Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the
Parliamentary Joint Committee on Intelligence and Security

Review of Administration and Expenditure

No.13 2013–2014

www.asio.gov.au

Contents

Scope of review

The Australian Security Intelligence Organisation (ASIO) submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) *Review into Administration and Expenditure No. 13* provides a detailed account of ASIO's activities during the financial year. For 2013–14 the PJCIS wrote to ASIO requesting a submission covering all aspects of administration, including:

- Strategic direction and priorities;
- Legislative changes that have impacted on administration of the agency, including, as appropriate, the frequency and nature of use of these powers, staffing implications, training, the role of legal officers and need for specialist staff and relationship with outside agencies such as police or the judiciary;
- Involvement (if any) in litigation matters;
- 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 any associated outsourcing arrangements;
- Public relations and/or public reporting, including requests for public access to records; and
- Ability to meet objectives within budget parameters, budget constraints, ongoing implications of the efficiency dividend, other savings measures, and the use of any supplementary funding.

This report examines ASIO's activities and performance in the areas requested above to provide the PJCIS with visibility of the fiscal, administrative and operational performance of the Organisation.

Executive summary

The security environment 2013–14 and outlook

Australia's security faces a disparate array of challenges at an intensity not seen since the end of the Cold War. These range from individuals motivated to undertake acts of politically motivated violence, sabotage, communal violence, espionage or individuals who abuse privileged access to private information, through to actions authored by foreign states, intended to interfere in our democracy, suborn public officials or steal government secrets. An emerging challenge is an increasing number of individuals who reject our democratic system and act to spread discontent within it.

Terrorism

The principal terrorist threat to Australians and Australian interests—nationally and internationally—continues to emanate from Sunni Islamist extremism. The conflict in Syria and Iraq continues to resonate with Islamist extremists around the globe, including in Australia, and remains the single most significant factor affecting the international security environment.

The threat from other groups and regions has not, however, abated. Terrorist groups in South, Central Asia and South-East Asia, in Africa and in other parts of the Middle East will continue to pose threats to Australians and Australian interests across the globe.

Espionage and clandestine foreign interference

Acts of espionage and foreign interference have continued to increase in terms of range, scale and sophistication.

The cyber threat

The threat posed by malicious activity conducted by cyber means has continued to increase. During the reporting period, ASIO provided industry partners with security advice and defensive briefings on the threat posed by cyber espionage to sensitive information and intellectual property.

Border integrity

While the number of illegal maritime arrivals has declined significantly, Australia's border integrity continues to be challenged and maritime people smuggling continues to pose a threat to Australia's border integrity and security.

Expenditure

ASIO's budget has been under increasing pressure over the last few years with ASIO absorbing a number of additional functions and activities without supplementation. These functions and activities included work in relation to serious threats to border integrity; increasing costs of telecommunications interception; the Counter Terrorism Control Centre; and increased litigation activity (during a period where the terrorism and espionage threats to Australia's security was also increasing). Although outside the reporting period, in early August 2014 the Government announced new funding to enhance security intelligence capabilities to counter the terrorism threat and to enable the organisation to employ more resources against this continually evolving threat.

Structure of the Organisation

ASIO has refined its structure and introduced a range of efficiency measures over the past year.

Corporate direction and strategic planning

ASIO's vision, mission and goals are set out in *ASIO's Strategic Plan 2013–16*. While the global and Australian security environments continue to change, ASIO must operate as effectively and efficiently as possible and work even more closely with the wider national security community.

The strategic plan sets our major goals and provides guidance in meeting the expectations of the Government or partners and the Australian community. It also articulates ASIO's strong commitment to developing and enhancing partnerships with law enforcement, national and international intelligence agencies and the Australian community.

ASIO's priority—to protect Australian lives and interests from security threats—including terrorism and other forms of politically motivated violence, communal violence, espionage and foreign interference and serious threats to border and territorial integrity—remains fundamental to Australia's national security.

Human resource management

Over the reporting period ASIO focussed recruitment on the difficult-to-fill roles of intelligence officer, technical officer and security assessor. ASIO also introduced a new technical officer graduate program to attract and develop entry-level staff in specialist areas.

Two Intelligence Development Programs were conducted over the reporting period. Planning has been undertaken outside of the reporting period to remodel the existing program to cater for the anticipated increase in intelligence officer intakes.

Legislation

ASIO has been operating at a heightened tempo over the reporting period with increased demands on its capabilities. These demands were further compounded by the challenges of working within a legislative framework that was enacted more than 30 years ago and had not kept pace with significant technological change.

