the Inspector-General of Intelligence and Security and ASIO's Ombudsman were involved across the suite of our training programs in providing advice on ethical and accountable behaviour in the workplace.

Harassment and Discrimination Adviser network

ASIO's network of Harassment and Discrimination Advisers (HaDAs) provides 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 complaints procedures. The role of a HaDA is voluntary, and appointment is for two years. There are currently 43 HaDAs across the Organisation.

Information provided to a HaDA is treated with strict confidence. However, if a HaDA believes there is a risk of harm to a staff member or a risk to security, relevant areas and support services will be advised.

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 work-related wrongdoing 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 2014, seven disclosures have been investigated and reported on, or allocated for investigation under another authority. During 2016–17, two disclosures were assessed as fitting the categories of possible maladministration and conduct that may result in disciplinary action and were allocated for investigation. Two disclosures were allocated to the Human Resources Branch for investigation under another authority.

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.

In 2016–17, the ASIO Ombudsman met regularly with our senior management and with representatives of the ASIO Staff Association. The ASIO Ombudsman also provided valuable support and advice to employees and line managers. During this reporting year, the ASIO Ombudsman:

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

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

In 2016–17, the ASIO Ombudsman was not involved in public interest disclosures.

Work health and safety

Our annual performance statement addresses the work health and safety matters we are required to address in our annual report under the *Work Health and Safety Act 2011* and the *Public Governance, Performance and Accountability Act 2013*.

During the reporting period we maintained a high level of workplace health and safety, through mechanisms such as our Work Health and Safety Committee, our health and safety representative network, first aid officers and our wellbeing program. ASIO's wellbeing program delivers cost-effective initiatives such as health assessments, an annual influenza vaccination program, and campaigns to raise awareness among staff about the benefits of a healthy lifestyle.

In 2016–17, ASIO conducted a performance review of our work health and safety (WHS) performance. The review evaluated the appropriateness of our WHS governance, communication and coordination arrangements and recognised efforts to integrate WHS considerations into our day-to-day work activities. It identified areas for action to further bolster our health and safety capacity and to ensure that the Organisation is best placed to respond to new and emerging WHS risks. Work is underway to implement the review's recommendations, which will strengthen our WHS framework.

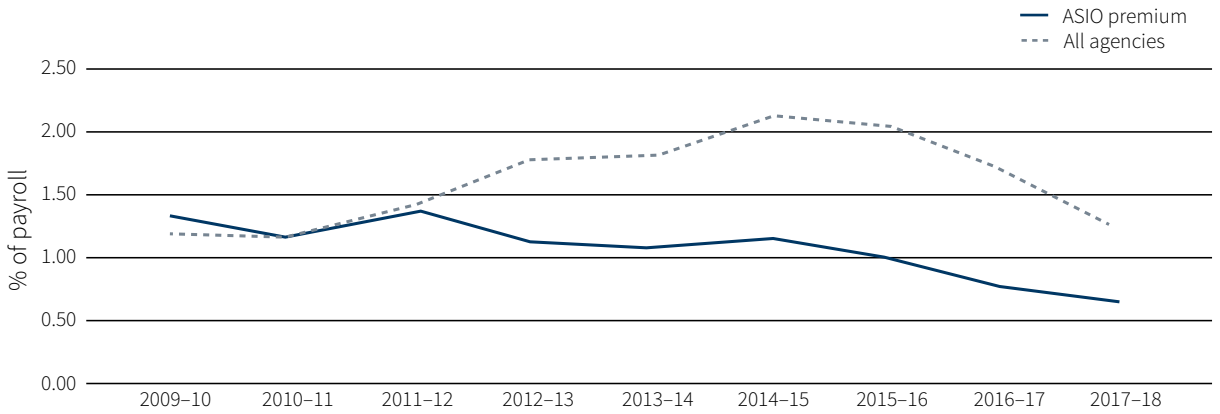
The effectiveness of our approach to WHS continues to be reflected in our Comcare premium rate, which remains well below the overall premium rate for Australian Government agencies (refer to Figure 11). In 2016–17, an internal audit examined ASIO's rehabilitation management system, processes and outcomes and validated our compliance with the *Safety, Rehabilitation and Compensation Act 1988* and Comcare's Guidelines for Rehabilitation Authorities 2012. No areas of noncompliance were identified.

