



Australian Government
Australian Security
Intelligence Organisation

ASIO Submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure

No.15 2015–2016



Contents

| | |
|--|----|
| Scope of the review..... | 1 |
| ASIO's role and functions..... | 2 |
| The security environment..... | 3 |
| Terrorism | 3 |
| Onshore terrorist attacks and disruptions | 3 |
| Global terrorist attacks | 6 |
| Communal violence and violent protest | 8 |
| Espionage, foreign interference and malicious insiders | 8 |
| Border integrity | 9 |
| Expenditure..... | 10 |
| Budget | 10 |
| Financial performance | 10 |
| Strategic allocation of resources | 11 |
| Financial management and internal controls | 12 |
| Structure of the Organisation..... | 13 |
| Organisational structure | 14 |
| Corporate direction and strategic planning..... | 15 |
| ASIO2020 | 15 |
| Corporate governance..... | 16 |
| ASIO Executive Board | 16 |
| Intelligence Coordination Committee | 16 |
| Workforce Capability Committee | 16 |
| ASIO Security Committee | 17 |
| Finance Committee | 17 |
| Audit and Risk Committee | 17 |
| Communication and leadership meetings | 17 |
| ASIO Consultative Council | 18 |
| Fraud control | 18 |

| | |
|--|----|
| Human resource management | 19 |
| Recruitment and workforce management | 19 |
| Diversity agenda | 20 |
| Workplace agreement | 20 |
| Performance Management Framework | 21 |
| Work health and safety | 22 |
| Workforce statistics | 22 |
| Separation rates | 25 |
| Redundancies | 26 |
| Attachments | 26 |
| Misconduct | 27 |
| Public Interest Disclosure Act | 27 |
| ASIO Ombudsman | 27 |
| Training and development | 28 |
| Intelligence training | 28 |
| Management and leadership development | 29 |
| Study support and language development programs | 29 |
| e-Learning | 29 |
| National Intelligence Community training | 30 |
| Legislation and litigation | 31 |
| Legislation amendment | 31 |
| Use of ASIO special powers | 32 |
| Litigation | 32 |
| Security of ASIO | 34 |
| Security governance and policy | 34 |
| Security clearances in ASIO | 34 |
| e-Security | 34 |
| Management of relationships and public reporting | 35 |
| Business Liaison Unit | 35 |
| Stakeholder satisfaction survey | 36 |
| Public statements and media | 36 |
| Official History of ASIO | 36 |
| Public access to ASIO records | 37 |
| ASIO's international relationships | 37 |
| Oversight and Accountability | 38 |
| Ministerial accountability | 38 |
| Independent oversight | 39 |

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. 15 provides a detailed account of ASIO's activities during the financial year 2015–16. The PJCIS wrote to ASIO requesting a submission covering all aspects of administration including:

- ▶ strategic direction and priorities;
- ▶ legislative changes that have an impact on the administration of the agency including, as appropriate, the frequency and nature of use of any new powers, staffing implications, training, the role of legal officers and need for specialist staff, and the relationships with outside agencies such as police or the judiciary;
- ▶ involvement (if any) in litigation matters, including any administrative reviews in the Administrative Appeals Tribunal (AAT);
- ▶ human resource management, including staffing numbers, recruitment and retention strategies, training and development, performance management, workplace diversity, language skills, staff complaints, separation rates and accommodation;
- ▶ changes (if any) to the structure of the Organisation, including the distribution of staff across different areas of the organisation, ratio of field and operational staff to administrative staff, ratio of executive to middle and lower level staff, and ratio of central office to outlying staff;

- ▶ security issues, including policies, training, security breaches and e-security;
- ▶ security clearances, including current procedures, timelines, delays and associated outsourcing arrangements;
- ▶ public relations and/or public reporting, including requests for public access to records; and
- ▶ performance management and accountability, including any outcomes relevant to administration and expenditure for the financial year.

In relation to expenditure, the Committee will again seek evidence as to ASIO's ability to meet its objectives within budget parameters as well as the impact of funding increases, any budget constraints, and ongoing implications of the efficiency dividend and other savings measures.

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 by providing advice to ministers, Australian government agencies, state authorities and other approved entities.

The *Australian Security Intelligence Organisation Act 1979* (ASIO Act) defines 'security' 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 also 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, including:

- ▶ 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 also 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.

ASIO works closely with a range of stakeholders, in responding to and investigating matters of national security, 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.

The security environment

Terrorism








Australia’s National Terrorism Threat Level is PROBABLE—credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to conduct terrorist attacks in Australia. The National Terrorism Threat Level was raised in September 2014¹. This was not a response to any one development but rather reflected a range of factors—driven by local and overseas events—that saw unprecedented fluidity in the domestic security environment. While these factors have evolved (and some have deteriorated), their cumulative impact remains significant, and so the National Terrorism Threat Level remains elevated.

During the year, one terrorist attack was conducted in Australia and three terrorist plots were disrupted.

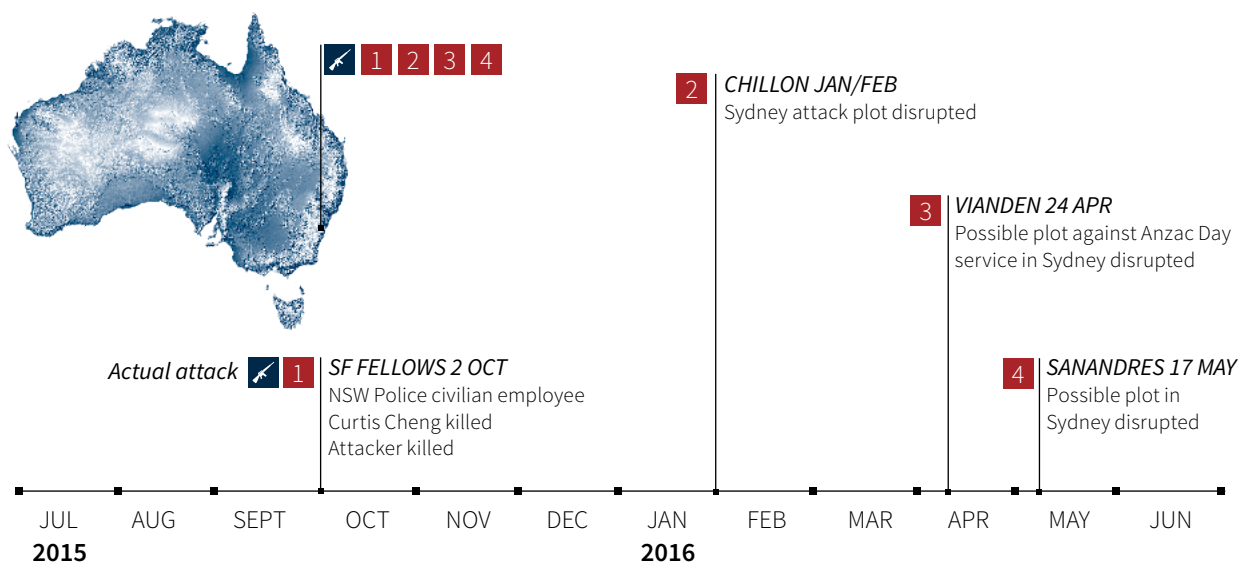
Onshore terrorist attacks and disruptions

The National Terrorism Threat Level is **PROBABLE**

Common factors

| | | | |
|---|---|---|----------------------------------|
|  | <i>Offshore influences</i> |  | <i>Onshore influences</i> |
|  | Direct communication with offshore extremists |  | Prevention of travel |
|  | Graphic and slick publications |  | Pressure from onshore extremists |
|  | targeted radicalisation | | |

- ▶ Providing justification, instruction, encouragement and direction for onshore attack
- ▶ Islamic State of Iraq and the Levant (ISIL) affiliation
- ▶ Rapid targeting
- ▶ Spontaneous and rudimentary attack methodology
- ▶ Targeting Australian Government and public



¹ In September 2014, the National Terrorism Threat Level was raised from MEDIUM to HIGH. Following implementation of the new National Threat Advisory System in November 2015—which is unclassified and published on www.nationalsecurity.gov.au—the National Terrorism Threat Level was allocated a level of PROBABLE in line with that system.

Australia

The principal terrorist threat in Australia emanates from the small number of Australia-based individuals who remain committed to anti-Western violent Sunni Islamist extremist ideology. This group presents a direct threat as well as a secondary threat due to their ability to influence others.

- ▶ Some have turned their attention to onshore attack-planning after the cancellation of their Australian passports—preventing them from travelling to join terrorist groups in the conflict zone in Syria and Iraq—while some are returnees from that conflict.
- ▶ There are around 40 returnees from the conflict in Syria and Iraq. ASIO assesses the vast majority of these are not of security concern, because their activities in Syria were not related to terrorist organisations and they returned before the declaration of the caliphate. However, in the longer term, the small number ASIO is concerned about will be joined by others returning from the conflict who have trained and fought with ISIL, and other groups of concern in the region. They will have been deeply indoctrinated into ISIL's ideology and inured to the use of extreme violence. It is possible they will undertake terrorist attacks themselves or enable others to do so. ASIO also holds concerns about their connections to networks of extremists who could be a source of information and guidance.
- ▶ Recruitment and radicalisation by Australia-based extremists is a key risk. Terrorist groups, particularly ISIL, are adept at broadly promoting their violent extremist message online by producing a plethora of high production quality, high-impact propaganda; this material resonates with some people in Australia.

The changing nature of terrorism provides challenges to the early identification and detection of threats. Large-scale attacks are still occurring around the world, including attacks coordinated by multiple individuals, but there has been a trend towards simpler attacks. Such attacks can require minimal preparation and be perpetrated by lone actors.

A lone actor is an individual (or small group of like-minded individuals) who conducts, or plans to conduct, a disruptive and typically violent activity for political or religious motives. At the time the action is performed they act independently of real-world accomplices. A range of Islamist extremist groups, most notably and recently ISIL, actively encourage terrorist attacks against 'far enemies'. This type of threat can develop quickly, typically requires little preparation or planning, and can come from individuals who are on the periphery of investigations or who are unknown to authorities. Many of the recent terrorist attacks and

disrupted plots in Australia involved individuals or small groups who were radicalised, often through isolated online activity, to the point where they were willing to act out their grievances through the use of violence. The four onshore attacks since 2014 were all conducted by single individuals using relatively simple weapons (two with knives and two with firearms). While symbols of government and authority—including military, police and security agencies—remain attractive targets, indiscriminate attacks against the public align with the objectives of terrorists. ISIL, and to a lesser degree al-Qa'ida, continues to endorse and celebrate indiscriminate attacks against innocent citizens so as to reinforce their message and incite fear.

- ▶ One aspect of this threat is ISIL's effective campaign of identifying individuals who are susceptible to peer-to-peer radicalisation, enabled by secure communications. Vulnerable individuals are typically young disenfranchised and marginalised males who are ill-equipped to consider the consequences of their actions.
- ▶ Recent onshore terrorist plots have centred on would-be attackers who were groomed and assisted by overseas extremists. While the number of individuals who fall into this category is small, attacks such as those in Nice, France, and Orlando, United States demonstrate the devastating impact a single attacker can have.

International

The international security environment is deteriorating due mainly to the influence of resurgent Islamist terrorist groups. The predominant threat emanates from two highly capable and well-financed terrorist groups: ISIL and al-Qa'ida. Both have an international following and global reach, and both leverage this to promote an anti-Western, violent Sunni Islamist extremist ideology. They conduct attacks against Western interests, religious minorities and secular interests, and also exhort adherents to take unilateral action. Regional threats come from a range of entities affiliated with, and inspired by, these two groups. These include the South-East Asia-based Abu Sayyaf Group (ASG), Africa-based Boko Haram, al-Shabaab and al-Qa'ida in the Islamic Mahgreb (al-Qa'ida-IM), and the Asia-based Taliban.

The conflict in Syria and Iraq is central to the global resurgence of Islamist extremist terrorism. The conflict presents overlapping security issues:

- ▶ the increase in ungoverned spaces and spaces controlled by extremists (such as northern Syria, northern Iraq, Yemen and Libya) that allows extremists to more easily recruit globally, train locally, and plot external attacks in Europe, South-East Asia, Africa, other Middle Eastern countries and elsewhere throughout the globe;
- ▶ the threat from returning foreign fighters. Many are battle-hardened, inured to the use of violence and have been further radicalised with a strengthened commitment to Islamist extremism. These individuals have credibility and influence which can be used to radicalise others; and
- ▶ the threat from those who have not travelled, or have been prevented from travelling, and remain in their home countries. With the opportunity to travel removed, some may turn their attention to onshore attacks, including low-capability attacks that require little skill to conduct effectively. Recent attacks and disruptions in Australia, Europe, the United States, Malaysia, Indonesia and Bangladesh underscore this threat.

