Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure

No.14 2014–2015

www.asio.gov.au

Contents

Executive Summary 3
- The security environment and outlook 3
- Expenditure 3
- Corporate direction and strategic planning 4
- Human resource management 4
- Legislation and litigation 5
- Security of ASIO 5
- Management of relationships and public reporting 5

Scope of the review 6

ASIO's role and functions 7

The security environment and outlook 8
- Terrorism 8
- Espionage and clandestine foreign interference 11
- Communal violence and violent protest 12
- Border integrity 13
- Outlook for the security environment 13

Expenditure 14
- Budget 14
- Financial performance 14
- Strategic allocation of resources 15
- Financial management and internal controls 16

Structure of the Organisation 17

Corporate direction and strategic planning 18
- ASIO Strategic Plan 2013–16 18
- Corporate governance 18
- ASIO Executive Board 18
- Intelligence Coordination Committee 19
- Workforce Capability Committee 19
- ASIO Security Committee 20
- Finance Committee 20
- Audit and Risk Committee 20
- Audit and fraud 20
- Communication and leadership meetings 21
- ASIO Consultative Council 21

Human resource management 22
Recruitment & work force management 22
Training and development 23
Separation Rates 28
Attachments 29
Staffing and personal matters 29
Public interest disclosure 29
Performance Management 30
Misconduct 30

Legislation and litigation 31
National Security Legislation Amendment Act (No. 1) 2014 31
Counter-Terrorism Legislation Amendment (No. 1) Act 2014 31
Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014 32
Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 32
Telecommunications and Other Legislation Amendment Bill 2015 32
Amendments to information privacy laws 33
Use of ASIO special powers 33
Litigation 33

Security of ASIO 34
Security governance and policy 34
Security clearances in ASIO 35
Security Breaches 35

Management of relationships and public reporting 36
36
Parliamentary oversight 36
Independent oversight 38
ASIO's domestic relationships 40
ASIO's international relationships 42

Executive Summary

The security environment and outlook

Australia is confronting a broad range of security challenges, particularly in its countering terrorism and countering espionage effort. While terrorism is the most obvious and immediate challenge—posing a direct and ongoing threat to the safety and wellbeing of Australians—espionage and foreign interference directed against Australia by foreign powers also presents a first order challenge, its impact having the potential to undermine Australia's sovereignty. Foreign interference in Australia by foreign powers persists. It spans community groups, business and social associations and is directed against the Australian government and the community.

While events, people and organisations overseas remain a factor for almost all security threats, in the counter-terrorism context these are increasingly finding expression through the actions of individuals without close or direct links to the overseas drivers. We continue to identify and investigate Islamist extremists in Australia who support or are engaged in terrorism-related activities, both here and overseas. Our investigations include groups and individuals who adhere to an extreme interpretation of Islam and whose ideologies have the potential to manifest in an onshore terrorist attack.

The conflict in Syria and Iraq continues to resonate strongly amongst those in Australia susceptible to the broad Islamist extremist narrative and to extremist messaging. A new generation of Islamist extremists has formed and the activities of these individuals will impact the Australian security environment for years to come; we are particularly concerned about the emerging threat from an increasingly young and volatile cohort of terrorist sympathisers and supporters in Australia.

Symbols of government, including the military, police and security agencies, remain targets of choice. However, a random attack against a public mass gathering or member of the public would align with terrorist targeting objectives and, regardless of scale, would have significant impact. Lone actors or small groups of like-minded individuals could mount such an attack without intelligence forewarning; this scenario represents a significant challenge to security and law enforcement agencies and threats emanating from such individuals may develop quickly, especially if the intended act requires minimal preparation.

Clandestine foreign interference activity and espionage against Australia and Australian interests is occurring on a large scale. The perpetrators are utilising techniques and capabilities—including human intelligence, technical collection methods and exploitation of the internet and information technology—to target strategically important Australian interests. There is an enduring requirement for ASIO to allocate resources to defensive outreach and advice to heighten awareness of the threat environment and to drive appropriate security policy responses.

Expenditure

In 2014–15 ASIO received an appropriation of $368.4 million which included $11.2 million of additional funding relating to the 'Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat' measure announced by the Government in August 2014. ASIO's budget, which includes a significant, non-discretionary component associated with the need to maintain high levels of security, has been under considerable pressure in recent years.

The budget continues to be a challenge due to the impact of the efficiency dividend, increased security overlay costs and expenditure ASIO absorbs, which includes security assessments relating to Illegal Maritime Arrivals (IMAs), costs associated with Operation Sovereign Borders and data retention. Additionally, ASIO will contribute to the National Security Hotline Campaign as well as savings measures required by government due to the budget savings measures.

Looking forward over the next four years, through the 'Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat' measure, ASIO will receive a further $128.5 million in operating funding and $41.4 million in capital to continue to strengthen ASIO's counter-terrorism capabilities. During this time ASIO will return around $93.7 million to government through the efficiency dividend and other savings measures ($65.9 million in efficiency dividend and $27.8 million on other savings measures or absorbed costs).

Corporate direction and strategic planning

ASIO's Strategic Plan 2013–16 ensures the organisation's activities are directed against identified priorities for the period. In 2014–15, ASIO focused closely on two of its strategic goals:

- 'We manage risk in a constantly evolving security environment'—identifying key risks and translating these into actionable work programs that are evaluated for effect.
- 'Attract, develop and retain a professional and highly competent workforce' —in response to the New Policy Proposal funding received during the reporting period, ASIO committed additional resources to effectively recruit new talent.

Human resource management

The funding received through the 'Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat' measure saw a shift in ASIO's people strategy from a focus on reducing and consolidating, to one of expanding capabilities and growth.

An online employment register was established during the reporting period, supported by a national recruitment awareness campaign. As at 30 June 2015, over 4900 applications had been submitted. ASIO's expenditure on recruitment advertising for difficult-to-fill roles increased from $599 739 in 2013–14 to $871 902 in 2014–15, with both greater participation in university career fairs and the employment register national campaign contributing to the majority of the increase.

A recruitment agency panel was established during the reporting period as a key strategy to provide talent sourcing expertise, increase screening capacity and as part of improving the first phase of the recruitment process. Use of the panel is a significant investment by the Organisation, and a review at the end of 2014–15 identified greater efficiency and effectiveness with regard to recruiting technical and ICT candidates, and a substantial increase in capacity.

ASIO invested heavily in its training and capability development over the reporting period. In July 2014, a new Training Branch was established and resourcing was increased to better service the training needs of ASIO's growing workforce and to address the challenges inherent in its operating and security environments.

Further, in November 2014, the Director-General commissioned a review of ASIO's training needs to ensure that ASIO officers are well positioned to serve the needs of the government and the nation. The results of this detailed review have informed ASIO's training over the final quarter of the reporting period and will continue to provide overarching direction into 2015–16.

There was also greater focus on enhancing existing partnerships with close national and international partners to deliver mutual training benefits and ensure best practice through benchmarking.

In recognition of the significance of ASIO's technical capabilities to achieving its intelligence mission, ASIO now offers a Technical Officer Graduate Program. It includes placements in a range of technical areas within ASIO's Technical Capabilities Division, including software development, technical development, telecommunications, computer forensics and technical operations.

Legislation and litigation

During the reporting period ASIO played a key role in the development of legislation in collaboration with the Attorney-General's Department (AGD) and other agencies. This legislative reform is an important step in ensuring that ASIO's legislative framework adequately equips and assists it to perform its statutory mandate in a rapidly changing threat environment.

To assist with the implementation of these legislative reforms a range of work was undertaken including internal training, policy formulation, development of internal fact sheets and frequently asked questions, updating existing warrant templates and the establishment of new warrant templates.

Security of ASIO

Strong personnel, physical, information and IT security are fundamental to the secure and effective conduct of ASIO operations and investigations. A range of governance, policy and technological mechanisms act to protect the information, people and business systems necessary to deliver ASIO's mission—to identify and investigate threats to security and provide advice to protect Australia, its people and its interests.

ASIO works closely with other agencies to support the Australian Government's defensive posture against the malicious insider threat. ASIO uses the HARM (Human Capital, Access, Resources, Manage Risk) approach and is focussing on the following four key areas:

- translating our investigative, analytical and personnel security assessment experience into new policy initiatives;
- development of malicious insider threat product for dissemination across government;
- targeted malicious insider threat briefings for key Australian Government agencies; and
- developing a range of targeted outreach activities to industry and government through the ASIO Business and Government Liaison Unit and the Contact Reporting Scheme (CRS).

HARM emphasises the importance of not only understanding the threat, but managing the resultant risk.

Management of relationships and public reporting

ASIO engages with the government and business sectors and the Australian public. While ASIO's outreach is often in respect of the provision of classified security-related advice, ASIO also delivers public information in order to enhance awareness of the work of the Organisation and the threat environment.

Under Attorney-General authority, ASIO engages with, and receives support from, a number of international partners. While international partnerships have always been important in the performance of ASIO's functions, the complexity of the 'foreign fighters' issue has made cooperation with foreign security and intelligence agencies even more critical. As a consequence, ASIO expanded its overseas liaison network during the reporting period.

ASIO operates under a strict legislative regime and is overseen by comprehensive oversight and accountability mechanisms to provide public reassurance of the legality and proprietary of ASIO's actions. These include the Attorney-General, parliamentary committees, the Inspector General of Intelligence and Security, the Australian National Audit Office, the Independent National Security Legislation Monitor and the Independent Reviewer of Adverse Security Assessments.

Scope of the review

ASIO's submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review into Administration and Expenditure No. 14 provides a detailed account of ASIO's activities during the financial year 2014–15. The PJCIS wrote to ASIO requesting a submission covering all aspects of administration including:

- Strategic direction and priorities;
- Legislative changes that have 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;
- 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.

The Committee is also seeking to examine the impact of changed recruitment practices and vetting processes on matters within the scope of its review.

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.

'Security' is defined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) 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 and outlook

Australia continues to confront a broad range of security challenges, particularly in its countering terrorism and countering espionage effort. While terrorism is the most obvious and immediate challenge—posing a direct and ongoing threat to the safety and wellbeing of Australians—espionage and foreign interference directed against Australia by foreign powers also presents a first order challenge. The harm caused by hostile intelligence activity can undermine Australia's national security and sovereignty, damage Australia's international reputation and relationships, degrade our diplomatic and trade relations, inflict substantial economic damage, degrade or compromise nationally vital assets and critical infrastructure, and threaten the safety of Australian nationals. Foreign interference in Australia by foreign powers is pervasive. It spans community groups, business and social associations and is directed against all levels of the Australian government and the community.

While events, people and organisations overseas remain a factor for almost all security threats, in the counter-terrorism context these are increasingly finding expression through the actions of individuals without close or direct links to the overseas drivers. We continue to identify and investigate Islamist extremists in Australia who support or are engaged in terrorism-related activities, both here and overseas. Our investigations include groups and individuals who adhere to an extreme interpretation of Islam and whose ideologies have the potential to manifest in an onshore terrorist attack.

The conflict in Syria and Iraq continues to resonate strongly amongst those in Australia susceptible to the broad Islamist extremist narrative and to extremist messaging. A new generation of Islamist extremists has formed and the activities of these individuals will impact the Australian security environment for years to come; we are particularly concerned about the emerging threat from an increasingly young and volatile cohort of terrorist sympathisers and supporters in Australia.

Symbols of government, including the military, police and security agencies remain targets of choice. However, a random attack against a public mass gathering or member of the public would align with terrorist targeting objectives and, regardless of scale, would have significant impact. Lone actors or small groups of like-minded individuals could mount such an attack without intelligence forewarning; this scenario represents a significant challenge to security and law enforcement agencies and threats emanating from such individuals may develop quickly, especially if the intended act requires minimal preparation.

Terrorism

The principal threat to Australia, Australians and Australian interests continues to come from those who adhere to a violent Islamist extremist ideology. The groups espousing violent extremism share the view that Western countries, including Australia, are enemies of Islam and that attacks against the citizens and interests of those countries are not only legitimate but also obligatory.

The challenge to Australia's domestic security and our interests abroad from politically motivated violence has increased markedly over the past two years. We now allocate the bulk of our resources to counter-terrorism activities, with most effort against individuals and groups subscribing to an Islamist extremist ideology. The outlook is not positive.

Indications are that we will continue to see an increase over the next twelve months in the number of people supporting a violent extremist ideology including to the extent of committing acts of terrorism and this trend will continue into the foreseeable future. We expect that individuals will continue to be attracted to violent extremism from a larger pool of supporters and sympathisers. These people will be of the view that Australia is an enemy and a legitimate target for attack.

Acknowledging the changing environment, the Director-General of Security, on 12 September 2014, increased Australia's general terrorism threat level to High, meaning a terrorist attack was assessed as likely. The same day, based on that revised threat level, the Australian Government increased the Terrorism Public Alert Level from Medium to High.