In line with legislated notification obligations, ASIO reported eight incidents to Comcare in 2016–17. Comcare did not initiate any investigations into the notifiable incidents, and no notices were issued to ASIO under the Work Health and Safety Act.

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

We continued during the reporting period to enhance our WHS arrangements through a layered approach to personal safety and security training that begins at induction training for staff and is supplemented thereafter by a suite of courses and refresher training consistent with the nature of each officer's work. Over the past three years, we delivered training courses on ASIO situational awareness, general personal security, de-escalation, and hostile environment awareness. Additionally, where required, staff received training in 'spontaneous protection', functional first aid and driver training.

Figure 11: Comparison of Comcare premium rates 2009–10 to 2017–18



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

Note: the percentage of payroll for 2017–18 is indicative only.

Diversity

ASIO is committed to building a productive, innovative, capable and inclusive workforce that values difference and creates an environment where staff are supported in reaching their full potential. In 2016–17 we undertook a range of work in support of that vision, including:

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

ASIO also launched our Gender Equity Bold Goals program, which reinforces our commitment to achieving gender equity across all levels of ASIO by 2020. Within this program, we introduced the first stage of an 'If not, why not' approach to flexible working. This approach to flexible workplace arrangements means that we are open to having a conversation with all employees about how they can work flexibly in their current role—noting that some exclusions will necessarily apply. In addition, we achieved the following:

- specified a shortlisting ratio of 40 per cent female, 40 per cent male and 20 per cent of either gender for promotion rounds at Executive Level 1 and above;
- delivered training on unconscious bias to Senior Executive Service officers and key functional areas;
- publicised (internally) detailed gender metrics for ASIO promotion, transfer and recruitment rounds;
- joined the Diversity Council of Australia; and
- appointed an SES Band 2 level officer as ASIO's Male Champions of Change Implementation Leader, a role that supports the Director-General's activities as a Male Champion of Change.

In 2016–17, we also provided opportunities for staff to broaden their understanding and awareness of gender equity issues through a range of presentations, including from Her Excellency Menna Rawlings CMG, British High Commissioner to Australia; and Annabel Crabb, journalist, author, television presenter and commentator.

Accommodation and facilities

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

TRAINING AND DEVELOPMENT

During this reporting period, ASIO provided a broad and growing range of personal and professional developmental opportunities to meet the diverse needs of our workforce, informed by the findings of a training review commissioned by the Director-General in 2014–15. In 2016–17:

- we approved or conducted 146 training courses, with 4256 face-to-face training activities attended by 1387 staff; and
- staff completed 2839 mandatory and 1928 non-mandatory e-learning courses.

The face-to-face training courses encompass a wide range of topics, including induction courses for new starters; officer safety and first aid training; foundational and advanced/refresher analytical and operational training; IT training; and management and leadership training.

Our training programs were delivered by in-house training and subject matter experts and by external training providers. We continued to review, evaluate and update programs as part of our focus on continuous improvement and alignment of training with ASIO's objectives. The consistently positive feedback from course participants and their line managers indicated that ASIO was effectively developing employees to perform the various roles which contribute to achieving our purpose.

Training initiatives

Training initiatives during the reporting period included improved identification of organisational resources, a new training continuum for technical staff, and significant improvements to existing training programs. The initiatives included the following:

- a new 'Train the ASIO Trainer' course, designed to provide expert practitioners with specific skills in building effective learning environments and materials;
- a moderation process added to the existing Surveillance Officer Training Program, which has improved both the performance management of candidates and the evaluation of their suitability for employment with ASIO;
- an in-depth training needs analysis for staff working in technical areas, which has resulted in a training and development continuum to meet core technical competencies, validate staff skills and help meet existing and anticipated future growth and demands; and
- an online training evaluation toolkit, designed to provide internal ASIO areas with the capability to independently measure in-house training program outcomes and identify areas for continued improvement. The toolkit was launched in April 2017, and internal ASIO areas can now self-manage the evaluation of their in-house programs, while strengthening their adherence to best-practice adult learning principles.

Intelligence training

ASIO's 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 the Organisation's intelligence collection operational capabilities. IOs perform both analytical and operational roles, while IAs 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 IAs.