The *National Security Legislation Amendment Act No.1 2014* (NSLA Act No. 1) commenced in October 2014 and contains a range of improvements and modernisation measures to the legislative framework governing Australia's intelligence agencies. The amendments aim to improve the effectiveness of processes, to modernise, to enhance cooperation and to protect information and capabilities. Outside the reporting period ASIO has provided submissions and attended hearings to assist with PJCIS consideration of a range of national security legislative reforms including the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

Litigation

Since 2005, there has been a significant increase in the volume of security assessment litigation and complex matters involving multiple Commonwealth agencies in the Federal and High Courts of Australia as well as the Administrative Appeals Tribunal (AAT).

In 2013–14 ASIO was involved in over 50 litigation matters, including terrorism and other criminal prosecutions, civil matters (in which ASIO material was sought as evidence) and judicial and administrative review of ASIO security assessments.

Security of ASIO

ASIO has a strong security framework and culture. The strong personnel security supported by appropriate governance, policy and technological processes are fundamental to the secure and effective conduct of ASIO operations.

Accountability

ASIO operates under a stringent oversight and accountability mechanism. These include:

- the Attorney-General, Parliamentary Ministers and the National Security Committee of Cabinet
- the Inspector-General of Intelligence and Security (who has the power akin to a standing Royal Commission, is accountable to Ministers, and also reports to the Parliament)
- the bipartisan Parliamentary Joint Committee on Intelligence and Security
- the Australian National Audit Office (who undertake independent performance audits with the authority contained in the *Auditor-General Act 1997)*
- ASIO's annual *Report to the Parliament*
- Independent National Security Legislation Monitor
- *Attorney-General's Guidelines*—provide guidance into how we do our business—such as, 'any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence'
- the Independent Reviewer of Adverse Security Assessments

ASIO officers are also subject to internal policies and procedures. They provide Director General's delegations of authority, direction and guidance to ensure all ASIO's operations and investigations are conducted in an environment of legality, accountability, efficiency, propriety and security designed to maximise our performance and contribution.

As part of the *National Security Legislation Amendment Act (No 1) 2014* the Government has committed to reviewing the *Attorney-General's Guidelines*, likely commencing in the first quarter of 2015.

Relationships

ASIO continues to work to enhance awareness of the work of the Organisation amongst the public as well as government and industry partners. Over the reporting period the Director-General addressed a number of public forums. These speeches can be accessed through the Organisation's website which also provides frequently asked questions and information sheets on the work of the Organisation. The Organisation also regularly conducts partnership forums for Senior Executive Service and senior officers in other government agencies and works closely with industry through the Business Liaison Unit which provides security advice and reporting.

Under Attorney-General authority ASIO engages with and receives support from a number of international partners. At the end of the reporting period, ASIO was authorised to liaise with 346 authorities in 129 countries.

ASIO's relationships with international partners were strengthened further by its work on the G20, some of which fell outside of the reporting period. ASIO provided security intelligence advice to help inform security arrangements for all G20 meetings and also provided security assessments for individuals working on G20 events.

ASIO's role and functions

ASIO is Australia's security intelligence service. Its role and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). ASIO's primary function is to collect, analyse, assess and disseminate security intelligence. Security intelligence is concerned with a specific set of activities that might harm Australia, Australians or Australian interests (including overseas). Those activities are:

- espionage;
- sabotage;
- politically motivated violence (including terrorism);
- the promotion of communal violence;
- attacks on Australia's defence system;
- acts of foreign interference; and
- the protection of Australia's territorial and border integrity from serious threats.

ASIO's responsibility for security intelligence extends beyond Australia's borders and includes Australia's 'security' obligations to other countries (in Australia and overseas). In fulfilling its obligation to protect Australia, its people and its interests, ASIO:

- collects intelligence through a wide range of means, including human sources and technical operations, using the least intrusive means possible in accordance with the *Attorney-General's Guidelines*;
- assesses security intelligence and provides advice to Government on security matters;
- investigates and responds to threats to security;
- maintains a national counter-terrorism capability;
- provides protective security advice; and
- provides security assessments, including for visa entry checks, access to classified material and designated security-controlled areas.

Under the ASIO Act and other legislation, ASIO is authorised to use intrusive powers under warrant, including inter alia, telecommunications interception, the entry and searching of premises, and compelling persons to appear before a prescribed authority to answer questions relating to terrorism matters. ASIO is responsible for collecting foreign intelligence within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence, and maintains specialist capabilities that can be deployed to assist in intelligence operations and incident response.

ASIO operates within a stringent oversight and accountability framework. The foundation of this framework is the ASIO Act, created to recognise the importance of individual rights, while safeguarding the public's collective right to be secure.