The raising of the general terrorism threat level took into account a range of factors, including:

- an increase in the number of Australians who are adopting a violent Islamist extremist ideology and are willing to use violence in support of this ideology;
- the unprecedented number of individuals in Australia with a desire to join terrorist groups in the conflict zone in Syria and Iraq but who have been prevented from doing so;
- the potential threat posed by Australians returning from the conflict with training and experience in the use of violence;
- the global influence of extremists in Syria and Iraq and the reach of their terrorist propaganda advocating attacks against the West—a message that continues to resonate with some individuals in Australia; and
- the change in preferred attack methodology to favour low-capability terrorist attacks, with the associated substantial reduction in capability that would-be attackers require and increased difficulty for authorities in obtaining forewarning and preventing attacks—demonstrated by the spike in successful low-capability terrorist attacks in the West, including in Australia, throughout the past twelve months.

Subsequent to the threat level and Public Alert Level being raised, three terrorist attacks occurred in Australia—two inside the reporting period and one since—and six terrorist plots have been disrupted.

- The first attack took place in Melbourne on 23 September 2014, when Ahmad Numan Haider stabbed two uniformed police officers outside the Endeavour Hills police station; in addition to the injuries sustained by the two police officers, Haider died in response to the attack.
- The second attack occurred in Sydney on 15–16 December 2014, when Mohammad Hassan Manteghi (also known as Man Haron Monis) took 17 people hostage inside the Lindt café in Martin Place, resulting in the deaths of hostages Katrina Dawson and Tori Johnson, as well as Manteghi.
- The third attack occurred in Sydney on 2 October 2015 (outside the reporting period), when New South Wales (NSW) police civilian employee Curtis Cheng was fatally shot, at close range as he was leaving the NSW police headquarters in Parramatta, by 15-year-old Farhad Jabar Khalil Mohammad, who himself was subsequently shot and killed by NSW Police Force Special Constables responding to the attack.

The new **National Terrorism Threat Advisory System** was launched on 26 November 2015, to better inform the public about the likelihood of a terrorist attack in Australia. Under the new system the new terrorism threat level for Australia is PROBABLE – *credible intelligence, assessed to represent a plausible scenario, indicates intention and capability to conduct an attack in Australia*.

The new system has not been established in response to a specific threat, but has been designed to reflect the modern terrorism environment facing Australia. Information on the national terrorism threat level, including public advice on the nature of the threat and what it means for all Australians, is available online at www.nationalsecurity.gov.au

Many individuals who subscribe to Islamist extremism are motivated by a sense of alienation from mainstream society, a feeling that they are treated unjustly (overseas and at home) and, in some cases, demonstrate a proclivity to violence. There are a range of social factors that motivate individuals—and these vary on a case by case basis. These factors are not dissimilar to those that motivate people to other criminal and anti-social behaviour. In this case, however, the Islamist extremist narrative not only fills a void, but provides the 'justification' for terrorism. The Islamist extremist narrative provides answers to questions in the form of an easy to understand and culturally familiar explanation of why the world is as it is, and a religious justification to address these problems.

The key elements of the narrative include:

- Islam and the West are at war;
- the West has double standards in its treatment of Muslims; and
- the destiny of Islam is to rule the world which is being thwarted by the West and apostate Muslims.

The declaration by the Islamic State of Iraq and the Levant (ISIL) of a caliphate in June 2014 has provided a strong impetus to this narrative, levying an obligation on Muslims who are able to migrate to the Caliphate and, for all other supporters, to conduct jihad wherever they reside.

The number of Australians participating in the conflict in Syria and Iraq increased across the reporting period. At the end of June 2015, ASIO was investigating around 120 Australians directly participating in the conflict—a significant increase from the previous reporting period. Most were involved with either ISIL or the Syria-based, al-Qa'ida-linked group Jabhat alNusra. During the reporting period, two Australians undertook suicide attacks in the conflict.

ASIO worked with local and overseas partners to disrupt the travel of would-be extremists, with travel mostly but not entirely related to the conflict in Syria and Iraq. The disruption of travel through such means as passport cancellations or refusals is one way Australia meets its international obligation not to export terrorism. Disruption of travel also limits Australian violent extremists' exposure to, and experience of, terrorism overseas, and this can contain their capability and commitment. In 2014–15, legislation was passed allowing ASIO to recommend the temporary suspension of Australian passports and the temporary seizure of foreign travel documents; this power came into force on 1 December 2014.

ASIO recommended the cancellation or refusal of the Australian passports of 93 Australians during the reporting period. The overwhelming majority of these assessments related to the conflict in Syria and Iraq.

Social media has become very important providing easy, anytime, anywhere access to material and connecting extremists globally. In this environment, radicalisation can occur relatively quickly—frequently enabled by social media. Radicalisation and extremism are no longer necessarily centred on mosques or similar facilities or on known extremist groups or networks, and individuals on the periphery of groups are being more readily and rapidly drawn in. Although still a minority, more women are becoming involved.

Past experience suggests returnees from the current conflict will present a long-term security issue and some will pose a direct threat to Australian interests both here and overseas. In addition to this, some of those Australians who have been prevented, through passport cancellations or other prevention measures, from travelling to the conflict in Syria and Iraq also pose an onshore threat. Some of these thwarted travellers have transferred their focus to onshore activities in support of violent extremist groups in Syria and Iraq—especially ISIL and Jabhat al-Nusra— acting as radicalisers, recruiters and facilitators. A persistent risk is that these individuals will refocus their commitment to violent extremism into planning an attack in Australia, especially if they exhaust their options for travel. Multiple ASIO investigations include individuals with cancelled or refused passports who are still seeking to travel via alternate means (with some lodging new applications for Australian passports, some applying for non-Australian travel documents, and some looking for other options to circumvent Australia's border controls), and some are expected to translate this commitment to onshore attack planning if they decide they have no prospect of departing. Already ASIO has seen that some thwarted travellers have considered undertaking attacks at home using simple weapons and tactics.

Since the threat level was raised in September 2014, nine Australians, whose access to travel documents had been removed to prevent their travel to join the conflict in Syria and Iraq, have been identified as significantly involved in subsequent onshore attack plans which were disrupted when they were searched, arrested or placed under control orders.

While the more likely scenario for any attack in Australia is a low-capability attack against a 'soft' target, perpetrated by a lone actor or a small group—as seen in the three terrorist attacks in Australia since September 2014—the threat of a complex attack, such as a coordinated mass shooting or a large, sophisticated explosive device, also persists.

The security challenges described above are not exclusive to Australia and similar threats are mirrored globally, posing not just a threat to those overseas nations but also to Australian interests in those countries. Terrorist attacks linked to the conflict in Syria and Iraq have been seen in North America, Europe, the Middle East and Asia. Of particular concern to Australia's security interests and our region are the growing links between ISIL and extremists in South-East Asia.

Espionage and clandestine foreign interference

While the impact of clandestine foreign interference activity and espionage against Australia and Australian interests might not be as apparent to the community as that of terrorism, it is occurring on a large scale and has the potential to seriously harm our national interests. The perpetrators are utilising techniques and capabilities—including human intelligence, technical collection methods and exploitation of the internet and information technology—to target strategically important Australian interests. ASIO uses a three-pronged approach to manage the threat presented by the hostile activities of foreign intelligence services:

- to discover the most harmful clandestine activity;
- to degrade its adverse impact on Australia; and
- to defend against future harmful clandestine activity, including by contributing to security policies and practices.

There is an enduring requirement for ASIO to allocate substantial resources to defensive outreach and advice to heighten awareness of the threat environment and to drive appropriate security policy responses. ASIO is working with other government agencies and the private sector to build awareness of the potential harm of the espionage threat to Australia from hostile entities.

ASIO looks at the espionage and foreign interference threat through the concept of H.A.R.M—Human capital (H), access (A), resources (R) and managing the risk (M).

- Foreign intelligence services target people (human capital) who have access to the resources they are interested in, or in an effort to covertly influence them and their activities.
- Foreign intelligence services seek to generate access to restricted or compartmentalised areas and information.
- Foreign intelligence services seek to obtain resources not publicly available to enhance their strategic objectives.

The risk posed by self-motivated individuals who exploit their access to classified or privileged information is another threat to Australia's national interests. ASIO identified vulnerabilities with current Australian personnel security arrangements and in recognition of these participated in a review, contributing to the reforms by sharing both our investigative and personnel security assessments experience as well as that of our allied partners.

ASIO works closely with the Treasury, and other government agencies, in relation to specific foreign investment applications which could be contrary to Australia's national security. The Treasury may request ASIO advice to ensure foreign acquisitions are consistent with Australia's national interest, including assessing the impact on Australia's national security. ASIO also advises the government on national security threats associated with foreign investment proposals which are exempt from the FIRB process, which ensures private investors in Australian critical infrastructure also meet Australia's rigorous national security requirements.

ASIO continues to play a significant role in the area of cyber security. Cyber espionage is attractive to foreign powers because it has the potential to provide access to large aggregations of valuable information. Through the Australian Cyber Security Centre (ASCS), including the Australian Signals Directorate and the Computer Emergency Response Team in the Attorney-General's Department, ASIO continues to promote awareness of, and defensive responses to, the increasing threat from hostile cyber activity.

Communal violence and violent protest

ASIO investigates protest activity only 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 *Australian Security Intelligence Organisation Act 1979*. During 2014–15 protests in Australia were mostly peaceful.

Anti-Islam groups, whose activities were previously mostly limited to online posts and occasional inflammatory publicity stunts, began to attract increased numbers to real-world events, such as the Reclaim Australia rallies and the Stop the Mosque protests. The reporting period saw a number of well-attended, coordinated Australia-wide protests with an overt anti-Islam and anti-immigration message; these protests attracted large numbers of supporters and counter-protesters.

In January 2015, members of Sydney's Muslim community and their supporters gathered in a peaceful 'We will not abandon our Prophet' rally organised by Hizb ut-Tahrir, at Sydney's Lakemba train station. The event was held in response to perceptions of anti-Islam sentiment following the terrorist attack on the *Charlie Hebdo* office in Paris. While the event was vocal, it passed without major incident.

While some overseas Group of Twenty (G20) meetings have been marred by widespread violence and property damage during anti-globalisation and anti-capitalism protests, Australia's G20 hosting commitment—which culminated in the Brisbane Leaders Summit in November 2014—concluded without incident. ASIO assisted the whole-of-government effort through tailored intelligence collection and reporting, the provision of protective security advice to the G20 Taskforce, and the security checking of individuals seeking G20 accreditation. This assistance was aimed at providing forewarning of any potential security-related issues at G20 events and at mitigating any potential threats.

Border integrity

ASIO continues to contribute to whole-of-government strategies to disrupt and deter people smugglers. The number of people -smuggling ventures and illegal maritime arrivals during the reporting period was very low. However, the security environment continues to evolve so that existing and new 'push' factors for illegal travel to Australia will motivate both people smugglers and illegal immigrants to consider the risk.

ASIO works closely with the Department of Immigration and Border Protection (DIBP) to meet DIBP and broader government priorities in respect of visa security assessments. In 2015–16 ASIO will receive referrals of a proportion of the 30,000 IMAs currently in the community. ASIO's efforts to meet the visa security assessment requirements for the additional Syrian–Iraqi refugees is expected to impact capacity to meet other visa security assessment priorities, including the IMA caseload.

Outlook for the security environment

Australia remains a terrorist target, and Islamist extremism remains the principal terrorist threat in Australia. We will continue to see terrorist attack planning in Australia into the foreseeable future. The underlying factors that contributed to the September 2014 increase in the national terrorism threat level for Australia are not improving. Since the level was raised, we have seen three attacks and six disrupted plots in Australia. These onshore incidents coincide with a spike in attacks in the West—the majority directed, influenced or inspired by Islamic State of Iraq and the Levant (ISIL)—most bearing stark similarities to incidents in Australia. While our main concern remains low-capability attacks by lone actors or small groups inspired by ISIL, we cannot dismiss the threat of a spectacular attack by a transnational terrorist group such as one of the al-Qa'ida affiliates. However, an attack of this type is less likely in the current environment.

Foreign powers will continue to undertake a range of activities—some clandestine and others overt—against Australia's interests here and overseas. Foreign intelligence services pose a persistent and increasing challenge to the security of Australia. The challenge increases as the aggressors acquire new technologies and glean more information from the Edward Snowden disclosures. ASIO is continuing to increase its efforts to counter foreign clandestine activity and insider threats. The more work undertaken to counter these activities, the more hostile activities—by a range of actors—are identified. As our understanding has grown, so too has our comprehension of the security vulnerabilities inherent in government and bureaucracy. Consequently, ASIO is working closely with government, bureaucracies and the private sector to drive security reform and resilience building.