Management and leadership development

Following the success of ASIO's award-winning[2] Management and Leadership in Security Intelligence Strategy (2013–16), ASIO's new Management and Leadership Strategy 2017–20 was launched in early 2017. The strategy supports the 70:20:10 model, with a diverse range of personal and professional development opportunities that—through experience, experimentation and reflection (70%), working with and through others (20%), and structured instructor-led programs, vocational education and training courses (10%)—will enable self-driven learning.

While the strategy has been substantially refreshed and updated, it continues to support and empower managers and future leaders by developing and enhancing their capability, knowledge and skills.

The development of a talent identification and management framework and advanced leadership program aims to identify and grow the capabilities of staff identified as the future leaders of our Organisation. It will also provide a broad and bespoke range of structured and targeted leadership development opportunities to support our leaders in managing organisational growth and change, while increasing capability and productivity to meet new and emerging challenges.

Study support and language skills

In 2016–17, the ASIO Study Support Program allocated $337 804 to 115 staff, attending over 70 programs, while the Language Skills in ASIO program allocated $291 661 to 34 employees (approximately 2 per cent of the workforce) for language capability development.

In addition to the Language Skills in ASIO program, various courses and seminars were designed and delivered by ASIO Language Capabilities for a broad ASIO and AIC audience.

National Intelligence Community training

ASIO continues to host the National Centre for Intelligence Training and Education (NCITE, formerly the National Intelligence Community Training Secretariat or NICTS) on behalf of the National Intelligence Community (NIC). 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.

SECURITY

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. We reviewed and updated our policies and procedures to reflect changes in broader government policy and our risk environment. We provided staff with security awareness training at their commencement with ASIO, requiring 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 supplemented the physical security arrangements for our headquarters building (the Ben Chifley Building) with armed officers from the Australian Federal Police (AFP).

Security policies and governance

In 2016–17, ASIO continued to foster a positive protective with 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 Security Committee

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

e-security

ASIO's information and communications technology (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 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.

Contact Reporting Scheme

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

Security clearances and vetting

ASIO's personnel security assessments are vital to securing the integrity of Australian Government business by providing advice to vetting agencies on the security implications of individuals being granted a security clearance.

- In 2016–17, ASIO completed 27 182 personnel security assessments.

ASIO continues to work closely with AGSVA to improve the efficiency of the security assessment process, while maintaining an appropriate level of assurance in relation to vetting candidates. A number of joint initiatives are planned or underway to increase efficiency, including automation of some elements.

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.

2 The Australian Human Resource Institute Rob Goffee Award for Leadership Development (2015)

OVERSIGHT AND ACCOUNTABILITY

Ministerial accountability

In 2016–17, ASIO's ministerial accountability was to the Attorney-General, Senator the Hon. George Brandis QC. We conducted our security intelligence activities in accordance with the Attorney-General's Guidelines, which are available from ASIO's website. The guidelines stipulate that our activities must be conducted in a lawful, timely and efficient manner, applying the principle of proportionality—that is, the methods used to investigate a person must be proportional to the threat posed—to ensure the least intrusion necessary into an individual's privacy. The guidelines are currently being reviewed by the Attorney-General's Department following a recommendation by the PJCIS. We contributed to the review during this reporting period.

We keep the Attorney-General informed of significant national security developments, as well as other important issues affecting ASIO. During the reporting period, we provided advice to the Attorney-General on a range of investigative, operational and administrative issues, primarily communicated through 288 formal submissions. The Director-General also briefed other ministers on security issues and matters relevant to their portfolios, when required.

Engagement with parliament

ASIO Annual Report 2016–17

ASIO's unclassified annual report for 2016–17 was tabled in parliament on 17 October 2017. A copy of the report is available from ASIO's website. The *ASIO annual report 2016–17* provides the following:

- a review of our work environment and performance in 2016–17 (Part 1);
- a description of ASIO's role and structure (Part 2);
- an overview of Australia's security environment and outlook (Part 3);
- a report on how ASIO performed against the performance measures and targets set out in our 2016–17 Corporate Plan (Part 4);
- a report on corporate management, oversight and accountability arrangements and external scrutiny of ASIO (Part 5); and
- our financial statements for 2016–17 (Part 6).

The annual report highlights key performance outcomes for ASIO during 2016–17, which are summarised in the 'Organisational performance' section of this report.

Leader of the Opposition and shadow ministers

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 him or her with a copy of ASIO's classified annual report. Throughout 2016–17, with the Attorney-General's knowledge, classified briefings on specific security matters were provided for shadow ministers.