Under the ASIO Act, the Organisation is responsible to the Australian Government through the Attorney-General. ASIO is also required to comply with the *Attorney-General Guidelines*, which outline how ASIO must conduct its operations. The Guidelines stipulate that ASIO's information collection activities should be conducted in a lawful, timely and efficient manner, using the least intrusion necessary into an individual's privacy and proportionate to the gravity of the threat being investigated.

The security environment 2013–14 and outlook

Australia's security faces a broad array of challenges at an intensity not seen since the end of the Cold War. The terrorist threat from Islamist extremists is increasingly serious and significant, and future prospects in the Middle-East, Africa, South-East Asia and the West are concerning. This worsening situation has direct ramifications for Australians and Australian interests and will have generational impact globally. An emerging challenge is an increasing number of individuals who reject Australia's democratic system and act to spread discontent within it.

The scale and breadth of espionage against Australia is significant. The risk to Government information—as well as the information shared by our closest international partners—is significant and carries serious implications for our national sovereignty and prosperity and our reputation with international partners. Beyond the threat to Government business, Australia's commercial, economic, and research and development activities are being targeted, representing a risk to future economic prosperity.

Terrorism

Within Australia the principal terrorist threat is from Australian Islamist extremists who subscribe to the distorted narrative that Australia is at war with Islam, and that the use of violence to support their ideology is not only legitimate but necessary.

The major challenge at present relates to Syria and Iraq, and it directly involves Australians. During the reporting period, around 60 Australian Islamist extremists were identified who travelled to Syria, Iraq and the immediate region. A similar number of Australians are known to be seeking to travel to Syria and Iraq; supporting Islamist extremist groups there; or facilitating travel by others. There will be others involved in such activities of whom ASIO is not aware.

The influence of the Syria and Iraq conflicts was also felt, notably in the scale of South-East Asian jihadist involvement in these conflicts. Combined with other developments, particularly in Indonesia, the potential return of jihadists from Syria and Iraq may result in a rise in attack capability in South-East Asia, potentially targeting Western—including Australian—interests.

While the conflicts in Syria and Iraq are currently the principal concerns, other jihadist terrorist threats persist, including the undiminished intent of transnational terrorist groups such as al-Qa'ida in the Arabian Peninsula and continued terrorist planning and attacks and kidnappings in Africa. Lone actors taking inspiration from overseas conflicts and being motivated to conduct an independent attack remain an issue of concern. Established jihadist organisations have recognised the potential of encouraging lone actors with no links to them to undertake attacks in the West, providing encouragement and instruction online.

ASIO also remains concerned over the impact of the conflict in the Australian domestic security environment, including the exacerbation of tensions between communities here.

Espionage and clandestine foreign interference

Espionage and clandestine foreign interference activity against Australian interests is extensive.

ASIO investigations over the reporting period provide an increased understanding of the threat from clandestine activity by foreign powers directed against Australia. Foreign powers use a wide range of techniques and capabilities, including human intelligence, technical collection and exploitation of the internet and information technology, to obtain intelligence or disrupt use (cyber attack).

In responding to this threat, ASIO pursues a three-part approach: to discover the most harmful clandestine activity; degrade its adverse impact on Australia and defend against future harmful clandestine activity, including by contributing to resilient security policies and practices. ASIO worked closely with business, government and key intelligence partners to counter the threat posed by these attacks.

Continued unauthorised disclosures of sensitive information during the reporting period have highlighted the threat posed by self-motivated malicious insiders. Such individuals who exploit their privileged access to government information to make unauthorised disclosures of classified or other privileged information are a constant source of potential harm to Australia's national interests. Modern technology which allows the aggregation and copying of large amounts of information has greatly increased the harm caused by these individuals. Edward Snowden is a compelling example of the wide-scale and indiscriminate harm that can be caused by malicious insiders, with the damage caused by his disclosure of classified information expected to be felt for many years.

The cyber threat

The threat posed by malicious activity conducted by cyber means has continued to increase. In 2013-14 the range, scale and sophistication of state actors engaged in hostile cyber espionage activity against Australian Government and private sector systems continued to increase. Critical to counter this persistent and highly damaging threat are holistic, well-established and widely adopted security practices and policies.

ASIO continues to allocate substantial resources to defensive outreach and advice to heighten awareness of the threat environment and to drive and shape appropriate security policy responses.

The establishment of the Australian Cyber Security Centre in late 2014 is expected to deliver substantial dividends and momentum on cyber security issues, not least in enhancing coordinated and targeted industry outreach.