With new and evolving global tensions the 'push' factors for illegal travel to Australia will motivate some potential illegal immigrants to consider the risk and expense of an illegal maritime venture to be worthwhile. Planning of illegal ventures continues to be undertaken by committed and capable people smugglers. Prolific and experienced people smugglers are resilient and adaptable, seizing upon perceived changes to Australia's approach to illegal maritime travel policy that could reinvigorate demand.

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 2014–15 ASIO received an appropriation of $368.4 million which included $11.2 million of additional funding relating to the 'Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat' measure announced by the Australian Government in August 2015. ASIO's budget, which includes a significant, non-discretionary component associated with the need to maintain high levels of security, has been under considerable pressure in recent years. The budget continues to be a challenge due to the impact of the increased security overlay costs, efficiency dividend and expenditure ASIO absorbs which includes security assessments relating to Illegal Maritime Arrivals (IMAs), costs associated with Operation Sovereign Borders and Data Retention. Additionally, ASIO will contribute to the National Security Hotline Campaign as well as savings measures required by government due to the budget savings measures.

Looking forward over the next four years, through the 'Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat' measure, ASIO will receive a further $128.5 million in operating funding and $41.4 million in capital to continue to strengthen ASIO's counter-terrorism capabilities. During this time ASIO will return around $93.7 million to government through the efficiency dividend and other savings measures ($65.9 million in efficiency dividend and $27.8 million on other savings measures or absorbed costs).

Financial performance

ASIO recorded an operating loss of $12.7 million, when depreciation is excluded. Depreciation costs were $63.8 million which creates an operating deficit of $76.5 million as ASIO does not receive funding for depreciation. This is in line with reporting of most other agencies due to the way depreciation is funded and reported.

Figure 1: Revenue from government

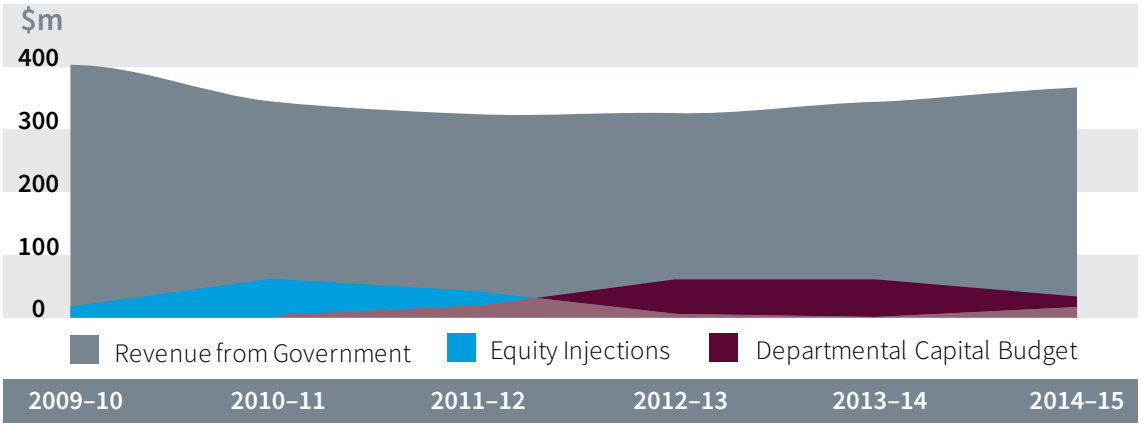
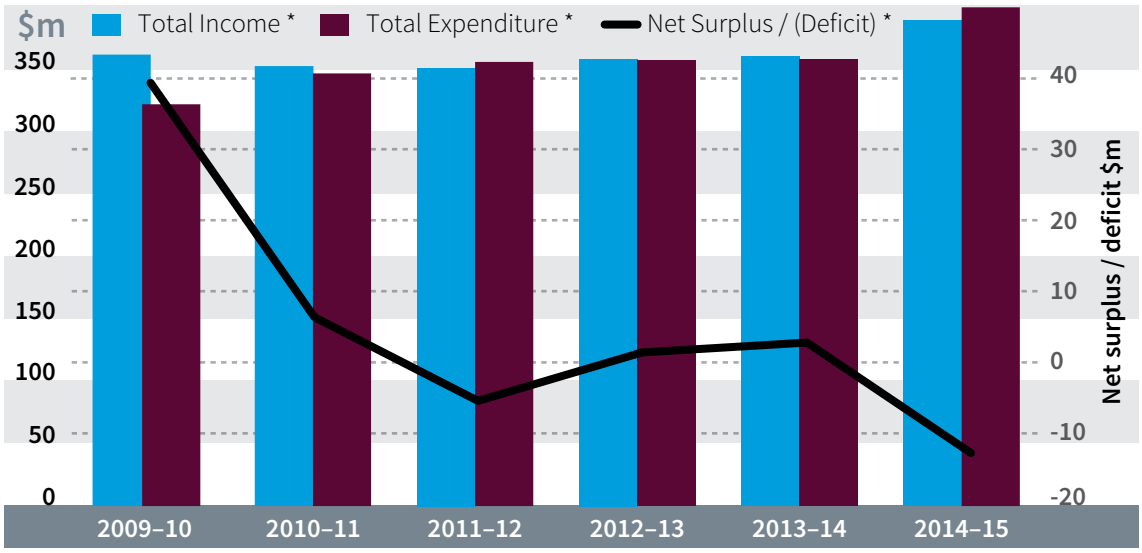


Figure 2: Financial Performance



Strategic allocation of resources

The Organisation's strategic direction is set by ASIO's Executive Board and is reflected in the allocation of resources across ASIO's activities. The Executive Board also ensures the Organisation's budget and resource allocation is aligned with organisational priorities, reviewing project proposals submitted through the Finance Committee.

In 2014–15 ASIO continued to focus across the core operational fields. Operational-related expenditure accounted for 81 per cent of ASIO's budget.
The terrorism threat environment in Australia has deteriorated in the last twelve months which is putting pressure on ASIO's counter-terrorism and technical capabilities, despite the injection of additional funds. The nation also faces a significant threat from foreign espionage and interference.
At the same time the work of intelligence agencies is becoming more complex, time consuming and risky as a result of the rapidly evolving technological environment and changes in the behaviour of intelligence targets.

Figure 3: Resource allocation

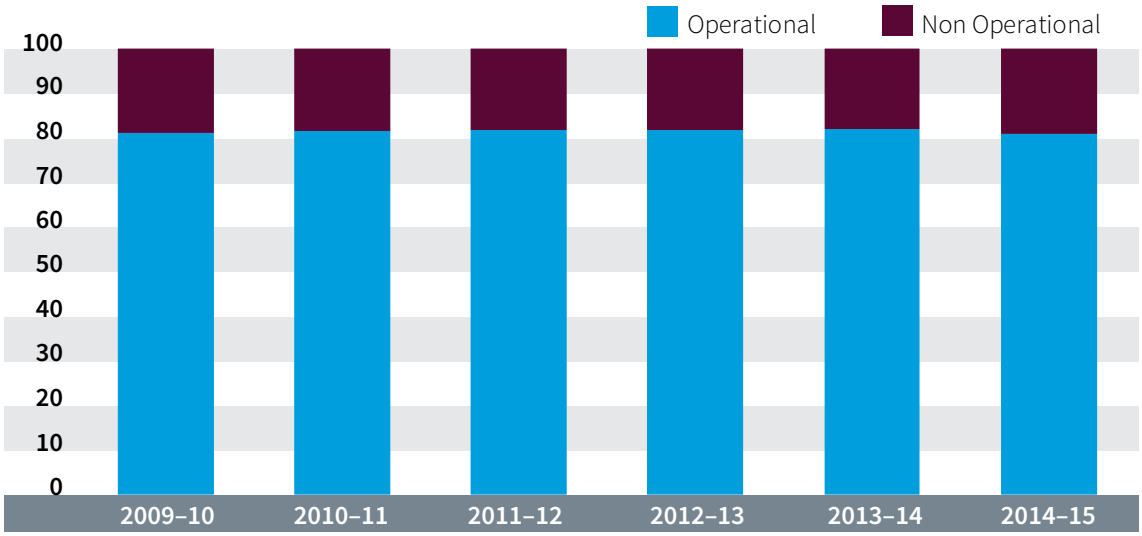
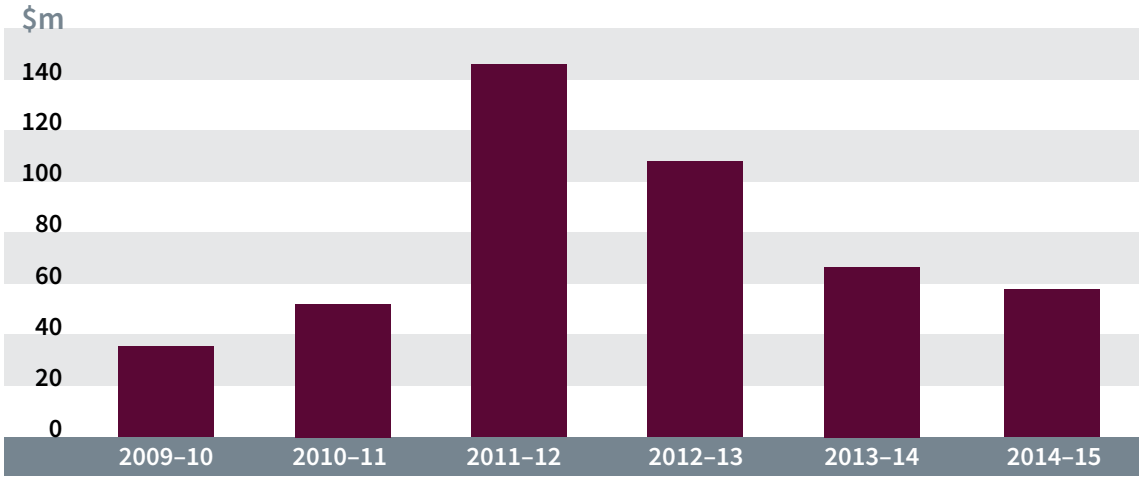


Figure 4: Purchase of Capital



Financial management and internal controls

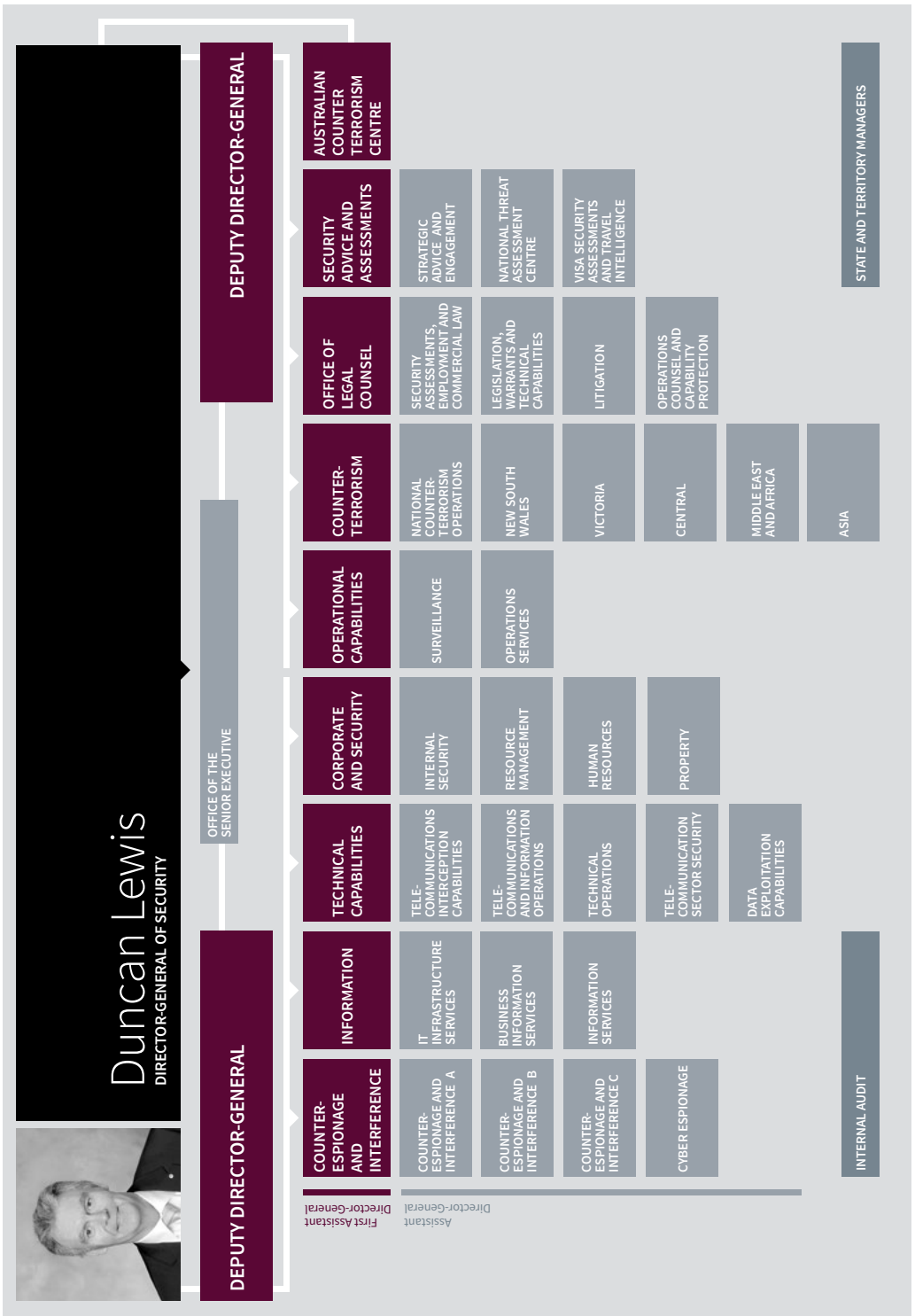
ASIO prepares annual financial statements in accordance with the provisions in subsection 42(2) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the *Financial Reporting Rules*. ASIO's financial statements are audited by the Australian National Audit Office (ANAO). As part of that process, the ANAO conducts an annual examination of the internal systems and key financial controls of the Organisation. In 2014–15 ASIO did not receive any adverse audit qualifications from the ANAO as part of its independent audit reporting to Parliament.