In South Asia, ISIL is increasing its influence. This is concerning in light of the broad ISIL message encouraging attacks against Westerners as well as secular and religious minorities. The al-Qa'ida threat in South Asia has not diminished either; the al-Qa'ida affiliate, al-Qa'ida in the Indian Subcontinent (al-Qa'ida IS), has increased its presence and undertaken attacks in Pakistan and Bangladesh. Additionally, al-Qa'ida-aligned groups such as Lashkar-e-Tayyiba continue to plot and conduct attacks. The security environment in Afghanistan will continue to deteriorate as the Taliban, al-Qa'ida and the Islamic State Khorasan Province continue to challenge the capability of Afghan security forces.

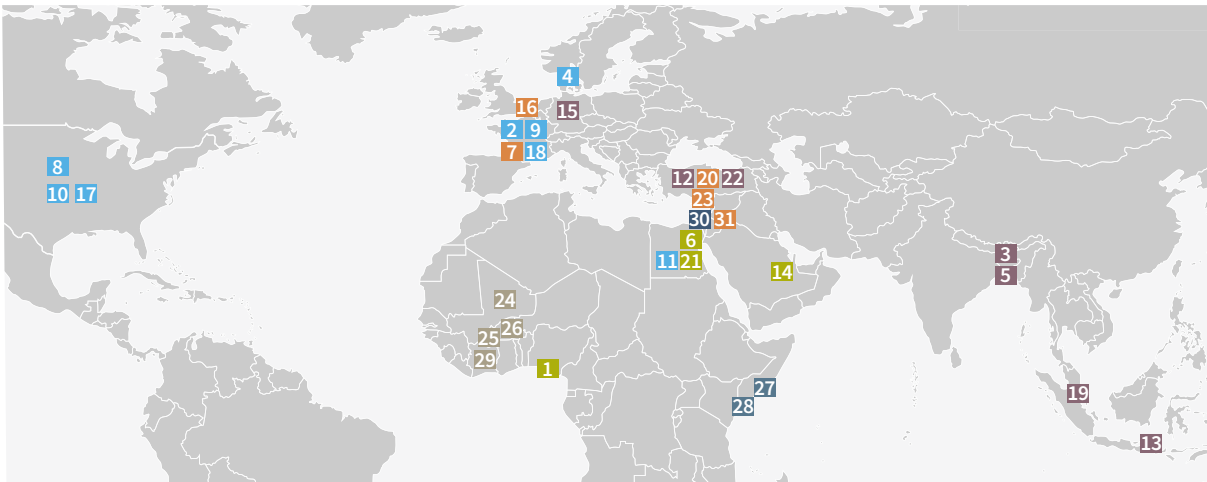
In Africa, ISIL and al-Qa'ida-aligned groups continue to flourish, evidenced by the number of newly declared ISIL provinces: ISIL-Sinai, ISIL-Libya, ISIL-Algeria and ISIL-West Africa (Boko Haram). This expansion threatens regions previously regarded as safe and poses an increasing threat to foreign interests.

In South-East Asia, the influence of ISIL is growing in a number of countries. In 2016, Indonesia and Malaysia suffered their first terrorist attacks conducted by ISIL-aligned extremists linked to South-East Asian foreign fighters based in Syria and Iraq. Hundreds of individuals from South-East Asia have travelled to Syria and Iraq to fight in the conflicts, including with ISIL. Some of these foreign fighters direct, advocate or encourage attacks, including against Australian interests, and this will motivate some individuals to act. Returnees from the conflict in Syria and Iraq may also increase the likelihood of a terrorist attack. A further troubling development is the declared allegiance of some Philippines groups to ISIL. ASIO is concerned that areas in the southern Philippines could develop into safe-havens for regional extremists and returning foreign fighters, who could plan attacks against Western interests throughout the region. The terrorist threat against Australians and Australian interests in the region is unlikely to abate in the near future.

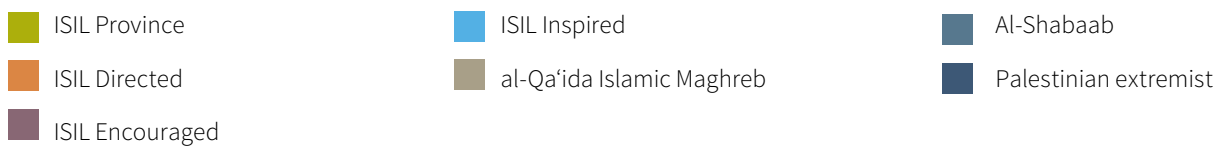
In Europe, the security environment worsened, as demonstrated by attacks in Paris in November 2015, in Brussels in April 2016, and more recently in Nice and Rouen in July 2016. Significant improvement in the foreseeable future is unlikely. Heightened security and counter-terrorism operations in the wake of devastating attacks in many countries likely delayed further terrorist attack plans, but the heightened effort is increasingly unsustainable and may only lead to temporary mitigation.

In Turkey, domestic tensions and proximity to the Syrian conflict negatively impacted on the security environment. There are now at least four active terrorist groups with the intent and capability to conduct large-scale attacks, and some have a stated or proven willingness to target tourists.

Global terrorist attacks



Attack provenance



Key

Dead Wounded

Weapons





























































- Basic weapon (edged)
- Basic weapon (vehicle)
- Explosive
- Firearm

Tactics

- Armed attacker
- Stabbing
- Explosion
- Hostage
- Suicide bombing
- Aviation bombing

Targets

- Public
- Government (military)
- Government (police)
- Australian aid workers
- Commercial

| | | | |
|--|---|--|--|
| <p>Nigeria 16.7.15 1</p> <p>Gombe market bombing, Damaturu prayer ground bombing.</p> <p>  X65 \ 0</p> | <p>France 7.1.16 9</p> <p>Lone actor attack on a Paris police station.</p> <p>  X0 \ 0</p> | <p>United States 12.6.16 17</p> <p>Mass shooting in Orlando, Florida by a lone gunman.</p> <p>  X49 \ 53</p> | <p>Burkina Faso 14.01.16 25</p> <p>Two Australians kidnapped.</p> <p>  X0 \ 2</p> |
| <p>France 21.8.15 2</p> <p>Terrorist attack on Paris-bound train — three injured.</p> <p>  X0 \ 3</p> | <p>United States 7.1.16 10</p> <p>Shooting attack on Philadelphia police officer.</p> <p>  X0 \ 1</p> | <p>France 13.6.16 18</p> <p>Attack on two police officers.</p> <p> X2 \ 0</p> | <p>Burkina Faso 15.01.16 26</p> <p>Hotel Cappuccino attack.</p> <p>  X30 \ 0</p> |
| <p>Bangladesh 28.9.15 3</p> <p>Multiple attackers shot and killed an Italian citizen.</p> <p>  X1 \ 0</p> | <p>Egypt 8.1.16 11</p> <p>Stabbing attack against European tourists — three people injured.</p> <p>  X0 \ 3</p> | <p>Malaysia 28.6.16 19</p> <p>Grenade attack on a bar in Puchong.</p> <p>  X0 \ 8</p> | <p>Somalia 2.2.16 27</p> <p>Daallo Airlines bombing.</p> <p>  X0 \ 0</p> |
| <p>Denmark 29.9.15 4</p> <p>A rejected Palestinian refugee stabbed a police officer at an asylum centre.</p> <p>  X0 \ 1</p> | <p>Turkey 12.1.16 12</p> <p>Likely ISIL suicide bomber kills 10 people, all foreigners, injuring 15.</p> <p>  X10 \ 15</p> | <p>Turkey 28.6.16 20</p> <p>Armed attack at Istanbul's Ataturk Airport.</p> <p>  X44 \ 236</p> | <p>Somalia 7.2.16 28</p> <p>Beledweyne Airport attack.</p> <p>  X6 \ 0</p> |
| <p>Bangladesh 3.10.15 5</p> <p>Multiple attackers shot and killed a Japanese citizen near Rangpur.</p> <p>  X1 \ 0</p> | <p>Indonesia 14.1.16 13</p> <p>Attack in central Jakarta targeting a Starbucks café and a police post.</p> <p>  X4 \ 23</p> | <p>Egypt 22.7.15 21</p> <p>ISIL beheaded a Croatian citizen.</p> <p> X1 \ 0</p> | <p>Cote d'Ivoire 13.3.16 29</p> <p>Grand Bassam attack.</p> <p>  X18 \ 33</p> |
| <p>Sinai, Egypt 31.10.15 6</p> <p>Explosion on board Russian Metrojet Flight 9268 killing 224 people.</p> <p>  X224 \ 0</p> | <p>Saudi Arabia 29.1.16 14</p> <p>Twin suicide attack on the Imam Rida mosque.</p> <p>  X4 \ 18</p> | <p>Turkey 10.10.15 22</p> <p>Twin suicide bombings in Ankara.</p> <p>  X102 \ 508</p> | <p>Israel 18.4.16 30</p> <p>Improvised explosive device attack on a bus in Jerusalem.</p> <p>  X0 \ 23</p> |
| <p>France 13.11.15 7</p> <p>Series of coordinated attacks in Paris, killing 130.</p> <p>  X130 \ 368</p> | <p>Germany 26.2.16 15</p> <p>A teenager stabbed a police officer at Hannover's main train station.</p> <p>  X0 \ 1</p> | <p>Lebanon 12.11.15 23</p> <p>Two ISIL suicide bombers attack Shia neighbourhood of Beirut.</p> <p>  X46 \ 240</p> | <p>Jordan 21.6.16 31</p> <p>Vehicle borne improvised explosive device attack against Jordanian Armed Forces at the Syrian border.</p> <p>  X7 \ 13</p> |
| <p>United States 2.12.15 8</p> <p>Shooting attack in San Bernardino, United States.</p> <p>  X14 \ 22</p> | <p>Belgium 22.3.16 16</p> <p>Coordinated bombings in Brussels.</p> <p>  X32 \ 340</p> | <p>Mali 20.11.15 24</p> <p>Radisson Blu hotel attack.</p> <p>  X22 \ 0</p> | |

Communal violence and violent protest

ASIO only investigates protest activity when it includes—or has the potential to include—premeditated violence, where it has the potential to impinge on the security of designated people and places, or where it suspects there is a link between the protest and conduct otherwise coming within the definition of security under the ASIO Act.

While Sunni Islamist extremism is the pre-eminent terrorist threat facing Australia, other groups continue to engage in politically motivated violence and the promotion of communal violence. Members of these groups are diverse and have differing agendas, including extreme right-wing and extreme left-wing ideologies. A few small subsets of these groups are willing to use violence to further their own interests. While their activities are concerning, they remain a small part of their broader movements and their activities are presently unlikely to lead to wide-scale violence or pose a threat to social cohesion.

Violence at protests in Australia is rare, and the vast majority of protest attendees are peaceful and support our democratic ideals. Social discourse around anti-Islam and anti-migration issues has increased, and public protests for and against have become more frequent; these provide an opportunity for ideological adversaries to converge and sporadic violence can result. Over the past 12 months, violence at protests has mostly comprised small-scale clashes between right-wing and left-wing opponents at anti-Islam protests or protesters targeting police maintaining public order.

Other groups with overseas separatist agendas are represented in Australia, but their membership is small and their influence is limited. Activities in support of overseas issues are mostly confined to fundraising and ideological support.

Espionage, foreign interference and malicious insiders

The harm caused by hostile intelligence activity can undermine Australia's national security and sovereignty. It can damage our international reputation and degrade our diplomatic and trade relations. Both espionage and foreign interference can inflict economic damage, degrade or compromise nationally vital assets and critical infrastructure, and threaten the safety of Australian nationals. Espionage and foreign interference targeting Australian interests remains pervasive and enduring. One of the most insidious features of both espionage and foreign interference is that the consequences of even a small level of activity can be severe, but can take years to be realised.

ASIO has observed increased targeting of Australian interests in Australia and abroad through a variety of methods against an array of sectors. Australia is a target of hostile foreign intelligence services as a result of:

- ▶ our alliance with the United States and the defence relationship we share;
- ▶ a desire to gain insights into our positions on international diplomatic, economic and military issues;
- ▶ our energy and mineral resources;
- ▶ our innovations in science and technology;
- ▶ a desire to shape the actions of decision-makers and public opinion; and
- ▶ the reach of online technologies enabling hostile cyber activities.