Parliamentary Joint Committee on Intelligence and Security

In late 2016, ASIO provided evidence to the PJCIS to support its review of the re-listing of six terrorist organisations under the Criminal Code, as well as its review of the declaration of Islamic State as a declared terrorist organisation under the *Australian Citizenship Act 2007*. In early 2017, we appeared before the committee for its review of the listing and re-listing of four terrorist organisations under the Criminal Code and for the committee's review of the Telecommunications and Other Legislation Amendment Bill 2016, for which we provided a classified submission. We also appeared before the PJCIS in closed and public hearings for its Review of Administration and Expenditure No. 15 2015–16, providing a classified and an unclassified submission.

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

The PJCIS's recommendations from its inquiries are reported to each House of the parliament and to the responsible minister. Our unclassified evidence to the PJCIS can be found on the relevant inquiry page on the committee's website.

During the reporting period, ASIO provided the PJCIS with background briefings on topical issues. PJCIS members also received in-depth briefings on security issues during a tour of the Ben Chifley Building on 12 May 2017.

Senate Legal and Constitutional Affairs Committee

ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate Estimates process on 18 October 2016, 28 February 2017 and 25 May 2017. Our evidence to the committee can be found in the Estimates *Hansard* for those days; the transcript is available on the Australian Parliament website.

Other parliamentary engagement

ASIO provided a submission to the Standing Committee of Privileges during this reporting period.

Independent oversight

Inspector-General of Intelligence and Security

The Hon. Margaret Stone was appointed Inspector-General of Intelligence and Security (IGIS) in August 2015. The role of the IGIS is to review the activities of the Australian Intelligence Community and provide assurance that agencies operate with propriety, according to law, consistent with ministerial guidelines and directives, and with due regard for human rights. The IGIS has powers akin to those of a standing royal commission.

During 2016–17, the IGIS undertook a regular inspection program of activities across ASIO's operational functions and investigated complaints received by her office. There were no formal inquiries or release of any reports of inquiries making findings in relation to ASIO. Details of the ongoing inspection work of the IGIS can be found in her annual report, available online from www.igis.gov.au.

Independent National Security Legislation Monitor

The Independent National Security Legislation Monitor (INSLM), Dr James Renwick SC, was appointed on 13 February 2017. He replaced the Hon. Roger Gyles AO QC, who held the role from 20 August 2015 until 31 October 2016. The INSLM's role is to review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation, and report to the Prime Minister and the parliament, on an ongoing basis.

During 2016–17, ASIO made submissions to the INSLM in relation to the following inquiries:

- certain questioning and questioning-and-detention powers in relation to terrorism; and
- the 2017 statutory review concerning Division 3A of Part IAA of the *Crimes Act 1914* (stop, search and seize powers); subsections 119.2 and 119.3 of the *Criminal Code Act 1995* (declared areas); and Divisions 104 and 105 of the *Criminal Code Act 1995* (control orders and preventative detention orders), including the interoperability of the control order regime and the *Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016*.

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

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

Independent Reviewer of Adverse Security Assessments

The role of the Independent Reviewer of Adverse Security Assessments is to conduct an independent advisory review of ASIO adverse security assessments furnished to the Department of Immigration and Border Protection (DIBP) for persons who remain in immigration detention, having been found by the department to be owed protection obligations under international law and to be ineligible for a permanent protection visa, or who have had their permanent protection visa cancelled because they are the subject of an adverse security assessment. The Independent Reviewer conducts an initial primary review of each adverse security assessment, and subsequent periodic reviews every 12 months for the duration of the adverse assessment.

In performing their task, the Independent Reviewer has access to all materials relied on by ASIO to make its assessment and any information obtained by ASIO since the adverse security assessment was completed or provided to the Independent Reviewer by the applicant or his or her legal representatives. Particularly for periodic reviews, the Independent Reviewer closely considers the overall security environment and any changes to the applicant's circumstances or ideology during his or her time in detention.

The current Independent Reviewer of Adverse Security Assessments is Mr Robert Cornall AO. On 1 July 2016, four matters remained within the Independent Reviewer's jurisdiction and no new matters arose during the year. The four cases—two periodic reviews and two primary reviews—were all finalised during 2016–17.