Internally, the Chief Finance Officer reports monthly to the ASIO Executive Board. Reporting covers current and future organisational financial performance matters and strategic financial management planning. Financial management practices are supported by a financial management information system with integrated internal controls aligned to the Organisation's financial framework. ASIO's Audit and Risk Committee also receives quarterly briefings from the Chief Finance Officer, in support of the committee's role to provide independent assurance and advice on design, operation and performance of ASIO's internal governance, risk and control framework.

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

Structure of the Organisation

Figure 5: Organisational structure



Corporate direction and strategic planning

ASIO Strategic Plan 2013–16

ASIO's Strategic Plan 2013–16 ensures the organisation's activities are directed against identified priorities for the period. It positions ASIO to respond with agility and remain resilient in an evolving threat environment. In 2014–15, ASIO focused on the two following goals:

- 'We manage risk in a constantly evolving security environment'— The evolving security environment has made it necessary for ASIO to be an adaptive organisation: efficiently identifying key risks and translating these into actionable work programs that are evaluated for effect. This evolution in the security threat environment has resulted in changes to the legislative foundation upon which ASIO operates.
- 'Attract, develop and retain a professional and highly competent workforce'—In response to the New Policy Proposal funding received during the reporting period, ASIO has committed additional resources to effectively recruit new talent. Maintaining a security-cleared and professional workforce is a great challenge; expanding that workforce is an even greater challenge.

Corporate governance

The Director-General of Security is responsible for ensuring that ASIO achieves its mission: to identify and investigate threats to security and provide advice to protect Australia, its people and its interests. ASIO's corporate governance framework provides information and advice to support the Director-General in his responsibilities.

During the reporting period and consistent with ASIO's new risk management policy and the requirements of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), ASIO committees changed the way they consider and manage risk.

ASIO has a range of corporate committees to support the leadership and decision making of the Director-General. ASIO's governance arrangements encompass the practices, policies and procedures established to:

- set strategic direction—identifying goals and priorities;
- plan and allocate—resources according to goals and priorities; and
- monitor and report—ensuring that ASIO is delivering its outcomes effectively and with accountability.

ASIO Executive Board

The Executive Board (the Board) comprises the Director-General of Security, the Deputy Directors-General and an external member. Up until May 2015, Ms Jenet Connell, a highly experienced and distinguished public servant serving at the time as the Chief Operating Officer of the Department of Finance, was the Board's external member. Mr John Lonsdale, Chief Operating Officer of the Department of the Treasury, has since taken on the role. The Australian National Audit Office (ANAO) reviews the outcomes of the Board as part of its governance audit.

The Board:

- leads strategic direction and planning;
- determines ASIO's overall organisational priorities and the alignment of resource allocation and investment activities with those priorities;
- leads ASIO's activities and performance in the delivery of its four key programs: security intelligence analysis and advice, protective security advice, security intelligence investigations and capabilities and foreign intelligence collection;
- provides oversight of ASIO's risk management policies, including the identification and treatment of key strategic risks to the Organisation; and
- ensures that ASIO's internal security measures are robust and appropriate to the needs of a security intelligence organisation.

The Board is responsible for:

- ensuring the success of ASIO through its executive management team and within the broad strategic directions set through its governance framework, including by the Minister;
- the overall development of ASIO's security intelligence capabilities and the skills and adaptability of ASIO's people;
- the establishment of ASIO Corporate Committees to support, as delegated, the Director-General's powers, functions or duties under or for the purposes of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act);
- ASIO's accountability framework and policies and procedures providing a high level of accountability, professionalism and the effective conduct of ASIO business; and
- ASIO meeting the requirements of its oversight bodies.

Over the reporting period, the Board received regular reporting and submissions from ASIO's Corporate Committees on corporate, workforce and security outcomes and issues, the Organisation's budget, the counter-terrorism new policy proposal, and risks.

Intelligence Coordination Committee

The Intelligence Coordination Committee (ICC) provides strategic direction and ensures effective coordination of ASIO's investigative and assessment priorities, allocating resources to these priorities on a risk management basis. The ICC provides strategic direction, manages risk, coordinates effort and evaluates performance in support of ASIO's mission and corporate governance arrangements.

The ICC approaches its responsibilities by dividing ASIO's work into thematic work programs, including:

- countering terrorism and the promotion of communal violence;
- countering espionage, foreign interference and malicious insiders;
- countering serious threats to Australia's border integrity; and
- security intelligence capabilities.

The ICC is chaired by a Deputy Director-General and is comprised of SES Band 2 and 3 representatives from across ASIO's structure.

Workforce Capability Committee

The Workforce Capability Committee (WCC) considers matters relevant to the size, skill set and accommodation of ASIO's workforce. It also provides reporting to ASIO's Executive Board on the performance of ASIO's recruitment, internal transfer and training programs. The Committee is chaired by a Deputy Director-General. A subcommittee of the WCC is the Work Health and Safety Committee, which is responsible for ensuring better health and safety policies and practices across ASIO.

Over the reporting period, the WCC oversaw: the progress of recruitment activities to increase ASIO's capacity in relation to the counter-terrorism New Policy Proposal; a review of ASIO's language capabilities; results from the ASIO staff survey; and policy changes in relation to internal transfer processes. The WCC reported to the Executive Board on the external and internal recruitment outcomes against the New Policy Proposal recruitment targets.

ASIO Security Committee

The ASIO Security Committee (ASC) reviews and addresses key issues relevant to the security of ASIO people, property, operational activities and information technology systems to ensure that they are continually evaluated in line with the security environment. The ASC reports directly to the Executive Board, providing assurance of sound and secure practices in ASIO. It also approves security policy and procedures and reviews ASIO's compliance in meeting legislative and policy responsibilities specific to Australian Government mandatory standards.

Finance Committee

ASIO's Finance Committee provides advice and makes recommendations to the ASIO Executive Board on resource allocation, and financial management and strategy.

The core Finance Committee responsibilities are:

- reviewing ASIO's operating budget, asset replacement activities and the ASIO Investment Program; and
- providing strategic advice, including future budget management strategies, to the Executive Board.

Two significant issues during 2014–15 were the injection of operating and capital funds associated with the counter-terrorism New Policy Proposal; and financial implications as the Ben Chifley Building became occupied and neared completion.

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 ASIO's financial and performance reporting responsibilities, risk oversight and management, and system of internal control.

Members of the Committee, including the Chair, are appointed for an initial period not exceeding three years. The Chair of the Audit and Risk Committee, Ms Lynelle Briggs AO, was appointed by the Director-General on 6 February 2012, and her tenure was extended on 11 February 2015 for a further twelve months. In 2014–15, the independence of the Committee was strengthened through the inclusion of a third external member, Australian Secret Intelligence Service (ASIS) Deputy Director-General, Capability and Corporate Management. Over the reporting period, six ASIO officers and three external members served as committee members; the Committee currently comprises three ASIO officers and three independent members.

In 2014 the Committee oversaw the rapid maturation of ASIO's Enterprise Risk Management Framework and began reviewing enterprise risk reporting from the other ASIO governance committees for risks requiring Executive Board attention.

The Committee considered all audits undertaken by ASIO's Internal Audit Directorate during the period and monitored and reviewed ASIO's response and action against recommendations. It also reviewed ASIO's response and action in relation to any significant issues raised in external audit and review reports and better practice guides.

ASIO has reviewed its internal audit function and is moving towards an integrated assurance model, which will increase and improve the level of assurance provided to the Committee and ASIO's Executive Board. The approach builds upon ASIO's risk framework and combines the internal audit function with other evaluation roles and brings together relevant expertise, focus, increased staffing, and depth and breadth to ASIO's audit and evaluation capacity.

Audit and fraud

Fraud control

The ASIO Fraud Management Group comprises senior executive officers who oversee the management of fraud control arrangements and report to ASIO's Audit and Risk Committee. In the reporting period, no serious fraud allegations were referred to the Fraud Management Group for investigation, and both the Fraud Management Group and the Audit and Risk Committee were satisfied with how minor fraud matters were dealt with through alternative administrative or investigative processes.

The Audit and Risk Committee was satisfied ASIO has the appropriate processes in place to detect, capture and respond to the fraud risks identified in the fraud risk assessment undertaken in early 2013. In accordance with Commonwealth fraud control policy, the Committee will require ASIO to undertake another fraud risk assessment in 2015–16.

Fraud awareness training for all new employees and contractors continues to be provided in ASIO's induction training. ASIO also provides a mandatory e-learning training module on fraud awareness, which ASIO personnel must complete every three years. The module recently underwent substantial amendment to ensure it continues to be of benefit for ASIO staff and reflects changes in ASIO and Commonwealth policies.

Audit

ASIO's Internal Audit Directorate undertakes evaluations of all financial and non-financial policies and operations. Internal audits and evaluations may cover any of the programs or activities of ASIO, as provided for in legislation, relevant business agreements, memorandums of understanding or contracts.

In 2014–15 Internal Audit undertook six mandatory compliance audits into the access and use by ASIO personnel of other agency database information.

An audit was conducted into ASIO processes to ensure travel approvals are provided by the appropriate delegate and in accordance with Australian Government Policy Official International Travel— Approval and Use of the Best Fare of the Day. The audit found updates to ASIO's travel guidance met the requirements of the resource management guide but policy advice in this area required updating.

In the reporting period, an audit of ASIO's compliance with the *Public Governance, Performance and Accountability Act 2015* (PGPA Act) framework was undertaken to augment existing compliance activities. The objective of the audit was to assess the suitability of the systems, controls and reporting that ASIO is relying upon in determining compliance or non-compliance with the requirements of the PGPA Act framework. While the audit found there was scope for improvement in some areas, the results attested to the efforts of ASIO in adopting and complying with the legislative framework.

Internal Audit Directorate regularly monitored and sought updates from work areas on the implementation of agreed audit and evaluation recommendations. The Audit and Risk Committee, at its quarterly meetings, was kept abreast of the progress of the implementation of recommendations.

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 (SES) 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, which is recognised by the Attorney-General, was established to enable ASIO management and staff to meet regularly, in a structured way, to discuss and resolve issues of interest and concern. The ACC aims to establish clearer lines of communication between management and staff thereby contributing to more effective and responsive decision making.

Over the reporting period, the ACC reviewed and updated its charter and membership, discussed and resolved issues relating to the relocation of staff to the Ben Chifley Building and transitionary arrangements, received information on, and provided input into, the Organisation's efforts to comply with the Australian Government Employment Bargaining Framework, received feedback on the outcomes of the 2014 ASIO Staff Survey, and contributed to the review and development of numerous Human Resources policies and initiatives.

Human resource management

Recruitment & work force management

The funding received through the 'Enhance Security Intelligence Capabilities to Counter the Islamist Terrorism Threat' announced in August 2014 by the Australian Government saw a shift in ASIO's people strategy from a focus on reducing and consolidating, to one of expanding capabilities and growth. This change brings challenges in terms of recruitment, vetting and training.

In 2014–15 recruitment focussed on the difficult-to-fill roles of intelligence officers, technical officers and information and communications technology (ICT) positions.

The security-related requirements for ASIO employees increases the challenge of attracting suitable candidates. ASIO attended 20 university career fairs around the country and conducted information sessions for targeted disciplines at a number of universities. This direct engagement with university students promoted ASIO and its employment opportunities. It also provided the opportunity to explain the security-related requirements expected of applicants.

An online employment register was established during the reporting period, supported by a national recruitment awareness campaign. The register allows those interested in ongoing opportunities with ASIO to lodge their interest. As at 30 June 2015, over 4900 applications had been submitted. ASIO's expenditure on recruitment advertising for difficult-to-fill roles increased from $599 739 in 2013–14 to $871 902 in 2014–15, with both greater participation in university career fairs and the employment register national campaign contributing to the majority of the increase.