A range of countries continue to conduct espionage against Australia's vital national interests, including our defence capabilities and economic intent. Economic espionage is driven by Australia's role as a global commodity supplier, potential joint venture partner, market competitor, and our advances in scientific research. Inappropriate and untoward foreign interference in Australia aims to shape the actions of decision-makers and public opinion in order to achieve an outcome favourable to foreign interests. Cyber espionage can have a significant impact on Australia's national security, economic prosperity, sovereignty and international reputation. Foreign state-sponsored adversaries are targeting the networks of the Australian Government, industry and individuals to achieve intelligence requirements relating to economic advantage, foreign policy, defence and security information, science and technology. The range, scale and sophistication of state actors engaged in hostile cyber espionage activity against Australian Government and private sector systems continues to increase, as does the threat from malicious insiders. An increasing number of countries are pursuing a cyber espionage program as this offers returns for relatively low cost and plausible deniability. The continued evolution of technology increases the sophistication and complexity of attacks, while rendering the capability increasingly accessible.

Understanding and degrading the espionage and foreign interference activities of Australia's adversaries is among the most challenging types of intelligence work. Undetected espionage activity can have long-term implications, undermining our society and way of life. ASIO works with all government agencies and the private sector to increase awareness of the threat and to implement effective mitigation strategies. ASIO actively works across government to prevent 'malicious insiders'. These are potential, current or former government employees who have privileged access to information, techniques, technology, assets or premises who deliberately compromise their privileged position breach their duty to maintain the appropriate security conferred upon them by the nature of this access. This potential harm has been aggravated by technologies allowing the aggregation and transfer of large amounts of information. Malicious insiders can undertake a range of damaging activities, including:

- ▶ influencing decision-making processes;
- ▶ sabotaging computer systems or equipment;
- ▶ using inside information to facilitate an attack;
- ▶ mounting a physical attack from the inside; or
- ▶ releasing information with the intent to harm Australia's national security and stability.

Malicious insiders are divided into two broad categories based on their intent and motivation:

- ▶ self-motivated malicious insiders— individuals whose actions are undertaken of their own volition and not initiated as the result of any connection to, or direction by, a third party; and
- ▶ recruited malicious insiders—individuals co-opted by third parties, such as a foreign intelligence service, to exploit their potential, current or former privileged access.

Border integrity

The people-smuggling environment remained similar to that of the past two reporting periods, with significant reduction in planned and actual illegal maritime ventures to Australia. However, people smugglers motivated by financial gain sustained their attempts to recruit potential illegal immigrants actively by marketing misinformation about Australia's border policy, political situation and other events as indicators that Australia's border policy would be relaxed. ASIO continued to work with other Australian Government agencies to counter people smuggling through participation in Operation Sovereign Borders.

Expenditure

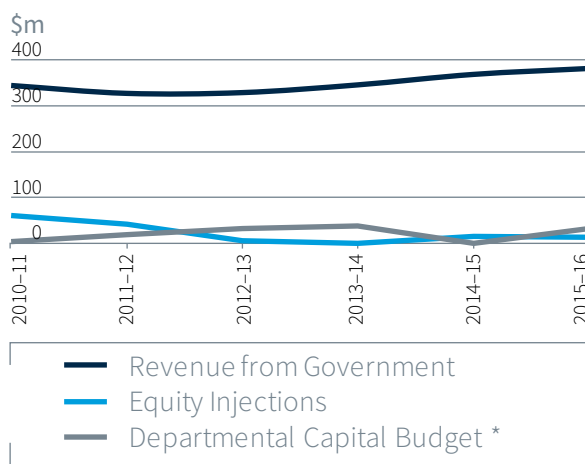
Budget

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 2015–16, ASIO received an appropriation of \$381 million. The 2015–16 financial year was the second year of the 'Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat' measure announced in August 2014, with funding received through the 2014–15 additional estimates process in February 2015. ASIO received \$31.2 million in operating funding and an equity injection of \$13.8 million for capital activities during 2015–16. ASIO anticipates receiving \$97.3 million in operating funding and \$27.6 million in capital funding for this measure over the next two financial years. ASIO was appropriated \$0.8 million under the 'Syrian and Iraqi Humanitarian Crisis' measure through the 2015–16 portfolio additional estimates process, and will receive a further \$0.6 million for this measure in 2016–17.

During 2015–16, ASIO returned around \$55.6 million to the government through the efficiency dividend and other savings measures (\$33 million in efficiency dividend and \$22.6 million in other savings measures or absorbed costs).

Figure 1: Revenue from government



Financial performance

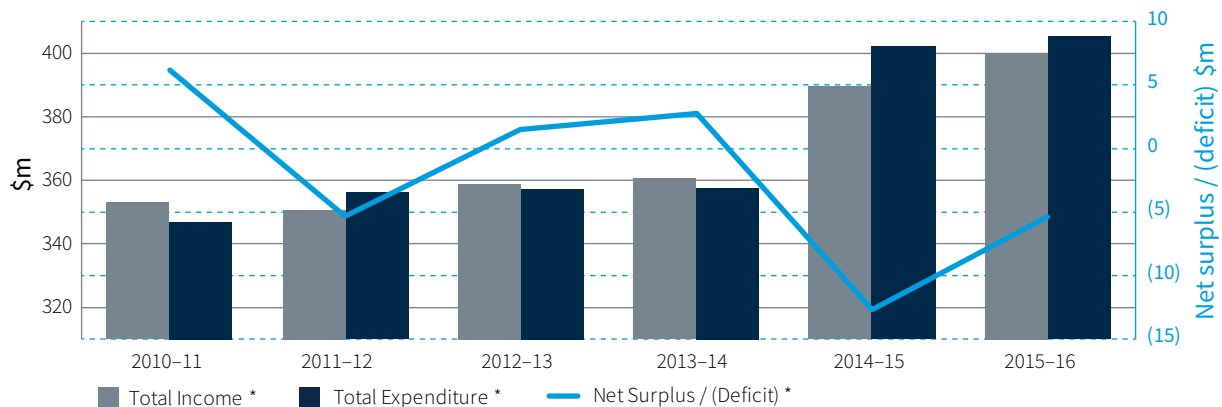
ASIO's financial position continued to be under pressure through the year due to the nature and number of investigations, the heightened security environment, and escalating business costs—including those associated with infrastructure, technologies and staff safety.

ASIO actively managed its expenditure; where possible, business practices were streamlined and selected activities re-prioritised to release funds for emerging priorities. Despite this, ASIO's financial result was an operating loss of \$5.4 million, excluding depreciation.

The Minister for Finance approved a \$2.8 million operating loss due to the accounting treatment required by Australian Accounting Standards Board Standard 'Employee benefits' (AASB119). External factors impacting on employee leave provisions moved disproportionately in the latter part of the year, resulting in a variance of \$4.4 million (as opposed to the approved figure of \$2.8 million).

ASIO's Departmental Capital Budget was \$32.1 million in 2015-16. Asset replacement funding was re-phased in previous financial years to align with the Organisation's updated replacement schedule. Capital acquisitions during the year reflected this program.

Figure 2: Financial performance



Strategic allocation of resources

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 predominately operationally related (81 per cent). ASIO resources are deployed across hundreds of investigations and thousands of leads. ASIO collects intelligence through human intelligence, warranted activities, surveillance, and requests for protected data. ASIO delivers hundreds of thousands of security assessments and communicate thousands of intelligence products and pieces of advice to enable action to be taken by our government, industry and international partners.

Figure 4: Purchase of Capital items

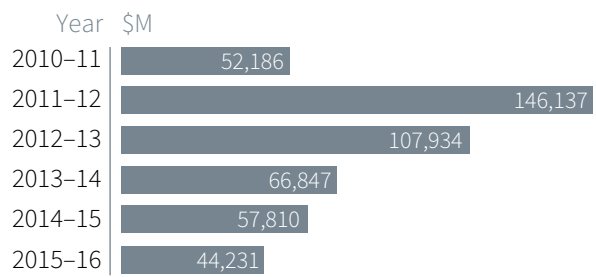
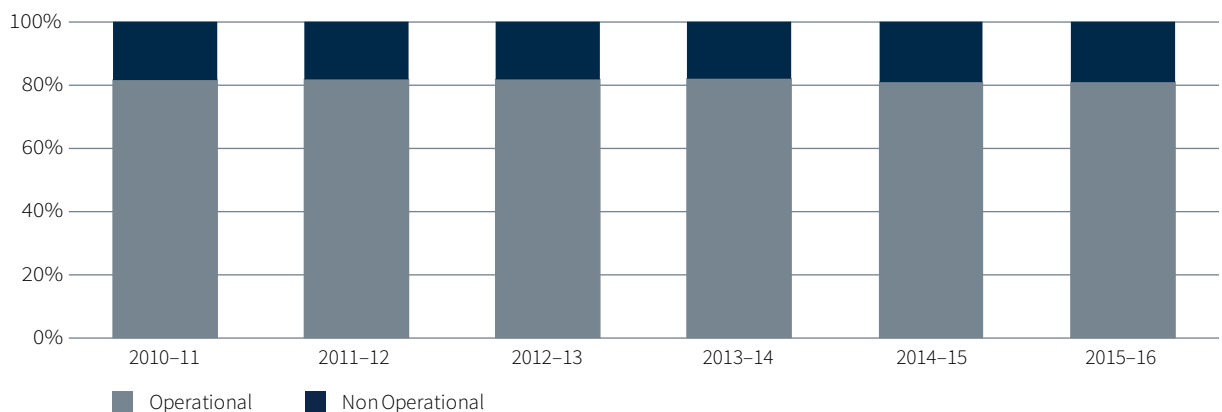


Figure 3: Resource allocation



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 2015–16, 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 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 Financial Officer also provides quarterly briefings to ASIO's Audit and Risk Committee to support the Committee's role of providing independent assurance about ASIO's internal governance, risk and control framework.

In addition to audits conducted by the ANAO and internal system controls, ASIO's internal audit function also undertakes financial audits.

Structure of the Organisation

In February 2015, a comprehensive review of ASIO's structure, resourcing and future posture was completed. A number of structural changes arising from that review were implemented on 3 August 2015. As a result, ASIO has moved from a two Deputy Director-General (DDG) to a three DDG structure, with the establishment of a Deputy Director-General Strategy. The positions of State Managers in Victoria and New South Wales were also elevated to First Assistant Director-General (FADG) level. An Executive Division FADG position was established, reporting to the new DDG Strategy.

In 2015–16, there were three groups in the Organisational structure:

- ▶ strategy;
- ▶ counter-espionage and interference, and capabilities; and
- ▶ counter-terrorism.

This functional arrangement allows for strengthened governance in relation to our high-risk CT and CE programs as well as an enhanced focus of the Organisation's strategy and corporate management:

- ▶ countering terrorism and the promotion of communal violence; and
- ▶ countering espionage, foreign interference and malicious insiders.



Duncan Lewis

DIRECTOR-GENERAL OF SECURITY

Organisational structure
as at 30 June 2016

| Deputy Director-General STRATEGY GROUP | Deputy Director-General CEI & CAPABILITIES GROUP | Deputy Director-General CT GROUP |
|--|--|---|
| <p>First Assistant Director-General</p> <p>State Manager NSW North Executive</p> <p>State Manager VIC South</p> <p>Corporate & Security</p> <p>Office of Legal Counsel</p> <p>Assistant Director-General</p> <p>Office of the Senior Executive</p> <p>Internal Security</p> <p>Security Assessments, Employment & Commercial Law</p> <p>Strategic Partnerships & Production</p> <p>Financial Management</p> <p>Legislation, Warrants & Technical Capabilities</p> <p>ASIO2020</p> <p>Litigation</p> <p>Human Resources</p> <p>Operations & Capability Protection</p> <p>State Manager QLD</p> <p>State Manager SA</p> <p>State Manager WA</p> <p>State Manager TAS</p> <p>Territory Manager NT</p> <p>Territory Manager ACT</p> | <p>Technical Capabilities</p> <p>Operational Capabilities & Training</p> <p>Information</p> <p>Counter- Espionage & Interference</p> <p>IT Infrastructure Services</p> <p>Physical Surveillance</p> <p>Business Information Systems</p> <p>Operations Services</p> <p>Training</p> <p>Computer Operations</p> <p>Close Access Operations</p> <p>Strategy & Performance</p> | <p>Counter- Terrorism</p> <p>Security Advice & Assessments</p> <p>Australian Counter- Terrorism Centre</p> <p>Counter- Terrorism Coordination</p> <p>National Threat Assessment Centre</p> <p>Australian Counter- Terrorism Centre</p> <p>Counter- Terrorism Investigations 1</p> <p>Border Investigations & Assessments</p> <p>Counter- Terrorism Investigations 2</p> <p>Intelligence Discovery, Investigations & Assessments</p> |

Corporate direction and strategic planning

ASIO released its first corporate plan under the PGPA Act in July 2015. The plan relates ASIO's purpose to its activities, delivery strategy, intended results, and new performance measures. ASIO continued to refine its corporate planning approach during the reporting period.