- Each of the periodic reviews was deferred, with the agreement of the applicant's solicitors, until ASIO had completed an internal review. In each case, ASIO furnished DIBP with a qualified security assessment in relation to the applicant.
- In both primary reviews, the Independent Reviewer disagreed with ASIO's assessment. After considering ASIO's own internal review and the Independent Reviewer's report, the Director-General of Security decided to furnish a qualified security assessment for both applicants.

LEGISLATION AND LITIGATION

Legislative changes that have impacted on administration of the agency

Several changes to legislation affected ASIO during 2016–17.

Counter-Terrorism Legislation Amendment Act (No. 1) 2016

The *Counter-Terrorism Legislation Amendment Act (No. 1) 2016* received royal assent on 29 November 2016, with all provisions coming into effect on that date except those relating to special advocates, which will commence by proclamation or 12 months after royal assent, whichever is earlier. Key changes made by the Act include the following:

- a change to Section 40 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), enabling ASIO to furnish security assessments directly to states and territories;
- a change to section 35P of the ASIO Act, creating separate 'insider' and 'outsider' offences for the unauthorised disclosure of information relating to Special Intelligence Operations, and including a defence of prior publication;
- a change to the control order framework, including amendments to:
  - enable an issuing court to impose a control order on persons 14 years or older;
  - introduce the ability to withhold national security information from the subject of a control order proceeding and their legal representative and still have it considered by the court; and
  - introduce the use of special advocates when national security information is withheld, to review that information and represent the interests of the subject.

Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016

The *Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016* amends the *Criminal Code Act 1995* (Cth) to introduce provisions enabling additional periods of imprisonment for terrorist offenders who have served their sentences but would remain an unacceptable risk to the community if they were to be released. The amending Act received royal assent on 7 December 2016 and commenced operation during 2017, in accordance with an implementation plan developed by the Commonwealth Attorney-General and the states.

Implications of legislative changes

The legislative changes made in 2016–17 have not had significant implications for staffing in the Organisation. There has, however, been a substantial increase in the staffing effort across ASIO on the development of legislative reform that has not yet resulted in new legislation.

The legislative changes made in 2016–17 have not resulted in identified specific training requirements.

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

ASIO in-house lawyers, with their specific legal skill sets, continue to provide legal advice to the Organisation on legislative development and the application of new and existing legislation.

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

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

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'. 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 AGD before progressing to the Attorney-General. The Attorney-General considers the warrant request and, if in agreement, issues the warrant.

There is no legislative requirement for the AGD 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

Administrative Appeals Tribunal administrative reviews

ASIO was involved in one Administrative Appeals Tribunal review that did not include a security assessment. The application, which related to a Freedom of Information issue, was commenced and dismissed in the reporting period.

Administrative Appeals Tribunal security assessment reviews

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

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

Security assessment judicial reviews

Two security assessments were reviewed by the Federal Court of Australia in the reporting period.

Applicants challenged the legal reasonableness of the assessments and alleged denial of procedural fairness, and noncompliance with our security assessment policies. During the reporting period, the full Federal Court found that one applicant was not sufficiently afforded procedural fairness during their interview with ASIO.

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

Coronial inquests

New South Wales coronial inquest: inquest into the deaths arising from the Lindt Café siege

On 24 May 2017, the New South Wales (NSW) State Coroner concluded the inquest into the deaths of Tori Johnson, Katrina Dawson and Man Haron Monis at the Lindt Café in December 2014. ASIO cooperated with the inquest, and six of our employees gave evidence in closed court in December 2015 and September 2016. The coroner made the following conclusions:

- ASIO's 2008 investigation of Mr Monis was 'balanced, comprehensive and appropriate in the circumstances'.
- The subsequent assessments ASIO conducted relating to Mr Monis, and our consideration of him, were adequate and appropriate.
- ASIO's treatment and management of the National Security Hotline reports in the period of their first receipt and during the siege, including their triage, was adequate and appropriate.

The coroner also found that two significant aspects of our politically motivated violence risk assessment process (relating to leads triaging and the criteria used for assessing politically motivated violence) required recalibration and that there were several examples of information that we ought to have shared with the NSW Police Force. The coroner's recommendations relating to ASIO included the following:

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

ASIO accepted the coroner's conclusions and, as at 30 June 2017, significant progress had been made towards implementing the recommendations relating to ASIO.