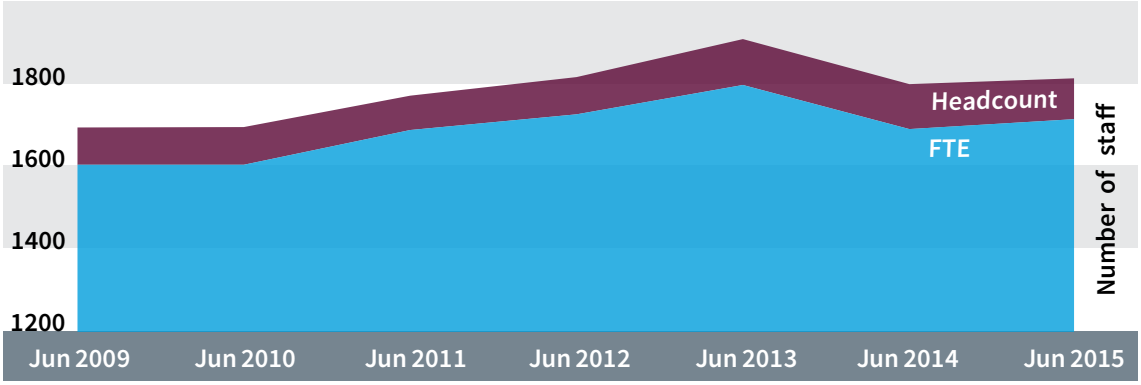
A recruitment agency panel was established during the reporting period as a key strategy to provide talent sourcing expertise, increase screening capacity and as part of improving the first phase of the recruitment process. Use of the panel is a significant investment by the Organisation, and a review at the end of 2014–15 identified greater efficiency and effectiveness with regard to recruiting technical and ICT candidates, and a substantial increase in capacity.

In 2014–15, a total of 153 recruitment activities were completed, including 73 technical and ICT activities. In contrast, 35 recruitment activities were completed in 2013–14 for the same job families. In 2014–15, 21 per cent of candidates for these job families were found suitable. By comparison in 2013–14, nine percent of candidates were found suitable.

When considering the total number of applicants found suitable across all job families in 2014–15 from an initial pool of 5462, there was a 28 per cent increase, with the total number increasing from 355 in 2013–14 to 455 in 2014–15.

The number of candidate withdrawals (prior to vetting) was also significantly lower, with 26 candidates in 2014–15 and 48 in 2013–14.

Figure 6: Staffing growth



The recruitment work undertaken has contributed towards all four goals in ASIO's Strategic Plan, particularly 'attracting, developing and retaining a professional and highly competent workforce'. ASIO continues to develop and refine programs and services that enable it to meet increasingly diverse and complex security challenges.

In October 2014 all ASIO employees were invited to participate in the biannual Staff Satisfaction Survey, with 62.3 per cent of staff submitting a response. The majority of respondents expressed positive views about working for ASIO, with results exceeding the outcomes from past surveys in many areas. Noteworthy results include:

- 95 per cent of respondents said they are proud to work for ASIO;
- 99 per cent said they were willing to assist ASIO meet its goals and objectives; 98 per cent of respondents said they support ASIO's mission and values, and 91 per cent of respondents said they have a clear understanding of how ASIO is achieving Government objectives; and
- 97 per cent of respondents said their colleagues uphold the Values and Code of Conduct and 95 per cent of respondents said their line manager upholds the Values and Code of Conduct.

Results also exceed Australian Public Service averages in several categories covered by the survey, including pride in working in the Organisation, work team culture and relationships, performance management, support for innovation, training and perceptions of leadership.

Throughout the reporting period, ASIO devoted extensive resources to the development of a submission to the Australian Public Service Commissioner seeking approval for ASIO's proposed bargaining position on terms and conditions of employment. The submission was prepared in accordance with the *Australian Government Public Sector Workplace Bargaining Policy*. ASIO continues to liaise with representatives of the Australian Public Service Commission to refine its submission and demonstrate that any proposed wage increase is both affordable and offset by genuine productivity improvements.

Training and development

ASIO invested heavily in its training and capability development over the reporting period. In July 2014, a new Training Branch was established and resourcing was increased to better service the training needs of ASIO's growing workforce and to address the challenges inherent in its operating and security environments.

Further, in November 2014, the Director-General commissioned a review of ASIO's training needs to ensure that ASIO officers are well positioned to serve the needs of the government and the nation. The results of this detailed review have informed ASIO's training over the final quarter of the reporting period and will continue to provide overarching direction into 2015–16.

There was also greater focus on enhancing existing partnerships with close national and international partners to deliver mutual training benefits and ensure best practice through benchmarking.

Intelligence training

The Intelligence Development Program (IDP) for new intelligence officers was remodelled in 2014, to provide an enhanced multifaceted program aimed at delivering 'job ready' graduates. The IDP is an intensive program delivered through classroom-based learning and practical exercises, with short-term placements in the workplace to solidify learning outcomes. It also includes a final three months of coaching and assessment on the job.

Two IDPs were completed in the reporting period. Over the same period, foundational intelligence training was also delivered to over 50 officers in either analytical or operational disciplines.

In recognition of the significance of ASIO's technical capabilities to achieving its intelligence mission, ASIO now offers a Technical Officer Graduate Program. This one-year structured program is aimed at university graduates. It includes placements in a range of technical areas within ASIO's Technical Capabilities Division, including software development, technical development, telecommunications, computer forensics and technical operations. Participants in this program will graduate in February 2016 and, given the success of this pilot program, the next Technical Officer Graduate Program will also commence in February 2016.

Significant focus was also given to refining current and developing advanced and specialised development opportunities for practising intelligence professionals. These initiatives are forward-looking and anticipatory in nature to ensure our officers are well positioned to meet both current and future challenges inherent in the Australian and international security environments. These include a range of joint training initiatives with close foreign partners, both onshore and offshore, to deliver mutual capability development outcomes.

Corporate Training

ASIO provides a range of training programs specific to an officer's role or Organisation-wide training. These training activities include an induction program for all new starters, administrative training, information technology training, and mandatory training to ensure all ASIO officers behave in accordance with the key principles and standards of ASIO and the Australian Public Service.

Mandatory training includes security awareness, ethics and accountability, public interest disclosure, work health and safety and workplace behavior.

In 2014–15, ASIO's new starter induction program was refreshed and remodelled to provide an effective introduction to ASIO's security intelligence role, security culture and practices, and a comprehensive understanding of ASIO's Values and Code of Conduct.

During the reporting period, ASIO approved 3426 instances of face-to-face training, attended by 1752 employees across 60 training courses. This represents more than double the instances of face-to-face training that occurred in the previous reporting period. Such face-to-face training includes management and leadership development (detailed below), corporate programs such as project management and financial management, personal safety and security training, and information technology courses.

Management and leadership development

Implementation of ASIO's Management and Leadership in Security Intelligence Strategy continued in 2014–15 (the strategy), including ASIO's shared-services approach to strengthening management and leadership capability across the Australian Intelligence Community (AIC). The strategy includes three primary pathway programs of which two are delivered together with AIC agency partners:

- Management Skills in ASIO Workshop—aimed at new or current supervisors and managers requiring foundational skills and/or knowledge refreshment at ASIO Employee (AE) 5–6 to ASIO Executive Employee (AEE) 3 levels (typically delivered 5 times per year);
- Introduction to Management Program—aimed at high-potential and aspiring frontline managers or new managers from the AE6 to AEE1 levels (typically delivered 3–4 times per year); and
- Mastering Management Program—aimed at high-potential and high-performing AEE2 employees (typically delivered 3–4 times per year).

In addition to the established pathway programs, ASIO has offered a range of further development opportunities to the graduates of the Introduction to Management Program and the Mastering Management Program to build on the learning outcomes for participants. These include participation in specialised leadership seminars and bespoke development opportunities including the Jawun Indigenous Community Australian Public Sector Secondment program.

ASIO's continuous evaluation processes have identified clear evidence that the Strategy's programs have had a positive impact across the Organisation. Participants highlighted the significant development of new knowledge and skills over time, a positive impact in the workplace by applying these skills, and an increase in sharing resources and heightened collaboration across agencies in the AIC.

Outside of the reporting period ASIO's strategy won the Australian Human Resources Institute (AHRI)—Rob Goffee Award for Leadership Development. This Award recognises outstanding leadership development initiatives, programs and strategies, implemented within an organisation in order to develop and encourage current and future leaders. ASIO's submission for the award was premised on the success of the strategy and our delivery of the associated training and development programs across the ASIO workforce detailed above.

Study support and language development programs

Over the reporting period, 10 per cent of ASIO staff received support to undertake study or language development. In 2014–15, 119 officers participated in ASIO-supported study programs, at a cost of $301 794. These programs included some 89 courses across a range of disciplines, including security and policy, conflict and strategic studies, business management, project management and information technology.

ASIO's Language Skills Development Program is aimed at building language capability, and ASIO employees are encouraged to apply for the program where relevant to their role. During the reporting period, ASIO spent $432 335 on language training for 46 employees across 15 languages, following 54 language development business cases.

e-learning

ASIO also conducted a review of its e-learning capability, resulting in the removal of obsolete modules and the republishing of in-house developed content, commencing with the mandatory training modules. Twelve new e-learning modules were published, including seven for personal safety and security and four relating to record-keeping, ensuring ASIO adheres to its obligations under relevant legislation. During the reporting period, ASIO recorded 3320 instances of mandatory and 1362 instances of nonmandatory e-learning completions.

National Intelligence Community training

The National Intelligence Community Training Secretariat (NICTS) is housed in the Ben Chifley Building, and is staffed and managed on a day-to-day basis by ASIO. The remit of the NICTS is to identify and deliver learning and development opportunities that promote and develop common understanding, cohesiveness and interconnectedness across the National Intelligence Community. ASIO also continues to actively contribute to NIC training programs as a presenter and a participant.

The NIC Training Committee provides the overarching strategic direction and guidance to the NICTS. The Committee is chaired on a rotating basis by a NIC senior officer and co-chaired by ASIO (Assistant Director-General of Training Branch).

ASIO also continues to work closely with the Australian National University's National Security College supporting its aim to enhance strategic understanding and critical thinking about Australia's national security. ASIO also regularly contributes presenters and participants for NSC programs.

Figure 8: Ratio of staff

Workforce

At the end of the reporting period ASIO had 49 Senior Executive Service officers, 499 AEO 1, 2 and 3 officers and 1281 other officers at APS1–6 equivalent.

Staff members engaged in operational and intelligence-focused functions (including Engineering and Technical, Intelligence and Security, Legal and Parliamentary) accounted for 68.6 per cent (1254 including attached officers) of the Organisation with 31.4 per cent (or 575) engaged in enabling functions (corporate, information management and public research).

Equity and diversity

For ASIO to operate effectively in the community it needs to have a workforce representative of that community.

ASIO's Director-General is an active member of the Heads of Intelligence Agency Meeting (HIAM). During 2014 HIAM initiated an investigation into the causes and implications of the existing gender imbalance across the AIC, noting that only 40 per cent of the AIC workforce is female, with the majority sitting within positions at the lower end of the organisational hierarchy. In ASIO 44 per cent of the workforce is female. While the Organisation has seen an increase in the number of women in Executive and Senior Executive roles, women continue to be most strongly represented in the APS (equivalent) level classifications.

To help inform this conversation and ensure an accurate understanding of the current situation, ASIO participated in an AIC-wide gender equity survey and facilitated follow-up focus groups with both male and female members of staff. In recognition of the importance of this issue and the extensive evidence demonstrating the link between a diverse and inclusive workforce and improved business performance, HIAM established a Gender Equity Steering Committee. Three members of ASIO's management team have been selected to represent ASIO on this committee and to lead the development and implementation of a Gender Equity Strategy. ASIO is currently focussed on developing a Gender Equity Strategy to consider gender issues specific to ASIO more closely.

Research has been completed in relation to identifying ASIO specific gender equity issues and the Executive Board is currently working with a view to finalising the Gender Equity Strategy by early 2016 to commence implementation in 2016. It is expected that ASIO will identify key metrics to monitor progress focussing on:

- culture change;
- strengthening capabilities; and
- flexible working arrangements.

Table 2: Diversity of ASIO's staff

Group	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)	49	16	0	0	1	49
Senior Officers [3]	499	186	18	2	6	499
AE6 [4]	652	327	56	3	7	641
AE5 [5]	346	180	17	0	2	346
AE1 – 4 [6]	167	84	12	2	1	162
Information Technology Officers Grades 1 and 2	107	16	6	2	3	107
Engineers Grades 1 and 2	9	0	0	0	0	9
Total	**1829**	**809**	**109**	**9**	**20**	**1813**

[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.