Border integrity

ASIO continues to contribute to the Whole-of-Government effort to counter serious threats to Australia's border and territorial integrity. This contribution has included identifying and investigating Australians and Australia-based individuals involved in maritime people smuggling, and providing appropriate advice to Government such as security assessments of people seeking a visa to enter Australia.

Since July 2013, the number of illegal maritime arrivals has declined significantly. Awareness among potential illegal immigrants of Australian Government policies, and implementation of these policies, has contributed to this decline. However, Australia's border integrity continues to be challenged, and maritime people smuggling continues to pose a threat to Australia's border integrity and security. People smugglers are resilient and adaptable, and some continue to target Australia.

Outlook for the security environment

The conflict in Syria and Iraq will remain a significant challenge over the next 12 months and well beyond. Australians and other Westerners will continue to be inspired by the successes of groups in Syria and Iraq—and they will continue to attempt to travel to join them. At the same time, we may see an increasing number of extremists who have fought in Syria and Iraq attempt to return to their home countries. They will likely return strongly radicalised with an increased capability—there have already been attacks in Europe perpetrated by conflict returnees.

As a result, there will be a steadily growing pool of supporters and sympathisers in Australia and other Western countries. Some will proceed to acts of politically motivated or communal violence. Of these, some will be known to security and law enforcement agencies—others will not.

Outside of Syria and Iraq, the security environment in our near region, in south and central Asia and in Africa will continue to deteriorate. Areas within these regions will continue to provide safe havens for al-Qai'da and its affiliates and environments conducive to radicalisation, training and potentially, plotting against the West.

Lone actors will present an ongoing challenge to Australia's national security and public safety, not only in respect of their potential to undertake acts of violence but for other areas of security, such as engaging in the release of non-public information, sabotage of critical systems and infrastructure. They are not limited to any one form of extremism. ASIO maintains a range of ongoing activities to identify such individuals. Nevertheless, although security and law enforcement agencies work constantly to detect individuals who support the use of violence to achieve a political, religious or ideological or personal goal, we will not be able to detect all lone actors.

The challenges Australia faces from clandestine foreign activity targeting Australian government and business information will persist, as will the threat from the actions of malicious insiders. Australia's defence will be multidimensional and will include raising awareness of the consequence for individuals who betray the trust associated with access to highly sensitive government information.

Expenditure

Budget

ASIO's budget is set out in the *Portfolio Budget Statements*, with the audited outcome published in the annual *ASIO 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 2013–14 ASIO's operating result was a $2.8 million surplus excluding depreciation. Revenue from Government for 2013–14 was $346.2 million, up from $329.7 million in 2012–13. $12.5 million of this increase is because ASIO was funded directly through appropriation for the Humanitarian Migration Programme rather than recovering funds from the Department of Immigration and Border Protection. ASIO was approved to operate at a loss of $13.0 million for 2012–13 for costs associated with the move to the Ben Chifley Building. Due to the delay in the move, this loss has been deferred to the 2014–15 financial year.

ASIO will receive $368.4 million departmental operating appropriation from Government in the 2014–15 budget. This includes $11.2 million to enhance security intelligence capabilities to counter the Islamist terrorism threat which is part of the measures announced by the Prime Minister in August 2014 to strengthen security and intelligence organisations.

In recent times ASIO has prioritised, cut and adjusted its activities consistent with broader Government objectives and budgetary situation. ASIO has continued to absorb a range of additional functions within its budget, including work in relation to serious threats to border integrity; increasing costs of telecommunications interception; the Counter Terrorism Control Centre; and increased litigation activity in an escalating threat environment.

ASIO's restructure in January 2013 and the introduction of a range of efficiencies sought to balance an appropriate level of operational activity and the longer term development of capability within ASIO's budgetary envelope.

There is a permanent, expensive, and unavoidable 'security overlay' associated with ensuring intelligence agencies can operate effectively and securely.

These are costs the agencies must bear with the consequence that efficiencies must be realised elsewhere in the agency operations.

Financial performance

ASIO recorded an operating deficit of $46.3 million in 2013–14. Excluding depreciation, ASIO achieved an operating surplus of $2.8 million.