ASIO has strategic plans for its activities in countering terrorism, espionage, foreign interference and malicious insiders.

ASIO2020

In July 2016, the Director-General launched the ASIO2020 program which will address the most significant challenges to the Organisation's future success. It will identify ways to proactively respond to the major pressures on ASIO's business over the coming years. It will ensure that ASIO remains focused on work that provides clear value for the Australian Government and that it has the right culture, people and systems to effectively and efficiently achieve its purpose. ASIO2020 has four strands of work that set ASIO's strategic capability agenda and goals for the next four years:

Context – *ASIO's authorising and task environments*

A compelling value proposition will ensure ASIO maximises its contribution to society and therefore enjoys continued public support, authority and resources. ASIO needs to have its value understood by society, government, and partners. ASIO also needs to focus on what the Organisation can best offer to partners so it is recognised as their national security partner of choice.

Culture – *the backbone to ASIO's success*

A positive work culture will drive ASIO's productivity and contribute to the Organisation being an employer of choice. ASIO needs to enable a culture of innovation and diversity and unlock the benefits for its work. ASIO also needs to promote a single Organisational vision while recognising the validity of different business models.

People – *ASIO's most important asset*

ASIO's workforce is its core asset in a competitive labour market. In order to succeed, the Organisation must obtain maximum benefit from our people within a frame of mutual obligation. Strong and flexible human resources management approaches consistently applied will lift ASIO's value proposition for attracting, recruiting, and retaining the people it needs.

Systems – *How ASIO works (practices, tools, and mindsets)*

Work systems and mindsets that are fit for purpose, can adapt to change, and support a data discovery approach will enable ASIO to learn, and manage tomorrow's security challenges. ASIO needs to address the data discovery challenge to reduce the Organisation's information liability, obtain more breathing space from adversaries, and work with partners to share risk and opportunities.

An agile development approach, driven by a new team responsible for the ASIO2020 project, is being taken to deliver the projects within each strand in consultation with ASIO's workforce.

Corporate governance

The Director-General of Security is the accountable authority for ASIO under the PGPA Act. ASIO's corporate governance committees support the Director-General in fulfilling his PGPA Act responsibilities.

ASIO Executive Board

The Executive Board is the peak advisory committee to the Director-General. The Executive Board comprises the Director-General, the Deputy Directors-General and an external member. The Executive Board meets monthly, and sets ASIO's overall strategic direction and oversees resource management. Over the reporting period,

the board received regular reporting from ASIO's committees on corporate outcomes and issues including, key security developments, budget, capability development, risk management and importantly ASIO's progress toward its diversity goals.

Intelligence Coordination Committee

The Intelligence Coordination Committee plays a key role in fulfilling ASIO's responsibilities in accordance with the PGPA Act, through the management of ASIO's security intelligence program.

The Committee provides strategic direction, manages risk, coordinates effort and evaluates performance. During the period, Deputy Director-General Counter-Terrorism chaired the Committee.

The Committee's work program comprised three of the activities ASIO pursues to achieve its purpose and a fourth element focused on ASIO's specialised intelligence capability requirements:

- ▶ countering terrorism and the promotion of communal violence;
- ▶ countering espionage, foreign interference and malicious insiders;

- ▶ countering serious threats to Australia's border integrity; and
- ▶ enhancing security intelligence capabilities.

Over the reporting period, the Committee increased its guidance and oversight of ASIO's Investment Program to better align the Organisation's development of new and enhanced intelligence capabilities with acute and enduring strategic and operational risks. The Committee also established a new security intelligence capabilities sub-program to ensure the organisation's operating paradigm and Information and Communications Technology (ICT) systems keep pace with the evolving threat and technological environment.

Workforce Capability Committee

The Workforce Capability Committee considers issues concerning ASIO's workforce to ensure it is sufficiently sized, skilled, equipped and accommodated to meet the current and future capability needs of the Organisation — including work health and safety (WHS) matters through a WHS subcommittee. During the period, Deputy Director-General Strategy chaired the Workforce Capability Committee.

During 2015–16, the Committee oversaw the initiation of the 10th Workplace Agreement, the ASIO Gender Equity Strategy, the progress of recruitment to build ASIO's counter-terrorism capacity and a range of broader workforce issues.

ASIO Security Committee

The Security Committee reports directly to the Executive Board, providing assurance of ASIO's security practices. It considers the evolving security environment, and reviews and addresses key issues relevant to the security of people, property, operational activities and information

technology. It also approves security policy and procedures and reviews ASIO's compliance in meeting legislative and policy responsibilities specific to Australian government mandatory standards. During the period, Deputy Director-General Strategy chaired the Committee.

Finance Committee

The Finance Committee provides advice and makes recommendations to the Executive Board on resource allocation and financial management and strategy. Resources include human capital, accommodation and

assets. During the period, Deputy Director-General Counter Espionage and Interference and Capabilities chaired the Committee.

Audit and Risk Committee

The role of the ASIO Audit and Risk Committee is to provide independent assurance and advice to the Director-General and the Executive Board on the design, operation and performance of ASIO's internal governance, risk and control framework and compliance with its internal and external accountabilities and responsibilities. The Committee is responsible for reviewing and advising on:

- ▶ risk management;
- ▶ internal audit and assurance;
- ▶ external audit and review;
- ▶ internal control;
- ▶ financial statements;
- ▶ legislative and policy compliance; and
- ▶ performance reporting.

Committee members, including the chair, are appointed for an initial period of no more than three years. Over the reporting period, three ASIO officers and five external members served as committee members. The Committee currently comprises three ASIO officers and three external members. Mr Geoff Knuckey, an external member, chairs the Committee.

Over the reporting period, the Committee met its responsibilities under its charter and assessed ASIO's 2014–15 financial performance as sound. Key activities included: overseeing the implementation of the Integrated Assurance Model; establishing an Assurance Group, bringing together several internal assurance, performance and accountability capabilities; and commissioning a refreshed Fraud Risk Assessment, whose findings informed the development of the ASIO Fraud Control Framework 2016–18.

Compliance and performance audits found ASIO to be compliant with all requirements under relevant legislation, policies and external agreements.

Communication and leadership meetings

ASIO's communication and leadership meetings focus on communicating current and emerging key strategic or emerging, corporate and operational issues as well as review significant outcomes. Key messages are then communicated to staff via Branch and Directorate meetings. The Senior Executive Meeting is a weekly

meeting of all officers at ASIO Senior Executive Service Level 2 and above. The Senior Executive Service Meeting is a monthly meeting of all officers at SES Level 1 and above.

ASIO Consultative Council

The ASIO Consultative Council, chaired by ASIO's First Assistant Director-General Corporate and Security, enables ASIO management and employees to meet in a regular and structured way to discuss and resolve issues. Two representatives from ASIO's Staff Association and two representatives from ASIO's management group constitute a quorum for the monthly meeting.

This year the council focused on:

- ▶ progress of the 10th Workplace Agreement negotiation process, and the consequent amendments to ASIO's Consolidated Determination, human resource delegations, and policies;

- ▶ clarifying the terms and conditions of the Surveillance job family; and
- ▶ contributing to a review of ASIO's performance management framework.

Into the next reporting period, the Council will continue to consider the proposed introduction of pre-employment and general employment medical standards and the concept of an ASIO career hub.

Fraud control

ASIO is committed to enhancing its fraud control and management arrangements so they reflect best practice. In the reporting period, the fraud risk assessment was updated which informed a revised fraud control plan and guidelines. The ASIO Fraud Control Framework 2016–18 is available online from www.asio.gov.au/asio-fraud-control-framework-2016-18.

In 2015–16, ASIO received no allegations of fraud. Fraud awareness training for all new employees and contractors has been a feature of ASIO induction training for several years. The Organisation also provides a mandatory training module on ethics and accountability, including fraud awareness, as part of its eLearning Academy.

During the reporting period, the internal audit team completed compliance audits in line with legislated requirements and those imposed by Memorandums of Understanding. These audits found:

- ▶ ASIO to be compliant with all requirements and identified only administrative issues that were promptly addressed. Performance audits were completed on asset management and external database search processes; and
- ▶ ASIO to be compliant and made recommendations to improve the efficiency and effectiveness of processes.

As part of ASIO's Integrated Assurance Model, a Baseline Assurance Map was compiled capturing all internal controls and assurance activities across ASIO's functions. This document has been used to set the assurance work program for 2016–17, which is closely aligned with, and supports, the ASIO2020 program.

During the year, ASIO made considerable progress in reviewing and updating its suite of operational policies and procedures. The resulting product—the Intelligence Practice Manual—increases the accessibility of guidance to staff, aligns with the contemporary operating environment, as well as legal and compliance frameworks, and makes future updates of operational guidance easier.

Human resource management

At the end of 2015–16, ASIO employed 1753.4 full-time equivalent (FTE) staff, an increase of just over 2 per cent from 2014–15; ASIO’s annual separation rate was 4.44 per cent.

ASIO’s priority was to increase staffing levels in accordance with the ‘Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat’ funding measure announced in August 2014, with funding received through the 2014–15 additional estimates process in February 2015. The growth in FTE has been, and will continue to be, in ASIO’s intelligence, technical, information and

communication technology areas. There was also some emphasis on building corporate capabilities, such as vetting and recruitment.

The Organisational Capability Program is a mechanism for deploying ASIO staff across the Organisation to distribute resourcing to critical positions. As this program continues to grow, it will provide staff with access to opportunities that align with their own development and also provide ASIO with the ability to deploy staff as priorities dictate.

Recruitment and workforce management

Recruitment efforts focused on the difficult-to-fill roles of surveillance officers, intelligence officers, technical officers and ICT positions. Two significant recruitment changes were made during the reporting period:

- ▶ the continuous acceptance of applications for intelligence officers (rather than only twice a year); and
- ▶ the introduction of an intelligence analyst development program stream.

The recruitment campaign for surveillance officers included a targeted media campaign to attract candidates with a trade background. This popular campaign attracted several thousand applications.

ASIO continued to use the recruitment agency panel established in 2014–15 to broaden the Organisation’s capability and capacity. This included providing administrative support for large recruitment campaigns, such as the surveillance campaign outlined above.

University graduates are one of the target audiences for intelligence officer, junior technical and ICT roles with ASIO. Market research provided insight into graduate employment preferences and feedback on ASIO’s recruitment marketing material. Recruitment brochures, relevant documentation and website content were reviewed and updated in line with the research findings. The research will inform ASIO’s recruitment activity in 2016–17.



Examples of ASIO surveillance officer recruitment campaign advertisements

ASIO also attended nine career fairs and held targeted information sessions for particular disciplines at a number of universities to promote employment opportunities and the Organisation, and to allow students to ask detailed questions.

ASIO's expenditure on recruitment advertising for difficult-to-fill roles and career fair attendance decreased from \$871 902 in 2014–15 to \$791 016 in 2015–16. This reduction was achieved by refining the Organisation's recruitment advertising and prioritising our attendance at career fairs. Over 6500 applications were also submitted to ASIO's online employment register during the year. The register allows those interested in ongoing opportunities to lodge their interest. Candidates were sourced from the register for a variety of vacancies.

In particular, it has been a valuable means to identify people interested in technical and ICT roles. The register was also further refined to attract more candidates with the skill sets in highest demand and it will be reviewed further in 2016–17. The register can be accessed from www.asio.gov.au/careers.html.

ASIO completed 54 recruitment activities in the reporting period. Recruitment activities for technical and ICT job families comprised 11 of the total recruitment activities for the Organisation.

ASIO received 12 997 applications for campaigns that were advertised in 2015–16 (with 322 candidates subsequently withdrawing). There were 278 candidates found suitable, who were either appointed or placed within a merit pool.