Figure 9: The gender breakdown of ASIO staff by classification level

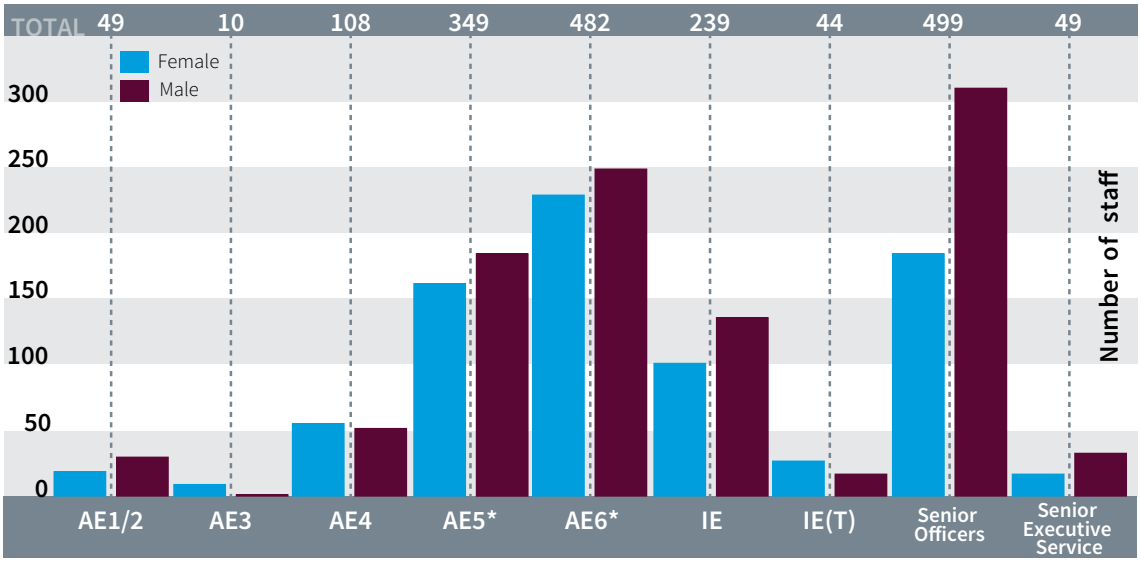


Figure 10: The age profile of ASIO staff

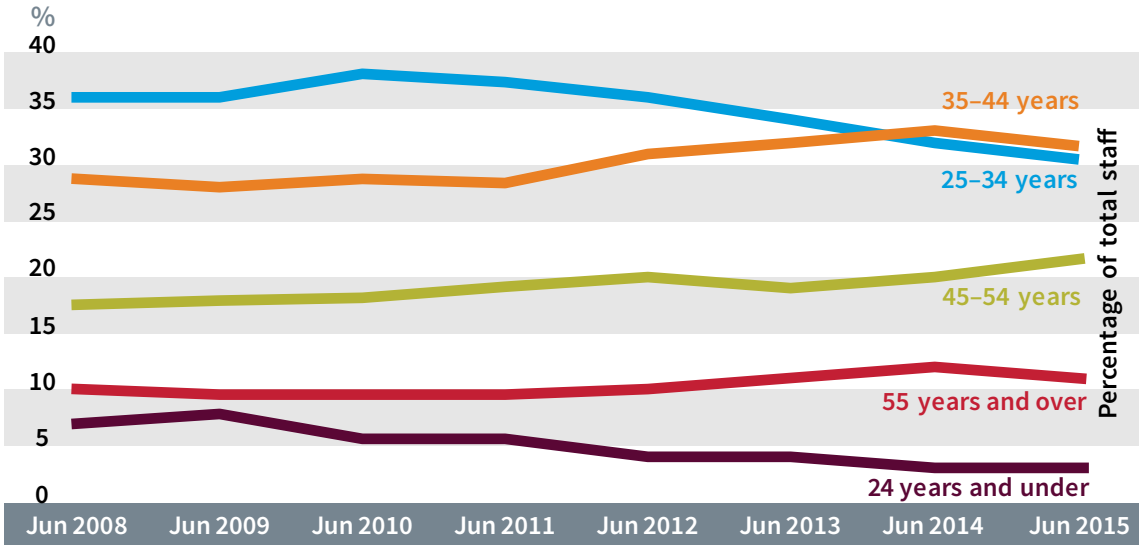
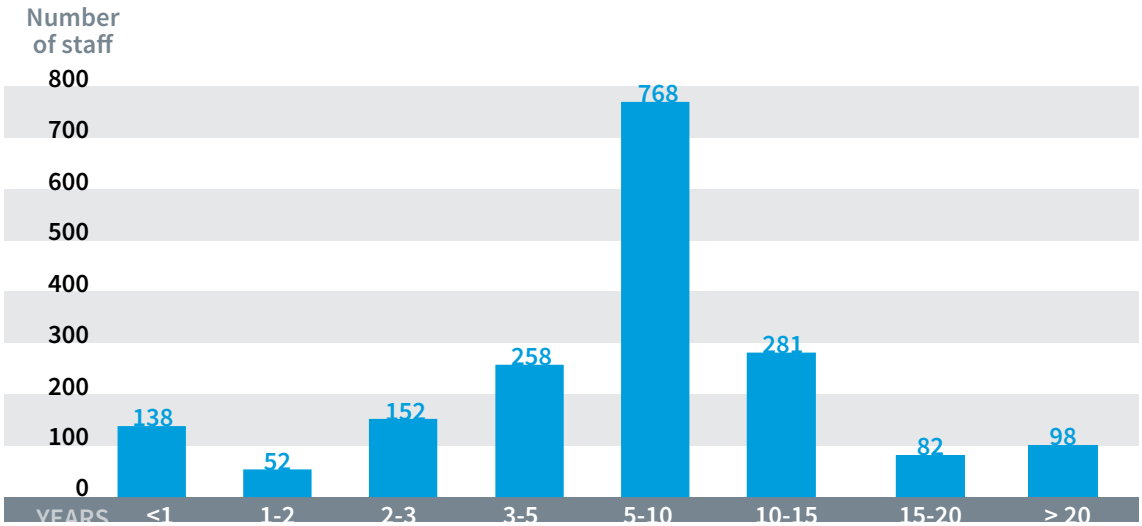


Figure 11: Staff length of service



Redundancies

In 2014–15 there were three voluntary redundancies, one AE6 employee and two Executive Level employees.

Separation Rates

During 2014–15 ASIO experienced a decrease in the separation rate from 7.68 per cent in 2013–14 to 4.81 per cent in 2014–15. The voluntary separation rate at 30 June 2015 (excluding voluntary redundancies) was 4.64 per cent.

Figure 12: Separation by reason

*Other includes Contract Expired, Deceased, Dismissed and Voluntary Redundancy

Attachments

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

- the Attorney-General's Department;
- the Australian Federal Police;
- the Australian Secret Intelligence Service;
- the Australian Geospatial-Intelligence Organisation;
- the Australian Signals Directorate;
- the Defence Intelligence Organisation;
- the Department of Foreign Affairs and Trade;
- the Department of Immigration and Border Protection;
- the Office of Transport Security, within the Department of Infrastructure and Regional Development;
- the Office of National Assessments;
- the Department of the Prime Minister and Cabinet;
- the Department of Human Services;
- the Department of the Treasury;
- the New South Wales Police Force;
- the Queensland Police Service;
- Victoria Police; and
- Western Australia Police.

Staffing and personal matters

A functional review of the role of the ASIO Ombudsman was undertaken during the reporting period to ensure the role met business requirements, supported employment legislation and provided adequate staff and management support. A limited tender was advertised in appointing the role to ensure it remains a position of impartiality.

The role of the ASIO Ombudsman will continue to include the provision of impartial and confidential services to staff and management. The position is a vehicle to address staff-related concerns through advice, consultation and mediation—and as a reporting mechanism to management on trends or themes to enable appropriate remedial action. The Ombudsman role also has some capacity to undertake complex formal investigations.

In 2014–15 the ASIO Ombudsman provided advice in relation to 35 general queries. It provided more substantial advice on nine occasions regarding performance, bullying and harassment.

The Ombudsman undertook four formal investigations: two investigations into allegations of inappropriate conduct in the workplace, one Public Interest Disclosure investigation, and one process inquiry into the advertising of internal job vacancies.

During this period, the ASIO Ombudsman provided input to a wide range of presentations relating to the role and the importance of the ASIO Values and Code of Conduct in establishing a proper and respectful workplace culture.

The Ombudsman continued to meet regularly with ASIO senior management and with representatives of the Staff Association to discuss the health of the workplace.

Public interest disclosure

The *Public Interest Disclosure Act 2013* (PID Act) enables all Commonwealth agencies to facilitate disclosure and investigate wrongdoing and maladministration in the Commonwealth public sector, including within ASIO.

For intelligence agencies, the PID Act works in conjunction with other legislation—such as the *ASIO Act*, the *Inspector-General of Intelligence and Security Act 1986, Intelligence Services Act 2001* and the *Crimes Act 1914*— to protect intelligence information and provides specific avenues for individuals to make a public interest disclosure involving intelligence information.

In the reporting period, three disclosures were received and allocated to an investigating authority. All three disclosures were completed, or allocated for investigation under another authority, within the required timeframes. The disclosure investigations found no findings of maladministration, wastage of public money or abuse of public trust, but cases did produce recommendations aimed at improving organisational communication, effectiveness and overall accountability.

ASIO complied with public interest disclosure reporting mechanisms by informing the Inspector-General of Intelligence of Security (IGIS) on the receipt and conclusion of each disclosure matter.

In 2014–15, the Human Resources Branch managed 72 formal personnel matters outlined in the table below.

Case category	Number of cases (2014–15)
Early intervention support for workers with nonwork-related injuries/illnesses	24
Early intervention support for workers with work-related injuries/ illnesses (did not proceed to workers' compensation claim)	21
Workers' compensation	23
Administrative Appeals Tribunal	1
Misconduct	3
Underperformance	0

Performance Management

ASIO is committed to creating a performance culture where the Organisation builds and develops capability to achieve our strategic and operational objectives to protect Australia, its people and its interests.

No employees were required to participate in the Organisation's formal underperformance management process during the reporting period.

Misconduct

During 2014–15 ASIO completed a total of three misconduct investigations with the areas of specific breach outlined below.

Table 4: Misconduct

Specific element *	Number (2014–15)
Contravened or failed to comply with a term or condition of employment, including the ASIO Values or the Code of Conduct	4
Been inefficient or lacks diligence in the performance of his or her duties	2
Been negligent or careless in the performance of his or her duties	0
Engaged in dishonest or misleading behaviour	2
Engaged in conduct that adversely affects the performance of his or her duties or has the potential to bring the Organisation into disrepute	0
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

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

Legislation and litigation

During the reporting period ASIO played a key role in the development of legislation in collaboration with the Attorney-General's Department (AGD) and other agencies. This legislative reform is an important step in ensuring that ASIO's legislative framework adequately equips and assists it to perform its statutory mandate in a rapidly changing threat environment.

To assist with the implementation of these legislative reforms a range of work was undertaken including internal training, policy formulation, development of internal fact sheets and frequently asked questions, updating existing warrant templates and the establishment of new warrant templates.

National Security Legislation Amendment Act (No. 1) 2014

Most provisions of the *National Security Legislation Amendment Act (No. 1) 2014* (NSLA Act) commenced on 30 October 2014. ASIO made a number of submissions to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the draft legislation and appeared before the Committee on 15 August 2014. The NSLA Act improves the legislative framework governing Australia's intelligence agencies, including the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (ISA), as well as modernisation measures.

Key measures of direct relevance to ASIO include:

- addressing problems relating to the scope and effectiveness of ASIO warrants, including amendments to ASIO's computer access warrant legislation to better reflect modern use of technology;
- introducing a new, single 'surveillance device' warrant;
- modernising ASIO's employment provisions;
- introducing a special intelligence operations scheme to protect ASIO employees and other people from civil and criminal liability for certain authorised activities that would otherwise be unlawful;
- introducing an 'identified person warrant', which, together with subsequent authorisations by the Attorney-General or the Director-General, may enable multiple powers to be exercised against an identified person under one warrant;
- enhancing cooperation between ASIO and the Australian Secret Intelligence Service (ASIS);
- enhancing cooperation between ASIO and the private sector; and
- creating and updating secrecy offences in the ASIO Act and the ISA.

Counter-Terrorism Legislation Amendment (No. 1) Act 2014

The *Counter-Terrorism Legislation Amendment (No. 1) Act 2014* (CTLA Act) commenced on 9 January 2015. The CTLA Act contains measures to assist intelligence and law enforcement agencies to disrupt terrorist threats.