Victorian coronial inquest: inquest into the death of Ahmed Numan Haider

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

Terrorism and other criminal prosecutions

During the reporting period, ASIO provided its law enforcement partners with evidence in 10 NSW and four Victorian counter-terrorism prosecutions. Evidence included intercepted telecommunications, physical surveillance, listening device and tracking device information.

The following persons were convicted of counter-terrorism offences during the period:

- On 27 July 2016, Omar Al-Kutobi and Mohammad Kiad pleaded guilty to conspiracy to undertake acts done in preparation for, or planning, terrorist acts. On 9 December 2016, the offenders were sentenced in the NSW Supreme Court to a term of 20 years imprisonment (non-parole period of 15 years).
- On 9 December 2016, a NSW District Court jury found Ali al-Talebi guilty of two counts of attempting to support/resource a terrorist organisation and one count of attempting to make funds available to a terrorist organisation. Mr al-Talebi was subsequently sentenced to 12 years imprisonment (non-parole period of nine years imprisonment).

RELATIONSHIP MANAGEMENT AND PUBLIC RECORDS

Government and business relations

ASIO continued to provide security intelligence advice to Australian businesses and government agencies and to foreign partners.

Business and Government Liaison Unit

The Business and Government Liaison Unit (BGLU) fulfils a central outreach function connecting ASIO with businesses and government agencies. Formerly known as the Business Liaison Unit, the name was changed during the reporting period to better reflect the full spectrum of engagement.

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 (covered by the 'For Official Use Only' handling instruction) relating to the domestic and international security environment. Hosted on the site are reports on terrorism, threats to critical infrastructure and crowded places, and espionage and foreign interference threats, as well as reference material for security managers.

During the reporting period, 64 reports were published on the BGLU website. These reports were drawn from the full range of ASIO's information holdings and expertise, including the multi-agency National Threat Assessment Centre (NTAC), ASIO's protective security area (ASIO-T4) and partner agencies.

The BGLU also coordinated nine classified briefing sessions on themes including security threats to aviation, crowded places, defence industries, energy and resources, mass passenger transport, communications, and banking and finance. The format of the briefing sessions was reviewed and refined in late 2016 to include external partner briefings and increased use of real-world case studies. BGLU also increased pre-briefing engagement with established stakeholders to ensure that requirements were understood and tailored presentations provided on high-priority issues.

During the reporting period, the BGLU also engaged with stakeholders through a range of broad government and industry forums, including the Australia – New Zealand Counter-Terrorism Committee Business Advisory Group, the Attorney-General's Department–led Trusted Information Sharing Network and the Critical Infrastructure Advisory Council. Engagement with other critical infrastructure sector-specific forums included the Office of Transport Security–led Aviation Security Advisory Forum, Regional Industry Consultative Meetings and the Maritime Industry Security Consultative Forum. This included delivering 76 briefings to federal, state and territory government agencies and industry partners on indicators of mobilisation to violence, to build a collective understanding of terrorist behaviour.

ASIO Protective Security Directorate (ASIO-T4)

ASIO-T4 provides expert protective security advice and technical surveillance countermeasures (TSCM) services to the Australian Government and other entities, including some companies and state and territory governments. 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.

In 2016–17, ASIO-T4's protective security advice and services remained in high demand, and a new intelligence-led prioritisation model was adopted to ensure advice and services supported the assets, infrastructure and systems most at risk from terrorism, espionage and foreign interference–related threats.

ASIO-T4 provided a range of advice and services during the reporting period, including 179 security product evaluations, 80 Zone 5 (Top Secret) facility inspections, four protective security training courses and a range of protective security publications, which were posted on the Australian Government's Govdex website and ASIO's BGLU website.

Annual Stakeholder Survey 2017

In 2016–17, ASIO commissioned interviews of 66 senior stakeholders in 64 federal, state and territory government and industry organisations and sought their feedback on the following:

- how effective they considered ASIO had been during 2016–17 in identifying and investigating threats to Australia's security; in providing advice, reporting and other services to support their organisation; and in partnering with their organisation;
- how ASIO's advice had shaped policy decisions or informed operational activities;
- what ASIO had done well during the year;
- the areas where ASIO could make improvements; and
- key priorities for their engagement with ASIO in the next 12 months.