Diversity agenda

ASIO continued its strong commitment to gender equity, diversity and inclusion in 2015–16. ASIO developed and implemented a Gender Equity Strategy; released on 8 March 2016 to mark International Women's Day. The Organisation's Gender Equity Reference Group, established in 2015, was critical to informing an action plan and ensuring staff engagement. A dedicated senior officer was appointed to lead the implementation of the strategy and to scope a broader diversity and inclusion program.

Throughout the period, the Director-General continued to regularly address diversity matters in his communications to staff.

ASIO staff also heard from other leaders on the topic of gender equity. In March 2016, Ms Lucy Turnbull AO addressed staff. In April 2016, ASIO hosted an Australian Intelligence Community (AIC) diversity event and AIC staff heard Dr Martin Parkinson PSM, Secretary of the

Department of the Prime Minister and Cabinet, and Ms Elizabeth Broderick AO, former Sex Discrimination Commissioner, speak about their experiences in addressing gender inequality.

Women comprise 45 per cent of ASIO's workforce. ASIO has made progress in improving the statistics of women in the SES, particularly at the SES Band 1 level where there is now around a 45 per cent representation. However, there is still more work to do, particularly at the executive levels. In the next period, and through to 2020, the diversity agenda will focus on a series of bold goals to achieve gender equity across all levels.

Recognising gender diversity is a whole-of-community concern. In 2015–16, the heads of AIC agencies intensified their commitment to gender equality and continued to support cross-AIC initiatives. ASIO contributed to these initiatives, including through its contribution to the AIC Gender Equity Steering Committee.

Workplace agreement

ASIO concluded the negotiation processes and voting for its 10th Workplace Agreement. ASIO is required by the ASIO Act to adopt the employment principles of the Australian Public Service (APS) to the extent they are consistent with the effective performance of the Organisation. All negotiation processes aligned with,

where possible, the broader Australian Government Employment Bargaining Framework. ASIO was bound by similar budgetary and time constraints as those of APS agencies and was required to demonstrate increased productivity and performance outcomes to offset any employee salary increases.

The proposed agreement was voted on by 71 per cent of ASIO employees, and 82 per cent of voters accepted the proposed agreement. The agreement took effect from 10 March 2016 for three years. Changes to terms and conditions under the workplace agreement related to certain leave types, part-time employment arrangements

and redundancy provisions. These changes allowed ASIO to:

- ▶ streamline the administration of these provisions and arrangements;
- ▶ apply further consistency to their application across ASIO; and
- ▶ create greater alignment and consistency with APS provisions and National Employment Standards.

Performance Management Framework

ASIO completed a review of all aspects of its Performance Management Framework. This review was designed to ensure ASIO continued to support and drive a high-performing culture, with a focus on further developing employee and Organisational capability and gaining efficiencies in people management.

Where possible, principles of the *Australian Public Service Commissioner Directions 2013*, Chapter 4 'Performance Management' were adopted, placing a greater level of accountability on employees, line managers and senior management to support and drive a performance-based culture. The outcomes of the review resulted in the:

- ▶ introduction of a standard annual salary advancement date for all employees, with stronger links to performance outcomes;
- ▶ development of further training for line managers in managing unsatisfactory performance or behaviour; and
- ▶ development of a broad suite of policy and process documents to support all areas of the performance management cycle.

In 2015–16, 98 per cent of staff completed their performance obligations. The 2 per cent who did not finalise their obligations comprised employees who were on extended periods of leave, employees who were ineligible due to periods of extended leave taken and employees who separated from the Organisation prior to the review being signed-off electronically.

In 2015–16, no ASIO employees were required to participate in formal underperformance management processes. Consistent with previous years, ASIO remained committed to creating a performance culture to build and develops capability to achieve our strategic and operational objectives to protect Australia, its people and its interests.

Figure 4. Mandatory Performance Management Compliance

No. staff required to undertake Enhancing Performance¹

| | |
|--|------|
| 1646 | |
| No. staff completed ALL Enhancing Performance requirements | 1613 |

¹ Excludes DG, DDGs, Casuals, Trainees, staff on probation and staff who do not have a performance record.

Work health and safety

ASIO's Health and Safety Representative network continues to engage with, and to inform, work teams on the importance of maintaining a safe workplace. In response to injury or incident, ASIO's first aid officers also provide an integral service to the workforce. ASIO's health and wellbeing program HealthINT was refocused during the reporting period. A new primary provider for the program was engaged to ensure initiatives are targeted and build awareness of the benefits of maintaining a healthy lifestyle. The program will continue throughout the year and will seek to deliver initiatives that are innovative and cost effective. In March 2016, the annual influenza vaccination program was offered to all employees who either could attend an in-house appointment or be reimbursed for vaccination cost.

The WHS Committee meets quarterly to discuss current issues and to endorse work health and safety policy and procedures. Attended by employee representatives, management representatives and Health and Safety Representatives, the Committee has an important role in ensuring a safe working environment.

Safety risk awareness drives ASIO's involvement in a number of training programs and ensures the safety and wellbeing of employees remains a key requirement in all ASIO functions. These programs and initiatives continue to highlight WHS risk as an important strategic issue for the Organisation.

An ongoing priority will be to focus on safety risk management processes and engage across the Organisation to further support ASIO's strategic safety agenda. The safety, engagement and overall resilience of ASIO's workforce is improved by these initiatives.

Awareness of the importance of reporting work health and safety incidents will also continue to be raised with

work teams and managers. Systems and reporting thresholds will also continue to be refined to ensure data is accurate.

In 2015–16, ASIO reported four incidents to Comcare in line with legislated notification obligations. One serious injury and three dangerous incidents were reported; however, Comcare recorded only three of these as notifiable incidents. Comcare did not initiate any investigations into the notifiable incidents, nor were any notices issued to ASIO under the *Work Health and Safety Act 2011*.

During the reporting period, ASIO managed:

- ▶ ten early intervention support cases for workers with non-work-related injuries/illnesses;
- ▶ twenty early intervention support cases for workers with work-related injuries/illnesses (did not proceed to workers compensation claim); and
- ▶ thirty seven workers compensation cases.

ASIO continued its active early intervention and preventative approach in compensation and rehabilitation—for both compensable and non-compensable staffing matters. This approach is reflected in the reduction of the compensation premium paid and the outcomes of rehabilitation audits.

The rehabilitation audit examined ASIO's Rehabilitation Management System, processes and outcomes, and validated ASIO's compliance with the *Safety Rehabilitation and Compensation Act 1988* and *Guidelines for Rehabilitation Authorities 2012*. No areas of non-compliance were identified. ASIO continues to enhance processes and maintains an active and positive relationship with the regulator Comcare in both WHS and rehabilitation.

Workforce statistics

Figure 5. Staffing Growth

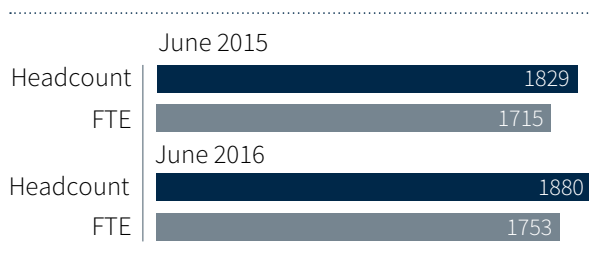


Table 1. Staff by load and employment status

| | 2014-15 | | | 2015-16 | | |
|--------------|--------------|-------------|--------------|--------------|-------------|--------------|
| | Ongoing | Non-ongoing | Total | Ongoing | Non-ongoing | Total |
| Full-time | 1 517 | 31 | 1 548 | 1 565 | 18 | 15 83 |
| Part-time | 211 | 17 | 228 | 225 | 15 | 240 |
| Casual | N/A | 53 | 53 | N/A | 57 | 57 |
| Total | 1 728 | 101 | 1 829 | 1 790 | 90 | 1 880 |

Notes: Non-ongoing employees include locally engaged staff and secondees.

Table 2. Staff by gender and employment status

| | 2014-15 | | | | 2015-16 | | | |
|--------------|--------------|-------------|-----------|--------------|--------------|-------------|-----------|--------------|
| | Ongoing | Non-ongoing | Casual | Total | Ongoing | Non-ongoing | Casual | Total |
| Female | 772 | 23 | 14 | 809 | 811 | 16 | 14 | 841 |
| Male | 956 | 25 | 39 | 1 020 | 979 | 17 | 43 | 1 039 |
| Total | 1 728 | 48 | 53 | 1 829 | 1 790 | 33 | 57 | 1 880 |

Notes: Non-ongoing employees include locally engaged staff and secondees.

Figure 6. Length of Service

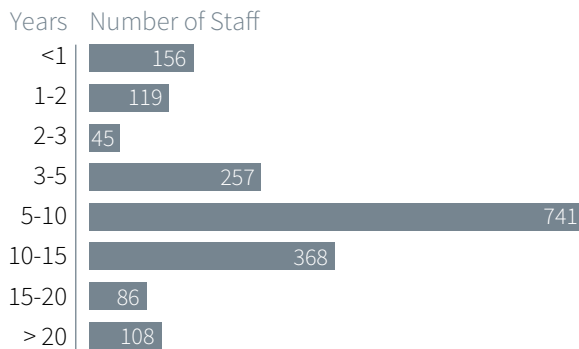
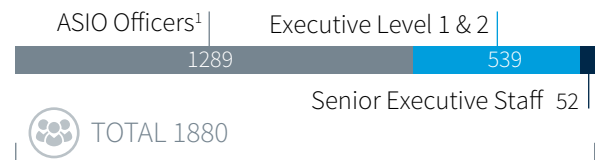


Figure 8. Ratio of Senior Executive to Middle and Lower Level Staff



¹ ASIO Officers include Secondees in and Locally Engaged Staff.

Figure 7. Age Profile

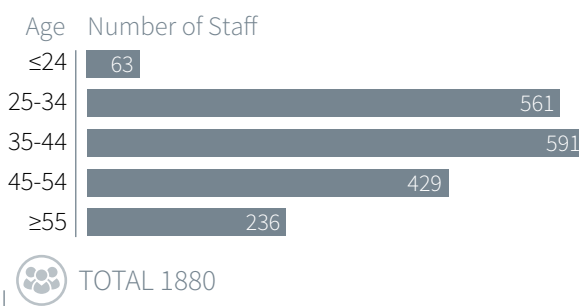


Table 3: Employees by classification and employment status

| | | 2014-15 | | | | 2015-16 | | | |
|--------------------------|------------|--------------|-------------|-----------|--------------|--------------|-------------|-----------|--------------|
| | | Ongoing | Non-ongoing | Casual | Total | Ongoing | Non-ongoing | Casual | Total |
| Senior Executive Service | SES Band 3 | 1 | 1 | 0 | 2 | 2 | 1 | 0 | 3 |
| | SES Band 2 | 8 | 2 | 0 | 10 | 12 | 1 | 0 | 13 |
| | SES Band 1 | 36 | 2 | 0 | 38 | 34 | 2 | 1 | 37 |
| Senior officers | AEE2/3 | 156 | 7 | 3 | 166 | 156 | 3 | 1 | 160 |
| | AEE1 | 330 | 6 | 3 | 339 | 372 | 3 | 4 | 379 |
| Employees | AE1-AE6 | 1083 | 29 | 46 | 1158 | 1085 | 23 | 50 | 1158 |
| IT employees | ITO1/2 | 105 | 1 | 1 | 107 | 121 | 0 | 1 | 122 |
| Engineers | Grade 1/2 | 9 | 0 | 0 | 9 | 8 | 0 | 0 | 8 |
| Total | | 1 728 | 48 | 53 | 1 829 | 1 790 | 33 | 57 | 1 880 |

Table 4. Staff breakdown by level

| Type of Staff | Headcount |
|----------------------------|--------------|
| ASIO Officers ¹ | 1289 |
| Executive Level 1, 2 & 3 | 539 |
| Senior Executive Staff | 52 |
| Total | 1 880 |

1. ASIO Officers include Secondees in and Locally Engaged Staff.

Table 5: Employees by location and employment status

| | | 2014-15 | | | | 2015-16 | | | |
|-----------------|--|--------------|-------------|-----------|--------------|--------------|-------------|-----------|--------------|
| | | Ongoing | Non-ongoing | Casual | Total | Ongoing | Non-ongoing | Casual | Total |
| Canberra-based | | 1 224 | 37 | 39 | 1 300 | 1 268 | 20 | 46 | 1 334 |
| Other locations | | 504 | 11 | 14 | 529 | 522 | 13 | 11 | 546 |
| Total | | 1 728 | 48 | 53 | 1 829 | 1 790 | 33 | 57 | 1 880 |