Key measures include:

- improving the control order framework, including making control orders available where a person trains with a terrorist organisation, facilitates a terrorist act or engages in foreign incursions;
- making explicit that it is a statutory function of ASIS to assist and cooperate with the Australian Defence Force (ADF);
- enabling the Minister for Foreign Affairs to give a class authorisation to enable ASIS to support ADF operations;
- enabling the Attorney-General to give agreement to a ministerial authorisation in relation to a class of Australians; and

- enabling ASIS, the Australian Signals Directorate and the Australian Geospatial-Intelligence Organisation to obtain ministerial authorisations in emergency situations.

During the reporting period, ASIO worked with AGD and other Australian Government agencies as part of the development of this legislation.

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014

The *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* addresses gaps in the counter-terrorism legislative framework, focusing on the threat posed by the return of Australians who have participated in foreign conflicts or trained with extremist groups overseas.

Key measures of relevance to ASIO include:

- substituting the 'last resort' requirement for obtaining ASIO questioning warrants with a requirement for the Attorney-General to be satisfied that the warrant request is reasonable in all the circumstances;
- extending to 2018 the sunset date of the ASIO questioning and questioning-and-detention warrants;
- introducing an offence for wilfully damaging things required to be produced under questioning and questioning-and-detention warrants;
- introducing new offences in the *Criminal Code Act 1995* (Criminal Code) (advocating terrorism and entering a declared area without legitimate purpose);
- introducing the temporary suspension of Australian and foreign travel documents;
- introducing the temporary cancellation of visas; and
- introducing the ability to cancel certain welfare benefits for individuals whose visa or passport has been cancelled on security grounds.

ASIO's advice has also informed the declarations by the Minister for Foreign Affairs under the Criminal Code of two geographical areas—al-Raqqa province in Syria (declared on 4 December 2014) and Mosul district in Iraq (declared on 2 March 2015)—making it an offence to travel to those areas without legitimate purpose.

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

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (TIAA Act) requires Australian telecommunications service providers to retain a limited set of telecommunications data for two years. Whilst the introduction of this obligation does not provide ASIO with any new powers, it is a critical step in ensuring that ASIO's access to telecommunications data is not further degraded. Telecommunications data is an important investigative capability which is used in virtually all security intelligence investigations. It importantly also provides an effective and proportionate means to rule individuals out of investigations.

ASIO made a number of submissions to the PJCIS review of the draft legislation (including access to journalists' telecommunications data), and appeared before the Committee on 17 December 2014 and 30 January 2015.

During the reporting period, ASIO took steps towards ensuring that it will be in compliance with the new statutory obligations which took effect on 13 October 2015. This included the delivery of training on, and the development of, new policies and procedures about the new warrant templates for journalist information warrants, the circulation of additional guidance material, the implementation of refined record-keeping and reporting practices, and briefings to key staff across the country.

Telecommunications and Other Legislation Amendment Bill 2015

During the reporting period, ASIO worked with AGD on the development of the draft legislation and associated explanatory material to amend the *Telecommunications Act 1997* and related legislation, including the *Telecommunications (Interception and Access) Act 1979* (TIA Act). The amendments seek to introduce a regulatory framework to better manage national security risks to Australia's telecommunications services and networks.

The draft Bill includes the following:

- an obligation for all carriers, carriage service providers and carriage service intermediaries (C/CSPs) to do their best to protect their networks from unauthorised access and interference;
- a requirement for C/CSPs to notify the Communications Access Coordinator within the AGD of key planned changes to networks and facilities that may make the network or facility vulnerable to unauthorised access and interference; and
- an information gathering power for the Secretary of AGD to facilitate compliance monitoring and compliance investigation activity in relation to compliance with the security obligation, and a further directions power for the Attorney-General to direct a C/CSP to do or not do a specified thing, enforceable by a civil remedies regime.

Amendments to information privacy laws

Consistent with the recommendation of the Joint Commonwealth – New South Wales review of the Martin Place Siege, and with the support of AGD, ASIO 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

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.

However, acknowledging the intrusive nature of these activities, ASIO must obtain a warrant from the Attorney-General prior to conducting these methods of investigation. 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. Central to the use of warrants is the principle of proportionality—ASIO must collect information using the most effective means that are proportionate to the gravity of the threat and its likelihood, and use as little intrusion into personal privacy as possible.

Litigation

The Administrative Appeals Tribunal (AAT) reviewed 11 security assessments, primarily concerning the cancellation of passports held by people who had travelled or intended to travel overseas for the purpose of engaging in politically motivated violence. All of the security assessments reviewed were affirmed by the AAT.

Security of ASIO

Strong personnel, physical, information and IT security are fundamental to the secure and effective conduct of ASIO operations and investigations. A range of governance, policy and technological mechanisms act to protect the information, people and business systems necessary to deliver ASIO's mission—to identify and investigate threats to security and provide advice to protect Australia, its people and its interests.

ASIO's integrated security program is overseen and driven by the Senior Executive and adheres to a best practice security model which meets Australian Government requirements. As threats and risks emerge and change, ASIO adapts internal security measures to meet the challenge of protecting ASIO employees, premises, information and assets.

Building on existing training, ASIO has invested heavily in developing an overarching and comprehensive personal safety and security training continuum for the workforce. A diverse range of training opportunities are offered commencing with a mandatory Personal Safety and Security Workshop for all staff, with more advanced modules delivered to staff based on role requirements. The workshop has also been provided to some staff from close partner agencies including the Australian Cyber Security Centre.

Security governance and policy

ASIO's security policies and practices are compliant with the Australian Government's *Protective Security Policy Framework* (PSPF). ASIO develops and maintains additional protective security policies and guidelines to address the specific security environment ASIO employees work within. ASIO also seeks opportunities to contribute to the maintenance of Australian Government security policy frameworks and policies.

Security governance in ASIO is overseen by the Security Committee. All ASIO employees must comply with mandatory training requirements, which highlight and explain new or changing security risks and provide tools and advice to address them. ASIO ensures that all employees have access to the training, tools and advice required to actively manage any security risks in a manner consistent with ASIO's strong security culture.

ASIO's approach to enhancing the Australian Government's defensive posture against the malicious insider threat is based on our HARM (Human Capital, Access, Resources, Manage Risk) approach. ASIO has focussed on four key areas:

- Translating our investigative, analytical and personnel security assessment experience into new policy initiatives through our participation in the Attorney-General's Department-led Personnel Security Strategic Reforms Taskforce (PSSRT).
- Development of malicious insider threat product for dissemination across government and security vetting officers at security levels ranging from For Official Use Only (FOUO) to Top Secret.
- Targeted malicious insider threat briefings for key Australian government agencies including the Australian Intelligence Community, the Australian Government Security Vetting Agency (AGSVA), Department of Defence, Department of Foreign Affairs and Trade (DFAT) and the PSSRT.
- Developing a range of targeted outreach activities to industry and government through the ASIO Business and Government Liaison Unit and the Contact Reporting Scheme (CRS).

Security clearances in ASIO

Initial and ongoing security vetting provides a critical counter-intelligence function and is conducted in line with whole-of-Government requirements, security risk management strategies, policies and procedures. All ASIO employees and those engaging in work on ASIO's behalf are required to maintain an appropriate high-level security clearance in accordance with the PSPF. ASIO clearance holders are continually assessed for ongoing suitability to hold a clearance. A suitable person demonstrates integrity and reliability and is not vulnerable to improper influence. ASIO employees have access to a number of support services to assist them in maintaining the attributes and behaviours required of an ASIO clearance holder.

The pressure on ASIO's initial vetting and vetting review has not abated since the last reporting period. ASIO's initial vetting and vetting review resources were bolstered in the reporting period in response to existing pressures and to support additional recruitment associated with supporting the government's response to the increased terrorism threat. The vetting of individuals for a positive vetting security clearance is a comprehensive and intrusive process and ASIO continues to be proactive in seeking ways to become more efficient in security vetting processes, such as: introducing critical testing earlier in recruitment processes; leveraging existing information sources wherever possible; reviewing the continued validity of processes; and taking a more active approach in maintaining clearances.

Security Breaches

ASIO is required to report annually on its security status to the Secretaries' Committee on National Security and the National Security Committee of Cabinet. This includes the reporting of security breaches, which are either accidental or an unintentional failure to observe protective security mandatory requirements. ASIO's Senior Executive is briefed on security breaches and relevant senior managers are notified when breaches occur to ensure proactive management of each incident. Action taken for multiple breaches by the same individual can range from formal counselling to misconduct sanctions.

e-Security

ASIO's information technology systems are subject to stringent security requirements. All ASIO information technology systems are subject to ongoing monitoring and audit activities to ensure that usage is both appropriate and secure. Review of systems' security is continuous, and system owners are responsive to evolving security challenges.

Management of relationships and public reporting

ASIO engages with the government and business sectors, the media and the Australian public. While ASIO's outreach is often in respect of the provision of classified security-related advice, ASIO also delivers an appropriate level of public information. ASIO is the only Australian intelligence agency that tables an unclassified annual Report to Parliament.

Review of *Attorney-General's Guidelines*

In response to a recommendation in the Parliamentary Joint Committee on Intelligence and Security *Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014*, the Attorney-General undertook to request a review of the *Attorney-General's Guidelines* to ASIO.

ASIO is working closely with the Attorney-General's Department on this project.

Parliamentary oversight

ASIO is responsible to the Australian Government through the Attorney-General as outlined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). The *Attorney-General's Guidelines* stipulate that ASIO's activities must be conducted in a lawful, timely and efficient manner, applying the principal 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.

ASIO's use of 'special powers' is subject to the approval of the Attorney-General (Part III, Division 3 of the ASIO Act) except for questioning warrants and questioning and detention warrants, which are issued by a 'prescribed authority'. For every warrant issued, ASIO must report to the Attorney-General on the extent to which it assisted the Organisation in carrying out its functions (see page 39 for further detail on ASIO warrants).

ASIO also keeps the Attorney-General informed of significant national security developments, as well as other important issues affecting the Organisation. During the reporting period, ASIO provided advice to the Attorney-General on a range of investigative, operational and administrative issues, primarily communicated through 347 submissions to the Attorney-General.

Report to Parliament

ASIO's 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

ASIO engaged with the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on a range of matters relevant to the Committee's role over the reporting period including:

- providing classified and unclassified submissions to the PJCIS on the Organisation's administration and expenditure;
- providing submissions to and attending hearings on the Committee's review of draft legislation, including the National Security Legislation Amendment Bill (No.1) 2014, the Counter- Terrorism Legislation Amendment (Foreign Fighters) Bill 2014, the Counter-Terrorism Legislation Amendment Bill (No.1) 2014 and the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014; and
- attending a number of hearings for the proscription and relisting of terrorist organisations.

Martin Place siege: Joint Commonwealth – New South Wales review

On 17 December 2014 the then Prime Minister, the Hon. Tony Abbott MP, and the New South Wales Premier, the Hon. Mike Baird MP, announced a review of the Martin Place incident in respect of national and state agencies and the cooperation between them. This review was conducted jointly by the Department of the Prime Minister and Cabinet (PM&C) and the New South Wales (NSW) Department of Premier and Cabinet.

ASIO engaged openly and actively with the review. ASIO holdings and actions as they related to Mohammad Hassan Manteghi (also known as Man Haron Monis) informed—and were referenced in—the final report of the joint review, which included a detailed appendix outlining ASIO's prioritisation model.

No recommendations were made regarding ASIO's conduct, or ASIO's processes and procedures as they related to Manteghi. One recommendation in the report related to ASIO's access to information. It recommended that all states and territories review relevant legislation—particularly with regard to privacy and health—to ensure appropriate access by ASIO. However, the report noted that ASIO was able to access all relevant information held by government agencies in this case.

Senate Standing Committee on Legal and Constitutional Affairs

Senate Estimates

As part of the Attorney-General's portfolio, ASIO appears before the Legal and Constitutional Affairs Committee. In 2014–15 the Director-General, Mr Duncan Lewis, and/or Deputy Director-General Ms Kerri Hartland, appeared before the Committee on three occasions: Supplementary Budget Estimates, on 10 December 2014; Additional Estimates, on 24 February 2015; and Budget Estimates, on 28 May 2015.

During these appearances, ASIO responded to questions on topics including ASIO's budget, security assessments in respect of passports, foreign fighters and the legislative changes to the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

Senate inquiry into the Telecommunications (Interception and Access) Act 1979

The Senate Legal and Constitutional Affairs References Committee completed its inquiry into the comprehensive revision of the TIA Act and tabled its report on 23 March 2015.

The focus of the report was on the mandatory data retention regime, issues on which the Committee members were unable to reach an agreed view and which were largely superseded as a result of the passage of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. There was a general recognition by the Committee of the need for urgent reform of the TIA Act.

During the reporting period former Director-General of Security, Mr David Irvine AO, attended a public hearing to supplement ASIO's unclassified submission to the inquiry.