The survey was conducted by a former deputy secretary of Defence, Mr Steve Meekin AM, in an independent capacity. The survey made the following conclusions:

- Without exception, ASIO is regarded as an effective, capable and reliable partner offering high-quality and largely unique services. Stakeholders see ASIO as a very credible organisation of well-trained and enthusiastic officers who are competent, capable and increasingly outward looking.
- ASIO's counter-terrorism effort is highly regarded, especially for the manner in which it has become more engaged, more open and less opaque to its counter-terrorism law enforcement partners. Similarly, there is high regard for its counter-espionage and counter-interference efforts.
- Close and effective engagement with key stakeholders is seen as being a high priority for ASIO. The ASIO brand is trusted, well regarded and respected by those interviewed. ASIO is an organisation that is seen to be heading in the right direction.
- However, success comes with challenges. A number of key stakeholders are seeking to build on success. They want closer and more enduring engagement. In some cases they are seeking a relationship that, if sustained, may stretch beyond current priorities for resourcing or beyond the edge of ASIO's mandate.
- ASIO's key stakeholders did not point to any significant performance shortfalls or underlying systemic problems. Where issues of concern were raised by key stakeholders, they were generally minor and largely related to exceptions which caused irritation. Many of these issues were reported to the relevant area of ASIO during the conduct of the survey, and remedial action was initiated promptly.
- A number of stakeholders sought to refine their relationship with ASIO. This was mainly from the perspective of transforming what was perceived as a good but in some cases limited or one-sided relationship into a far more effective one.

The next stakeholder survey will be conducted in 2018. We will also capture working-level feedback from stakeholders continuously throughout the year. This feedback will be reported to the ASIO Executive Board as part of our tri-annual performance reporting system (refer to 'Corporate governance', above).

ASIO's international relationships

Australia's interests stretch to every corner of the globe, as do our unique partnerships. For nearly seven decades, we have been working with cooperating intelligence and security services all over the world to protect Australians and their interests. We opened our first overseas liaison office in 1956, and today we have relationships with over 350 intelligence services in more than 130 countries.

ASIO is a trusted, professional partner for these intelligence services. These relationships provide us with access to unique lines of intelligence that help us protect Australians. They also allow us to share capabilities and training to ensure our skills remain world-class.

In a number of posts, ASIO is the sole representative of the Australian Intelligence Community. ASIO also hosts and manages a number of foreign service representatives in Australia and uses those relationships to complement engagement through 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, operational and capability development matters.

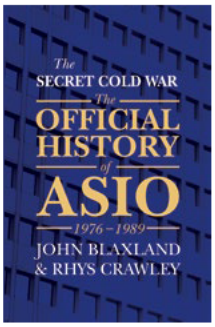
Public records

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 speak at select public seminars or conferences. ASIO's website has details on public speeches and statements made in 2016–17.

The media can contact ASIO directly through a publicly listed media contact number and email address. In 2016–17, ASIO continued to respond to media inquiries, without commenting on operations, investigations, individuals or operational capabilities.

Official History of ASIO



The third and final volume of ASIO's history, *The secret Cold War: the official history of ASIO 1975–1989*, authored by Dr Blaxland and Dr Rhys Crawley, was released in 2016–17. The book was launched by the Attorney-General at ASIO's headquarters and attended by former Directors-General of Security, as well as a small group of officers who joined ASIO at the Organisation's inception in 1949.

Public access to ASIO records

ASIO is an exempt agency under the *Freedom of Information Act 1982* but is subject to the release of records under the *Archives Act 1983* (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 in or before 1993. ASIO works closely with the National Archives in facilitating access to ASIO records while balancing various and sometimes competing priorities.

During the reporting period, 484 applications were made for access to records, and a total of 478 requests were completed.

The number of requests has remained steady after a peak in 2014–15. ASIO considers the increase in 2014–15 was due to publicity surrounding the release of the book *Dirty secrets*. The book, edited by Meredith Burgmann, contains the reflections of 26 well-known Australians who have read their ASIO files.

'Internal reconsideration' cases are where a previous decision regarding the redaction of a document is reviewed under section 42 of the Archives Act. In 2016–17, four 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. One application which commenced an AAT action on 23 December 2015 was dismissed on 2 September 2016.

Table 8: Access to ASIO records

	2014–15	2015–16	2016–17
Applications for record access	790	473	484
Requests completed	811	650	478