Table 6. Workplace Diversity

| Classification | Total Staff ¹ | Women | Non-English Speaking Background | Aboriginal and Torres Strait Islander | People with a Disability | Available EEO Data ² |
|---|--------------------------|------------|---------------------------------|---------------------------------------|--------------------------|---------------------------------|
| Senior Executive Service (excl DG) ⁷ | 53 | 19 | 0 | 0 | 0 | 47 |
| Senior Officers ³ | 539 | 195 | 19 | 1 | 6 | 495 |
| AE6 ⁴ | 639 | 337 | 53 | 3 | 7 | 595 |
| AE5 ⁵ | 348 | 186 | 17 | 1 | 1 | 329 |
| AE1 – 4 ⁶ | 171 | 83 | 11 | 3 | 1 | 156 |
| Information Technology Officers Grades 1 and 2 | 122 | 21 | 6 | 2 | 3 | 116 |
| Engineers Grades 1 and 2 | 8 | 0 | 0 | 0 | 0 | 8 |
| Total | 1,880 | 841 | 106 | 10 | 18 | 1,746 |

1. Based on staff salary classifications recorded in ASIO's human resource information system.
2. Provision of EEO data is voluntary.
3. Translates to the APS Executive Level 1 and 2 classifications and includes equivalent staff in the Engineer and Information Technology classifications.
4. ASIO Employee grade 6 group translates to APS Level 6.
5. ASIO Employee grade 5 group translates to APS Level 5.
6. Translates to span the APS 1 to 4 classification levels and includes Locally Engaged Staff and non-SES Secondedes IN.
7. Data excludes the DG and includes Secondedes IN at the equivalent level.

Separation rates

ASIO's annual separation rate decreased from 4.81 per cent in 2014–15 to 4.44 per cent in 2015–16. This figure includes one voluntary redundancy.

Figure 9. Commencements and Separations by Classification

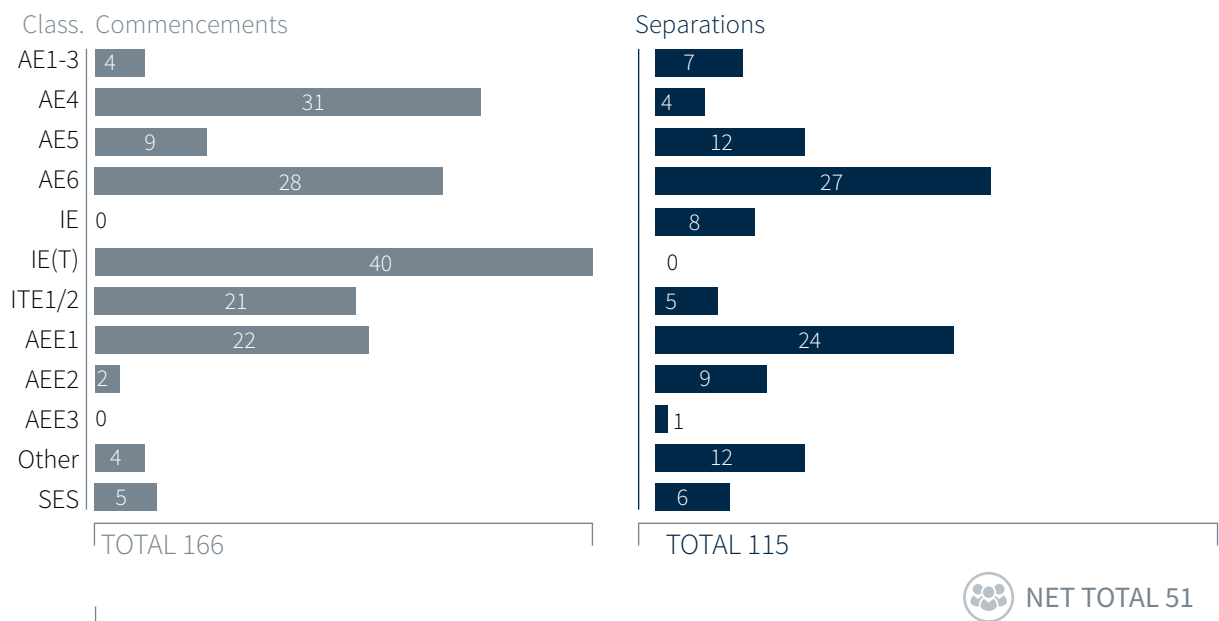


Table 7. Separation by percentage of total staff and reason

| | Resignation | Resignation % ¹ | Age Retirement | Age Retirement % ¹ | Other ² | Other % |
|-------|-------------|----------------------------|----------------|-------------------------------|--------------------|---------|
| Total | 68 | 3.62% | 10 | 0.53% | 37 | 1.97% |

1. Percentage is of total headcount as at 30 June 2016.

2. Other includes contract expired, deceased, dismissed and voluntary redundancy.

Redundancies

ASIO offered one voluntary redundancy during 2015–16.

Attachments

ASIO remains committed to its outreach with regard to secondments, with attachments to and/or from the following agencies:

Table 8. Australian government agency attachments

| Agency |
|--|
| Attorney-General's Department |
| Australian Criminal Intelligence Commission |
| Australian Federal Police |
| Australian Geospatial Intelligence Organisation |
| Australian Signals Directorate |
| Australian Secret Intelligence Service |
| Australian Strategic Policy Institute |
| Australian Transaction Reports and Analysis Centre |
| Defence Intelligence Organisation |
| Defence Security and Vetting Service |
| Department of Defence |
| Department of Foreign Affairs and Trade |
| Department of Immigration and Border Protection |
| Department of Parliamentary Services |
| New South Wales Crime Commission |
| Office of National Assessments |
| Queensland Police Service |
| Treasury |

Misconduct

ASIO conducted two formal misconduct investigations during 2015–16.

Table 9: Nature of misconduct

| Specific element ¹ | Number |
|---|--------|
| Contravened or failed to comply with a term or condition of employment, including the ASIO Values or the Code of Conduct | 2 |
| Been inefficient or lacks diligence in the performance of his or her duties | 1 |
| Been negligent or careless in the performance of his or her duties | 1 |
| Engaged in dishonest or misleading behaviour | 1 |
| Engaged in conduct that adversely affects the performance of his or her duties or has the potential to bring the Organisation into disrepute | 2 |
| Before or after becoming a staff member, wilfully supplied to a person information in connection with his or her application for employment, or his or employment, that was false or misleading | 0 |

1 An individual employee may be counted against more than one type of suspected misconduct

Public Interest Disclosure Act

ASIO did not receive any public interest disclosures during 2015–16.

ASIO is committed to the highest standards of ethical and accountable conduct and support for staff members who make a public interest disclosure in accordance with the *Public Interest Disclosure Act 2013* (PID Act). Where ASIO does receive a disclosure, it provides annual reporting to

the Office of the Inspector-General of Intelligence and Security (IGIS) in accordance with legislative requirements. This, in turn, is included in the IGIS Annual Report and mandatory reporting to the Commonwealth Ombudsman from the IGIS, on behalf of the AIC. Some further information about how ASIO meets its responsibilities under the PID Act is available on the ASIO website at www.asio.gov.au/p-i-d-act.html.

ASIO Ombudsman

The ASIO Ombudsman is an external service provider who acts to resolve staff issues or concerns impartially and informally, through advice, consultation and mediation. The Ombudsman continued to meet regularly with ASIO senior management and with representatives of the Staff Association to discuss the health of the workplace. The Ombudsman continued to provide valuable support and advice to employees and line managers during the reporting period. During the year, the Ombudsman:

- ▶ provided advice and guidance in response to 20 informal contacts from staff;
- ▶ provided formal advice based on investigations into eight matters. Four investigations were relevant to the Code of Conduct, two were related to Organisational restructure conditions, and two were independent reviews of management actions;
- ▶ provided assistance to an inquiry from the IGIS related to a previous employee; and

- ▶ undertook formal consideration of conditions-of-service matters and provided advice to staff and management.

During the reporting period, the Ombudsman also actively promoted the role of the Ombudsman and the importance of the ASIO Values and Code of Conduct in establishing a proper and respectful workplace culture, in a wide range of presentations, branch meetings, induction programs and management training sessions. The Ombudsman was also directly involved with the Harassment and Discrimination Network.

In 2015–16, the ASIO Ombudsman did not participate in any work related to public interest disclosures.

Training and development

ASIO continued its training and capability development in line with the principles of a learning Organisation and the 70:20:10 principle. The principles of a learning Organisation include creating, acquiring and transferring knowledge, and synthesising new knowledge and insights. The 70:20:10 principle advocates that, of all employee learning:

- ▶ 70 per cent should be acquired by on-the-job experience;
- ▶ 20 per cent should be acquired by informal learning; and
- ▶ 10 per cent should be acquired by formal learning.

This approach aligns with the outcomes of the ASIO training review commissioned by the Director-General in 2014–15.

ASIO's continued investment in this area has seen new programs developed in line with the changes in the Organisation's operating, security and technical environments. ASIO broadened and diversified its training delivery models so that staff can access training opportunities using different mediums. This ensures staff can continue to develop their skills and capabilities despite the high operational tempo. During the reporting period, ASIO continued its focus on enhancing relationships with close national and international partners to deliver mutual training benefits and ensure best practice through benchmarking. These partnerships have enabled the sharing of training opportunities, facilities, instructors and standards.

Intelligence training

ASIO continued to expand its graduate development programs, through which it recruits, develops and produces 'job ready' officers with the necessary intelligence discipline skills. The programs are the:

- ▶ Intelligence Officer Development Program (IODP);
- ▶ Technical Graduate Program (TGP); and
- ▶ Intelligence Analyst Development Program (IADP).

These programs reflect the focus on attracting and developing a high-quality and skilled workforce for the future. The IODP trains and develops new intelligence officers in analytical and operational tradecraft. The program incorporates classroom-based learning and practical exercises, integrated mentoring and short-term placements in the workplace to solidify learning outcomes. Two IODPs were completed in the reporting period.

The new TGP is being run on an annual basis since the success of the first iteration in 2014–15. The TGP includes specialist training, integrated mentoring, and placements in a range of technical areas within ASIO's Technical Capabilities Division, including in software development, technical development, telecommunications, computer forensics and technical operations.

In recognition of the importance of ASIO's analytical and assessment function, a new IADP commenced in June 2016. The IADP includes classroom-based learning and practical exercises, new specialist analytical training, integrated mentoring, and a range of short-term placements across ASIO's analytical and assessment areas.

ASIO continued to focus on developing advanced and specialised intelligence training courses during this reporting period. This included investing in refresher training for perishable skills, as well as developing and delivering new programs to further develop or refine advanced skill sets. New programs included tailored leadership training for each intelligence discipline, which complement broader management and leadership programs.

Management and leadership development

ASIO continued to deliver management and leadership development opportunities in line with ASIO's overarching Management and Leadership in Security Intelligence Strategy (2013–16). Notably, this strategy, and associated development programs, was awarded the 2015 Rob Goffee Award for Leadership Development by the Australian Human Resources Institute.

In addition to ASIO's well-developed pathway programs—the Management Skills in ASIO program, the Introduction to Management Program and the Mastering Management Program—the Organisation's management and leadership program now includes a range of alumni and leadership networking events. These opportunities build on the investment made in ASIO's formal management and leadership programs over recent years and serve to enhance the Organisation's relationships and strategic alignment with close partners.

Investment in the development of ASIO's SES also continued, including through:

- ▶ external mentoring partnerships;

- ▶ internal leadership-themed events, including a leadership speakers program—launched by the Governor-General, His Excellency General the Honourable Sir Peter Cosgrove AK MC (Retd), and with speakers including Dr Martin Parkinson PSM, Secretary of the Department of the Prime Minister and Cabinet; and
- ▶ targeted individual development opportunities, including attachments and/or formal development programs delivered internally or by academic institutions. This investment, in which every ASIO SES officer has been involved, represents ASIO's commitment to develop and maintain a diverse pool of leadership talent capable of leading the Organisation to meet future challenges.

A new Management and Leadership in Security Intelligence Strategy will be developed for the 2017–20 period, to align with key strategic objectives including the ASIO 2020 program and the Organisation's diversity goals.