Independent oversight

Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office holder responsible for reviewing the activities of the Australian Intelligence Community to provide assurance that agencies operate with propriety, according to law, consistent with ministerial guidelines and directives and with due regard for human rights.

Dr Vivienne Thom held the position of IGIS during the reporting period, (Ms Margaret Stone, the Independent Reviewer of Adverse Security Assessments during the reporting period and a former Federal Court judge, commenced as IGIS on 24 August 2015). Appointed in 2010, Dr Thom concluded her term as IGIS in July 2015. 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 need, and it 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.

Independent Reviewer of Adverse Security Assessments

The Independent Reviewer conducts independent advisory reviews of ASIO adverse security assessments provided to the Department of Immigration and Border Protection (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.

The Hon. Margaret Stone held the position of Independent Reviewer during the reporting period.

The Independent Reviewer has access to all materials relied on by ASIO in making its assessment, as well as any additional information obtained by ASIO since the assessment was completed. At the conclusion of the reporting period, the Independent Reviewer had finalised 46 of the 47 primary reviews within her cohort. Having finalised 22 primary reviews in previous years, in financial year 2014–15 the Independent Reviewer finalised a further 24. Of these:

- In six cases the Independent Reviewer found the adverse security assessments were appropriate.
- In two cases the reviews were well advanced when ASIO furnished new assessments—one qualified and the other non-prejudicial. In both cases, the Independent Reviewer completed her review and agreed the new assessments were appropriate.
- In six cases, the Independent Reviewer found the adverse security assessments had been appropriate at the time they were furnished but were no longer appropriate, and recommended either qualified or non-prejudicial security assessments. After re-examining the cases, in five cases ASIO furnished either qualified or non-prejudicial assessments in accordance with the Independent Reviewer's recommendation.
- In one case, the Independent Reviewer recommended ASIO issue a non-prejudicial security assessment. Following consideration, ASIO furnished a qualified security assessment. The Independent Reviewer completed her report finding the qualified security assessment was not appropriate and maintaining her view that a non-prejudicial security assessment would be an appropriate outcome.
- In five cases, new (qualified or non-prejudicial) security assessments were furnished by ASIO following new information referred by the Independent Reviewer, and the outcomes of ASIO's own investigations.
- In two cases, the Independent Reviewer found there were flaws in ASIO's assessment and she was unable to form a view as to the appropriateness of the adverse security assessment. In both cases, ASIO furnished qualified security assessments, which the Independent Reviewer agreed were appropriate.

- In three cases, the Independent Reviewer found the adverse security assessments were not appropriate. Of these: In one case, the Independent Reviewer recommended ASIO issue either a non-prejudicial or qualified security assessment. After re-examining the case ASIO furnished a non-prejudicial security assessment.
- In two cases, the Independent Reviewer recommended ASIO issue a non-prejudicial security assessment. After re-examining the cases ASIO furnished non-prejudicial security assessments.

In addition to the finalised cases, the Independent Reviewer referred new information concerning one case to ASIO, together with an incomplete but advanced draft of her report. The draft summarised all the information before her but did not include any recommendation. ASIO was considering the new information at the end of the reporting period. Under the terms of reference, the review process for this case remains on hold until ASIO concludes its consideration of the new information.

Periodic Review by the Independent Reviewer of Adverse Security Assessments

In parallel with the Independent Review process, ASIO undertook a large number of internal reviews of its own volition (see below). The Independent Reviewer decided to proceed with periodic reviews, regardless of the status of the ASIO internal review, and (provided the legal representatives had been given ample notice) regardless of whether or not any additional submissions had been provided to her office. This approach was in the best interests of applicants as it was anticipated that the opinion expressed in the Independent Reviewer's draft report would be of assistance to ASIO in its internal review. A number of legal representatives advised they would await the outcome of the ASIO internal review prior to turning their attention to the Independent Reviewer's periodic review process. A number of periodic reviews ceased in the reporting period due to ASIO's furnishing of non-prejudicial or qualified security assessments of its own volition.

There were 14 extant adverse security assessments at the end of the reporting period, which were eligible for periodic review. By the end of the reporting period, the Independent Reviewer had provided four draft periodic review reports to ASIO.

ASIO internal review of adverse visa security assessments

ASIO has its own internal review process to review assessments where the subjects of the adverse visa security assessment are in detention and have no rights to merits review other than through the Independent Reviewer.

- With the passage of time, new information can become available to ASIO. Where new information becomes available, ASIO reviews it to determine whether it may have a bearing on an extant security assessment.
- New information can include additional information supplied by the applicant, DIBP, the Independent Reviewer, information obtained through ASIO investigations, or a new strategic assessment which may change ASIO's evaluation of previous information.
- ASIO may conduct a review of an adverse security assessment after a period of time, irrespective of whether new security relevant information is available. This typically, but not exclusively, applies to Illegal Maritime Arrivals (IMAs), who have been found to be refugees but who do not have access to merits review apart from the independent review process.

Independent National Security Legislation Monitor

The Independent National Security Legislation Monitor (INSLM) was established by the *Independent National Security Legislation Monitor Act 2010*. The role of the INSLM is to assist ministers in ensuring Australia's counterterrorism and national security legislation:

- is effective in deterring, preventing and responding to terrorism;
- is consistent with Australia's international obligations; and
- contains appropriate safeguards to protect the rights of individuals.

The Hon. Roger Gyles AO QC commenced in the position of INSLM on 7 December 2014.

During the reporting period, Mr Gyles commenced an inquiry into section 35P of the *Australian Security Intelligence Organisation Act 1979* in relation to special intelligence operations. ASIO has appeared at private and public hearings as part of the inquiry and provided classified and unclassified submissions in response to requests for information. This included briefings to Mr Gyles on ASIO operational activity.

ASIO's domestic relationships

Business Liaison Unit

In the reporting period ASIO's Business Liaison Unit (BLU) continued to provide corporate security managers with credible, intelligence-backed reporting to enable them to brief executive management and staff on the security environment and to help inform their organisational risk management and continuity planning. The advice is provided primarily via a secure, subscriber-only website which publishes ASIO reports in a 'For Official Use Only' format. In addition, the BLU embarked on a program of outreach to ensure the information provided in the reports meets the requirements of corporations in Australia.

Over the reporting period the BLU also hosted six industry forums for specific sectors including aviation, banking, energy, places of mass gathering and defence. The BLU also made presentations to industry forums including tertiary education managers, aviation, defence, mining, and oil and gas.

The BLU also coordinates an executive program, arranging meetings between company CEOs and the Director-General.

ASIO Partnership Forum

The ASIO Partnership Forums are an important part of ASIO's government engagement. The forums are designed to provide participants from across government with a better understanding of ASIO's role, structure and priorities.

During the reporting period, ASIO held separate programs for the Senior Executive Service and for senior officers (Executive Level 1, Executive Level 2 and equivalent military and police levels) from a range of Australian government and state and territory agencies. Feedback from the forums was overwhelmingly positive, with attendees remarking on the high level of detail and contemporary nature of information provided.

ASIO Classified Briefing Day (Security-in-Government Conference)

The Security-in-Government Conference is an annual Attorney-General's Department-led whole-of-Government three-day conference. As part of this conference ASIO hosts a classified briefing day. This conference provides ASIO with an opportunity to speak directly to all NV1 (or above) cleared agency security advisers and security practitioners in government. Known as the 'classified briefing day' it is an important annual platform to deliver ASIO's strategic security messages and describe the changing environment to all those who work in it. The theme for the briefing day held in 2014 was 'Mitigating the malicious insider threat'.

Stakeholder Satisfaction Survey

The Stakeholder Satisfaction Survey is conducted annually and provides a valuable insight into the levels of satisfaction of key partners. ASIO surveys key stakeholders in the Australian government and states and territories to capture feedback on the quality of ASIO advice, the effectiveness of our capabilities and people, and the value ASIO adds through cooperation and engagement. Feedback from external stakeholders is critical to the evaluation of ASIO's performance and effectiveness and to its commitment to continual improvement and provides an opportunity to explore areas for enhanced engagement.

As per ASIO's Strategic Plan 2013–16 the survey is one of the tools used to identify any risk, in particular reputational, which may impact on the Organisation's ability to deliver against its mandate.

During the reporting period ASIO engaged an external consultant with extensive experience in the Australian Intelligence Community to prepare and conduct the survey to ensure feedback was forthright.

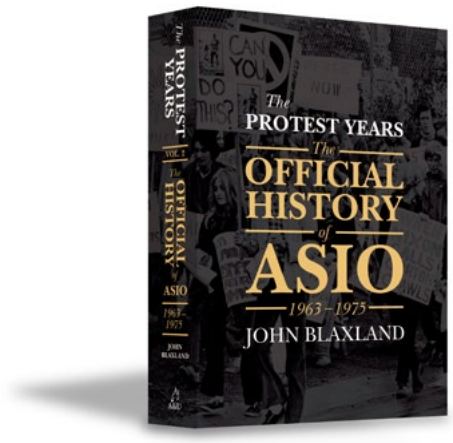
Preparations for the next survey, scheduled for July–August 2016, will be presented to senior management early 2016.

Public statements and media

ASIO has a publicly listed media contact number and email address. ASIO routinely responds to media inquiries but does not comment on operations, investigations or individuals, nor does it comment on operational capabilities.

Attributable public statements are occasionally provided by the Director-General through media responses, public speeches, or appearances at parliamentary or senate hearings. The Director-General occasionally speaks at public seminars or conferences.

ASIO's media effort includes, where possible, assisting the media in its reporting of national security matters. For ASIO, it is an opportunity to clarify information and to inform the Australian public about matters of security concern. ASIO appreciates the value of accurate media reporting on national security.



Official History of ASIO

The Spy Catchers: The Official History of ASIO 1949–1963, volume 1 of the official history of ASIO, was launched by the Attorney-General on 7 October 2014 at the Museum of Democracy, Old Parliament House, Canberra. The book was written by Professor David Horner of the ANU's Strategic and Defence Studies Centre. Overall responsibility and direction for the project at the ANU lies with Professor Horner.

During the reporting period *The Spy Catchers* sold over 7000 copies, and a paperback version was released in October 2015. *The Spy Catchers* won the St Ermin's Hotel Intelligence Book of the Year Award 2015 in the United Kingdom. Outside of the reporting period this volume was a joint winner of the prize for Australian history in the 2015 Prime Minister's Literary Awards.

The second volume in the series, entitled *The Protest Years: The Official History of ASIO 1963–1975*, has been written by Dr John Blaxland and was published by Allen & Unwin in October 2015. A third volume will cover the period 1975–1989.

The ANU researchers have viewed over 7000 unredacted ASIO files. Progress of the project is monitored by the History of ASIO Advisory Committee. The Committee meets every six months and comprises Mr Geoff Gallop AC, the Director-General and a Deputy Director-General. Mr Jim Carlton AO, who was formerly a member of the committee, passed away in December 2015. As the project is in its final stages the position occupied by Mr Carlton will not be filled.

Public access to ASIO records

ASIO is subject to the release of records under the *Archives Act 1983* (Archives Act), which allows the public to request access to Australian government records in the open period. The open period currently covers all records created in or before 1989.

All public requests for ASIO records are made to the National Archives of Australia (NAA) in the first instance, and the NAA passes the request to ASIO. ASIO assesses relevant records and then provides advice to the NAA about whether the records contain information that should be exempt from public release under section 33(1) of the Archives Act. Exemption decisions are based on whether the information is sensitive now, not whether it was sensitive at the time the record was created.

ASIO continues to face challenges in meeting the 90-day legislative turnaround time. ASIO prioritises requests to provide equitable access and gives greater priority to requests from those seeking records on themselves or family members. This is in accordance with the 1992 direction from the Parliamentary Joint Committee on ASIO, endorsed in 2008 by the Inspector-General of Intelligence and Security. Currently 10 individual applicants are responsible for 50 per cent of requests for access.

In 2014–15 requests for access to ASIO records continued to increase, with a total of 811 requests completed.

Applicants dissatisfied with exemptions claimed by ASIO may request that NAA reconsider the decision. In 2014–15, one request was reconsidered with the NAA upholding the ASIO exemptions.

Applicants may also appeal to the Administrative Appeals Tribunal (AAT) regarding ASIO exemptions or if their request is not completed within 90 days. One application from 2012–13 continues to be the subject of action under the auspices of the AAT; this matter concerns 'deemed refusal' of multiple requests. During the reporting period, hearings on this matter led to some reprioritisation by the applicant of other access requests to ASIO. There were no new AAT appeals in this reporting period.

ASIO's international relationships

ASIO engages with, and receives support from, a number of international partners. While international partnerships have always been important in the performance of ASIO's functions, the complexity of the 'foreign fighters' issue has made cooperation with foreign security and intelligence agencies even more critical. As a consequence, ASIO expanded its overseas liaison network during the reporting period.

Many security threats are transnational in nature. Liaison relationships enable ASIO to draw on the expertise and capability of overseas partners.