Study support and language development programs

ASIO continued to support its staff to undertake study or language development during 2015–16 with over 10 per cent of ASIO staff receiving support.

- ▶ A total of 117 officers participated in 79 ASIO-supported study programs, at a cost of \$301 635. The studies spanned a range of disciplines, including security and policy, conflict and strategic studies, business management, project management and information technology.

- ▶ In 2015–16, a new internal language program was developed. This has been well received and enhanced the capacity for staff to build language skills. ASIO spent \$370 281 on language training for 69 employees across 21 languages.

e-Learning

An area of significant focus over the reporting period was building on existing online training, known as the eLearning Academy, to design and deliver training courses for our workforce. To ensure alignment with workforce requirements, the new program was developed with input from a working group representing relevant ASIO divisions. All staff members now have access to a range of training opportunities, including more advanced or specialised modules based on specific role requirements.

The eLearning Academy continued to deliver mandatory competency-based training on a range of subject areas, such as WHS, workplace behaviour, ethics and accountability, environmental management and the

public interest disclosure scheme. New modules were developed and added to the existing catalogue, including some in support of ASIO's safety and security training program. Of note, two additional information technology modules related to core systems training were added to further support the accreditation of staff.

During the reporting period, there were 2498 mandatory and 1760 non-mandatory eLearning Academy course completions. This figure is in addition to 4728 instances of face-to-face training, attended by 1643 employees across 120 training courses.

National Intelligence Community training

The National Intelligence Community Training Secretariat (NICTS) identifies and delivers learning and development opportunities that enhance common understanding across the National Intelligence Community (NIC). The NICTS is managed on a day-to-day basis, staffed by ASIO and housed in ASIO's Ben Chifley Building. The strategic direction for the NICTS is set by the NIC Training Committee, which is chaired on a rotating basis by a NIC senior officer and co-chaired by an ASIO SES officer (Assistant Director-General, Training Branch). In 2015–16, ASIO continued to contribute to NIC training programs as a presenter and a participant.

During the reporting period, ASIO worked closely with the Australian National University's (ANU's) National Security College (NSC) in support of its goal of enhancing strategic understanding and critical thinking about Australia's national security. ASIO regularly contributes presenters and participants for NSC programs.

Legislation and litigation

Legislation amendment

During the reporting period ASIO continued to work closely with the Attorney-General's Department (AGD) and other agencies on the development of legislation affecting its operations. Ongoing legislative reform is important to ensure that ASIO's legislative framework enables and assists it to perform its statutory mandate in a rapidly changing security environment.

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* received Royal Assent on 13 April 2015 and the operative provisions came into effect on 13 October 2015. The Act amended the *Telecommunications (Interception and Access) Act 1979 (TIA Act)* and the *Telecommunications Act 1997* to introduce a statutory obligation for telecommunications service providers to retain specified telecommunications data for a minimum two year period. The data retention scheme does not provide ASIO any additional powers, or give ASIO any new capacity to access communications data. The amendments also introduced a new warrant to regulate access to telecommunications data relating to a journalist to provide additional protection for journalists and their confidential sources. ASIO may seek a journalist information warrant where a purpose of accessing telecommunications data is to identify a person who is known or reasonably believed to be a source.

Australian Citizenship Amendment (Allegiance to Australia) Act 2015

The *Australian Citizenship Amendment (Allegiance to Australia) Act 2015* (Allegiance Act) passed in both Houses of Parliament on 3 December 2015 and commenced on 12 December 2015. The Allegiance Act amends the *Australian Citizenship Act 2007* and introduces three key provisions which result in the loss of Australian citizenship where the person is a dual citizen:

- ▶ the person renounces their Australian citizenship if they act inconsistently with their allegiance to Australia by engaging in specified terrorist related conduct;

- ▶ the person ceases to be an Australian citizen if the person fights for, or is in the service of, a declared terrorist organisation; and
- ▶ the Minister for Immigration and Border Protection makes a determination that a person ceases to be an Australian citizen if the person is convicted of a specified terrorism offence.

Australian Security Intelligence Organisation Regulation 2016

The *Australian Security Intelligence Organisation Regulation 2016*, which came into effect on 01 April 2016, includes a new regulation to enhance ASIO's ability to cooperate with the Department of Defence (Defence) including the Australian Defence Force, by prescribing Defence as a body with which ASIO may cooperate for the purposes of the ASIO Act. This would allow ASIO to assist Defence in the performance of its functions. Assistance may include, but is not limited to, capability sharing such as the provision of linguistic, analytical, technical or logistical support.

This amendment to section 19A of the ASIO Act was proposed to cover any future requirement where ASIO is requested to assist the Defence, including the Australian Defence Force, for the performance of their functions. Section 19A already allowed for engagement with the Australian Signals Directorate and the Australian Geospatial Organisation, but not the rest of Defence.

Telecommunications and Other Legislation Amendment Bill

During the reporting period, ASIO continued to work with AGD on proposed amendments to the *Telecommunications Act 1997* and related legislation to introduce a regulatory framework to better manage national security risks to Australia's telecommunications services and networks. Public comment on the draft Bill, as well as the explanatory memorandum and draft industry guidelines, was sought between November 2015 and January 2016. The Bill will:

- ▶ establish a security obligation for carriers and carriage service providers to require them to do their best to protect their networks from unauthorised access and interference;

- ▶ require carriers and some carriage service providers to notify the Commonwealth Government of planned key changes to networks and services that could compromise their ability to comply with the security obligation;
- ▶ empower the Secretary AGD to request information from carriers and carriage service providers to monitor compliance with the security obligation; and
- ▶ provide the Attorney-General with a power to issue a Carrier/Carrier Service Providers a direction requiring them to do or refrain from doing a specified thing to manage security risks.

Amendments to information privacy laws

As reported in 2014–15 Submission and consistent with the recommendation of the *Joint Commonwealth–New South Wales review of the Martin Place Siege*, ASIO with the support of AGD, has been pursuing amendments to state and territory legislation in relation to information privacy. The review recommended, amongst other things, that all states and territories should review relevant legislation, in particular with respect to privacy and health, to ensure appropriate access by ASIO.

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. Each warrant request is independently reviewed by AGD before progressing to the Attorney-General. The Attorney-General considers the request and, if in agreement, issues the warrant.

To perform its functions, ASIO is authorised under the ASIO Act and the TIA Act to undertake the following methods of investigation:

- ▶ telecommunications interception and access;
- ▶ use of surveillance devices;

- ▶ entry 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 for questioning for 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.

Litigation

ASIO’s involvement in civil litigation (in particular, merits reviews and judicial reviews of its security assessments) and criminal prosecutions and control order hearings (especially in relation to counterterrorism matters) continued this year. ASIO worked to provide the AAT, courts and applicants with relevant material in security assessment reviews, and to contribute sensitive information as evidence in criminal and civil proceedings. A particular concern was to balance the necessary protection of sensitive information (including intelligence capabilities and methods, officer and source identities, and liaison relationships) with ASIO’s obligation to meet discovery requirements, assist the Crown to meet disclosure obligations and provide the fullest possible responses to subpoenas and statutory requests. Coronial inquests are one area in which there has been a considerable increase in the involvement of national security agencies, including ASIO. ASIO gave evidence in two coronial inquests during the reporting period: those

held into the deaths arising from the Lindt Cafe siege in Martin Place and the death of Ahmed Numan Haider.

Judicial reviews—security assessments

Two security assessment reviews were also commenced in the Federal Court of Australia during the reporting period.

- ▶ *BSX15 v Minister for Immigration and Border Protection and Director-General of Security (VID473/2015)* was commenced in August 2015 and heard by Justice Markovic on 19 April 2016 (decision reserved).
- ▶ *Mustapha El Ossman v Minister for Immigration and Border Protection and Director-General of Security (NSD885/2016)* was commenced in June 2016 (and yet to be heard at the time of reporting). Both matters were still before the courts and both applicants were in immigration detention at the time of this reporting.

Tribunal reviews—security assessments

ASIO managed nine security assessment reviews by the AAT and an additional 13 reviews were commenced during the reporting period. Of these 22 security assessment reviews:

- ▶ nine were withdrawn at various stages of ASIO preparation;
- ▶ two were heard by the AAT and one is yet to be decided. The other was affirmed and reported as *TNFD v Director-General of Security; Minister for Foreign Affairs* [2015] AATA 752 (25 September 2015).

Coronial inquest into the deaths arising from the Lindt Café siege in Martin Place

The State Coroner of NSW (Michael Barnes) is presiding over a coronial inquest into the deaths of Tori Johnson, Katrina Dawson and Man Haron Monis arising from the Lindt Cafe siege in Martin Place on 15 and 16 December 2014. The AGD is coordinating Commonwealth cooperation.

The inquest is investigating a wide range of issues, including issues relevant to ASIO; in particular, whether ASIO appropriately assessed, and took action in relation to the threat Mr Monis posed to the community. ASIO has a responsibility to provide evidence about ASIO's activities in support of the coroner's aims. ASIO is engaged and cooperating fully with the inquest.

Coronial inquest into the death of Ahmed Numan Haider

The State Coroner of Victoria (John Ollie) is presiding over a coronial inquest into the death of Ahmed Numan Haider. On 23 September 2014, Joint Counter Terrorism Team (JCTT) officers invited Mr Haider to attend an interview at the Endeavour Hills Police Station. Mr Haider met with two JCTT police officers in the car park, where he produced a knife and attacked both officers. Both police officers were seriously injured. Mr Haider was fatally shot by one of the police officers. ASIO is engaged and cooperating fully with the inquest.

Terrorism and other criminal prosecutions

At the end of the reporting period, ASIO was involved in 11 national security prosecutions, where ASIO has provided information collected from security investigations for inclusion in briefs of evidence and/or the accused was a person of interest to ASIO.

Security of ASIO

Over recent years, changes to the security environment have resulted in an increased threat to the personal safety of ASIO staff. Recent low-capability, lone actor terrorist attacks around the world—including attacks against police here in Australia—demonstrate the real danger to staff. ASIO officers are operating in an environment that puts their personal safety at risk from spontaneous or opportunistic attack using readily acquired weapons and relatively simple tactics. Reporting of suspicious activities and behaviours in and around ASIO premises has risen. To address the threat, ASIO's protective security measures have increased commensurate with the level of risk. ASIO has diverted resources to further build layered security and safety measures. These include:

- ▶ developing and operating new staff-tracking and duress alert technologies to support employees working operationally;
- ▶ introducing a range of enhanced security measures for ASIO premises, including overt physical security measures and the patrolling of ASIO's headquarters by armed AFP officers; and
- ▶ introducing a suite of enhanced personal safety and security training courses to equip employees to operate in a more hostile environment.

Security awareness training courses are delivered frequently through the year and across Australia. In addition, elements of these courses were extended to close partner agencies that operate in a similar environment and have similar staff development requirements. Elements have also been adopted by close partner agencies to enhance their own internal programs and the safety and security of their staff.

Security governance and policy

ASIO's security governance is overseen by its Security Committee. That committee reports to ASIO's Executive Board, is chaired by a Deputy Director-General and has Senior Executive Service membership drawn from Divisions across the Organisation.

The Committee ensures ASIO's security policies and practices comply with the Australian Government's Protective Security Policy Framework (PSPF), and that the Organisation has appropriate protective security measures in place commensurate with its specific security environment. This includes ensuring that all

employees have access to the training, tools and advice required to actively manage security risks consistent with ASIO's strong security culture.

ASIO seeks opportunities to contribute to the maintenance of Australian Government security policy frameworks and policies. This includes enhancing the Australian Government's defensive posture against the malicious insider threat. ASIO has focussed on four key areas:

- ▶ Translating investigative, analytical and personnel security assessment experience into policy initiatives through participation in the Attorney-General's Department-led Personnel Security Strategic Reforms Taskforce (PSSRT);
- ▶ Dissemination of threat advice to government and security vetting officers;
- ▶ Provision of threat briefings to Australian government agencies; and
- ▶ Outreach activities to industry and government through the ASIO Business Liaison Unit and the Contact Reporting Scheme.

Security clearances in ASIO

The pressure on ASIO's initial and ongoing vetting has continued through the reporting period. ASIO's vetting resources were bolstered in the previous reporting periods in response to existing pressures and to support additional recruitment associated with supporting the government's response to the increased terrorism threat.

e-Security

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

Management of relationships and public reporting

Business Liaison Unit

ASIO's Business Liaison Unit (BLU) provides an interface between the Australian Intelligence Community (AIC) and the private sector. The BLU hosts a secure website which has a total of 3612 subscribers and where intelligence-backed, declassified reports are published. The BLU website was upgraded to improve user experience and search functionality in June 2016.

The BLU hosted five classified briefing days for high-threat sectors (such as aviation, communication and places of mass gathering), provided hundreds of tailored briefings to corporate security managers, and facilitated dozens of executive-level briefings. The detailed, sector-specific information provided by the BLU to the private sector ensures owners and operators of critical infrastructure, and other high threat sectors, have the necessary security information regardless of their clearance level.

ASIO's cyber outreach activities were coordinated through its membership of the multi-agency Australian Cyber Security Centre (ACSC). The ACSC comprises elements of Australian Signals Directorate, Defence Intelligence Organisation, Computer Emergency Response Team Australia, the Australian Federal Police, Australian Criminal Intelligence Commission and ASIO. The ACSC is a hub for collaboration and information sharing with the private sector, state and territory governments, academia and international partners to combat the full range of cyber threats. More information on the ACSC is available at www.acsc.gov.au.

ASIO continued to provide advice to Australia's telecommunications industry on the national security threats to the sector and worked closely with key partners to mitigate risks of unauthorised access or interference to their networks and data holdings. Services provided by the telecommunications industry are critical to Australia's national security, growth and prosperity. ASIO's advice helped the industry consider and mitigate risks to the availability, integrity and security of these services. This advice complemented, and was enriched by, the best-practice information assurance principles and policies developed within the ACSC for broader industry and government engagement on cyber security issues.

Increased government outreach continued during the reporting period. Expanded liaison supported major international events, including regular briefings to inter-departmental committees, security working groups and organising committees of major international events.

ASIO provided protective security advice in the lead-up to, and during, major international events to support the Australian Government's broader security responses leveraging ASIO's international partnerships and threat assessment capability. ASIO's activities helped build resilience and raise awareness by broadening the understanding of threats faced by the Australian community. ASIO supported events including World War One Centenary commemoration services in Turkey, France and Belgium, the Olympic Games, the Asia-Pacific Economic Cooperation forum, the Commonwealth Heads of Government Meeting, and the Group of Twenty forum.

Stakeholder satisfaction survey

ASIO surveys key stakeholders in the Australian Government and states and territories each year. The survey seeks to capture feedback on the quality of ASIO's advice, the effectiveness of the Organisation's capabilities and people, and the value added through cooperation and collaboration. Stakeholders surveyed indicated:

- ▶ ASIO is highly or well regarded by agencies, with the Organisation and its staff seen as professional and responsive;
 - ▶ ASIO is a key partner by many stakeholders across all Australian governments;
 - ▶ ASIO assistance to build or enhance stakeholder capabilities would be/is appreciated;
- ▶ ASIO's assessed product and analytical capability is respected, across both the counter-terrorism and countering espionage and interference activities, and many stakeholders expressed an appetite for more anticipatory assessments; and
 - ▶ ASIO remained responsive and agile in providing counter-terrorism intelligence and support to partners, and law enforcement partners expressed an appetite for increased availability of unclassified information to enhance ASIO's cooperation and enable their activities.

Public statements and 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 2015–16: www.asio.gov.au/media/speeches-and-statements.html.

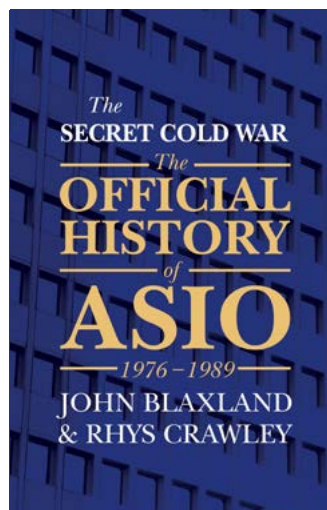
The media can contact ASIO directly through a publicly listed media contact number and email address.

In 2015–16, ASIO continued to respond to media inquiries, without commenting on operations, investigations, individuals or operational capabilities.

Official History of ASIO

The Attorney-General launched *The Protest Years: the Official History of ASIO 1963–1975*, Volume II of the history, on 16 October 2015. Dr John Blaxland of the ANU Strategic and Defence Studies Centre wrote this volume. Overall responsibility and direction for the project at the ANU remains with Professor David Horner AM. The third and final volume, *The Secret Cold War: the Official History of ASIO 1975–1989*, authored by Dr Blaxland and Dr Rhys Crawley, is to be the last in the current project.

Since their release, Volume I, *The Spy Catchers: the Official History of ASIO 1949–1963*, has sold over 8500 copies and was named a joint winner of the Prime Minister's Literary Awards Prize for Australian History. Volume II has sold over 5000 copies. ASIO's website has more information about the project at www.asio.gov.au/history.html.



Public access to ASIO records

The *Archives Act 1983* allows for public access to all Australian Government records in the open access period. The open access period currently covers access to records created in or before 1991. Requests to access ASIO records are made to the National Archives of Australia (NAA). The NAA passes the application to ASIO where relevant records are located and assessed. ASIO determines whether any information should be exempt from public release on national security grounds, balancing the request for public access with the need to protect sensitive information.

Applicants dissatisfied with ASIO exemptions can request a reconsideration of the decision. In 2015–16, there were

four internal considerations. The NAA upheld the ASIO exemptions in each case. Applicants may also appeal the exemptions to the AAT if their request is not completed within 90 days. There was one new AAT appeal in the reporting period, which remains ongoing. One application from 2012–13 for ‘deemed refusal’ of multiple requests was finalised in February 2016 after ASIO provided the applicant with 11 032 pages of records.

In 2015–16, the number of applications made for access to records decreased. A total of 650 requests were completed in 2015–16. Although the number of requests completed declined, the number of pages examined increased.

Table 10. Processing of applications for access to ASIO records

| | 2014–15 | 2015–16 |
|--------------------------------|---------|---------|
| Applications for record access | 790 | 473 |
| Requests completed | 811 | 650 |

ASIO’s international relationships

ASIO’s international engagement program is a cornerstone of the Organisation’s intelligence collection and assessment capability. International liaison relationships are a force multiplier, enabling ASIO to draw on the information, experience and capability of other services.

Oversight and Accountability

Ministerial accountability

ASIO's ministerial accountability is to the Attorney-General, Senator the Hon. George Brandis QC. ASIO conducts security intelligence activities in accordance with the Attorney-General's Guidelines, which are available online at www.asio.gov.au/attorney-generals-guidelines.html. The guidelines stipulate that ASIO's 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 AGD following a recommendation by the PJCIS.

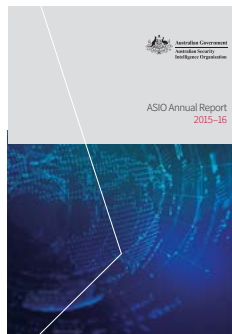
ASIO keeps the Attorney-General informed of significant national security developments, as well as other important issues affecting ASIO. During the reporting period, ASIO provided advice to the Attorney-General on a range of investigative, operational and administrative issues, primarily communicated through 321 formal submissions. The Director-General also briefs other ministers on security issues and matters relevant to their portfolios, when required.

Leader of the Opposition

The Director-General of Security is a statutory position, with a responsibility to provide impartial advice. The ASIO Act requires the Director-General to regularly brief the Leader of the Opposition on matters relating to security and to provide him or her with a copy of ASIO's classified annual report. From time to time, with the Attorney-General's knowledge, classified briefings on specific security cases have been provided for other shadow ministers. During 2015–16, the Director-General briefed the Leader of the Opposition on significant security matters when required.

Report to Parliament

ASIO's Annual Report to Parliament contains an account of ASIO's activities during the reporting period, including the nature of the threat environment, an account of ASIO's performance across its functions, details of ASIO's corporate human resources and governance arrangements, and ASIO's financial statements.



In addition to this unclassified report, ASIO also produces a highly classified annual report outlining ASIO's operational and corporate activities in greater detail. This classified annual report is distributed externally to the Attorney-General and a select group of ministers, including the National Security Committee of

Cabinet, the Leader of the Opposition and a small group of senior Australian Government officials.

Parliamentary Joint Committee on Intelligence and Security

During 2015–16, ASIO made one submission to the Committee as part of its Review of Administration and Expenditure No. 14 (2014–15) Australian Intelligence Agencies. Representatives from ASIO attended a private hearing relating to the submission in February 2016.

In September 2015, ASIO representatives attended the public hearings on the review of the re-listing of Al-Shabaab, Hamas Izz al-Din al-Qassam Brigades, Kurdistan Workers' Party (PKK), Lashkar-e-Tayyiba and Palestinian Islamic Jihad as terrorist organisations.

In August 2015, ASIO representatives attended the public hearings on the PJCIS Advisory report on the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015. ASIO's evidence to the Committee can be found on the relevant inquiry page on the Committee's website http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security.

Senate Standing Committee on Legal and Constitutional Affairs

ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the senate estimates process on 9 February 2016 and 5 May 2016 (ASIO was released from appearing at the hearing on 15 October 2015). ASIO's evidence to the Committee can be found in the estimates Hansard for the relevant days (go to www.aph.gov.au/Parliamentary_Business/Senate_Estimates and navigate to the relevant hearing).

Independent oversight

Inspector-General of Intelligence and Security

The Hon. Margaret Stone was appointed as IGIS in August 2015. The role of the IGIS is to review the activities of the AIC and provide assurance that agencies operate with propriety, according to law, consistent with ministerial guidelines and directives, and with due regard for human rights.

The powers of the IGIS are wide-ranging and similar to those of a royal commission and include access to ASIO records and premises. The IGIS conducts regular inspections of ASIO investigative activities and other projects—including reviewing ASIO’s implementation of IGIS recommendations. ASIO senior leadership and the IGIS meet regularly to discuss current issues, and a bi-monthly roundtable is also held, with ASIO proactively identifying issues. ASIO ensures the staff of the Office of the IGIS have the access they require, and provides the Office with briefings about particular aspects of ASIO’s work and systems.

The independent oversight provided by the IGIS, and compliance recommendations arising from IGIS reviews and inspections, is used by ASIO to improve its processes.

During 2015–16, the IGIS undertook a regular inspection program of activities across ASIO’s operational and investigative 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 Reviewer of Adverse Security Assessments

Mr Robert Cornall AO was appointed as Independent Reviewer on 3 September 2015.² The Independent Reviewer conducts independent advisory reviews of ASIO adverse security assessments provided to the DIBP in relation to ‘eligible persons’. An ‘eligible person’ is an individual who:

- ▶ remains in immigration detention, having been found by DIBP to be owed protection obligations under international law;
- ▶ is ineligible for a permanent protection visa; or
- ▶ has had their permanent protection visa cancelled, because they are the subject of an adverse security assessment.

During the reporting period:

- ▶ Ten adverse security assessments were reviewed (one primary and nine periodic reviews).
 - ▶ There was no difference of opinion between the Independent Reviewer and the Director-General as to the appropriate outcome in any of those cases.
 - ▶ Only four cases remain before the Independent Reviewer: two primary and two periodic reviews.
- At the end of the reporting period:

- ▶ one primary review was close to completion;
- ▶ the other primary review was under active consideration and awaiting a submission from the applicant’s solicitors;
- ▶ a complicated matter due for periodic review was deferred with the agreement of the applicant’s solicitors, pending the outcome of ASIO’s internal review of that adverse security assessment; and
- ▶ one periodic review (deferred by the former Independent Reviewer) remained deferred with the agreement of the applicant’s legal advisers, pending the completion of ASIO’s separate internal review (which was in train at the end of the reporting period).

² The Hon. Margaret Stone concluded her term as Independent Reviewer of Adverse Security Assessments on 21 August 2015 due to her new appointment as IGIS.

Independent National Security Legislation Monitor

The Hon. Roger Gyles AO QC was appointed as the Independent National Security Legislation Monitor on 7 December 2014. The Monitor'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 2015–16, ASIO made submissions to the Monitor on the following inquiries:

- ▶ section 35P of the ASIO Act concerning offences for the disclosure of information relating to a special intelligence operation; and
- ▶ certain questioning and questioning and detention powers in relation to terrorism.

ASIO representatives also attended the public and private hearings on these matters. ASIO's submissions to the Monitor and evidence given at public hearings can be found on the relevant inquiry page on the Monitor's website: www.inslm.gov.au.