Figure 1: Revenue from government for years from 2008-2009 to 2013–14

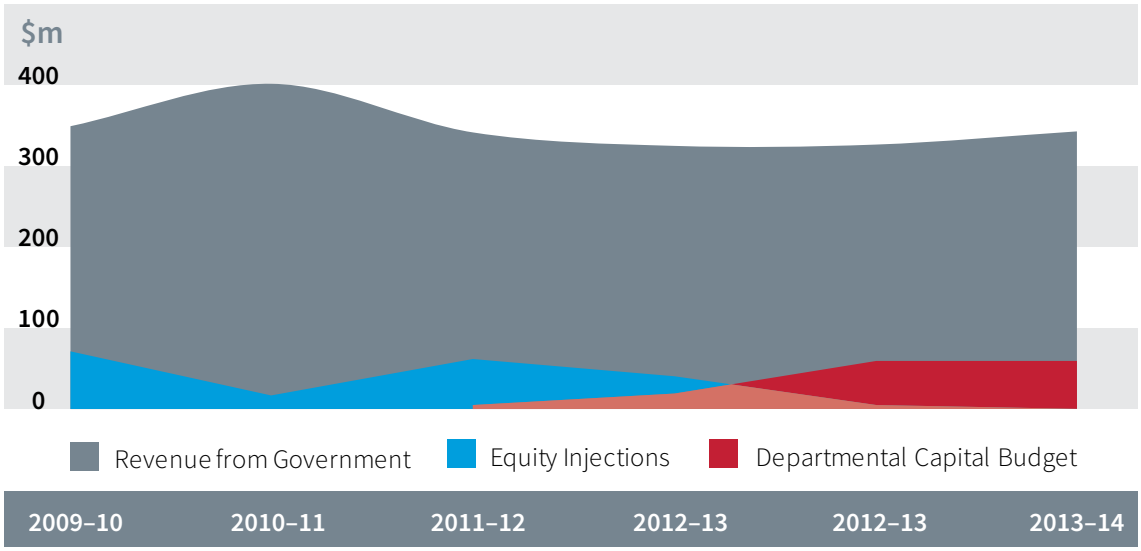
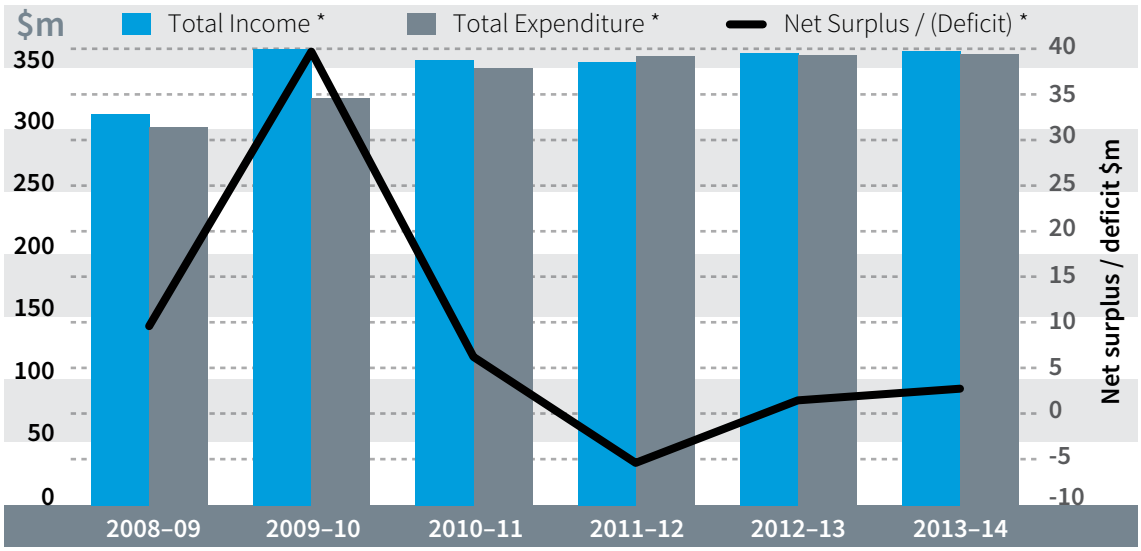


Figure 2: Financial performance for years from 2008–09 to 2013–14



Strategic allocation of resources

ASIO's Executive Board sets the Organisation's strategic direction which is reflected in the allocation of resources across ASIO's activities. The Finance Committee reports to the ASIO Executive Board to ensure the Organisation's budget and resource allocation is aligned with organisational priorities.

Project proposals are submitted through the relevant ASIO Governance Committee—the Finance Committee to agree on funding strategies before being put to the ASIO Executive Board for endorsement. In 2013–14 ASIO continued to focus on maintaining and enhancing capabilities across the collection, operational and technical fields.

Rapid technological advances continue to present significant challenges to ASIO in maintaining its capabilities. ASIO supports legislative reform that seeks to modernise and improve the Australian intelligence community's effectiveness and ability to work together.

Figure 3: Resource allocation

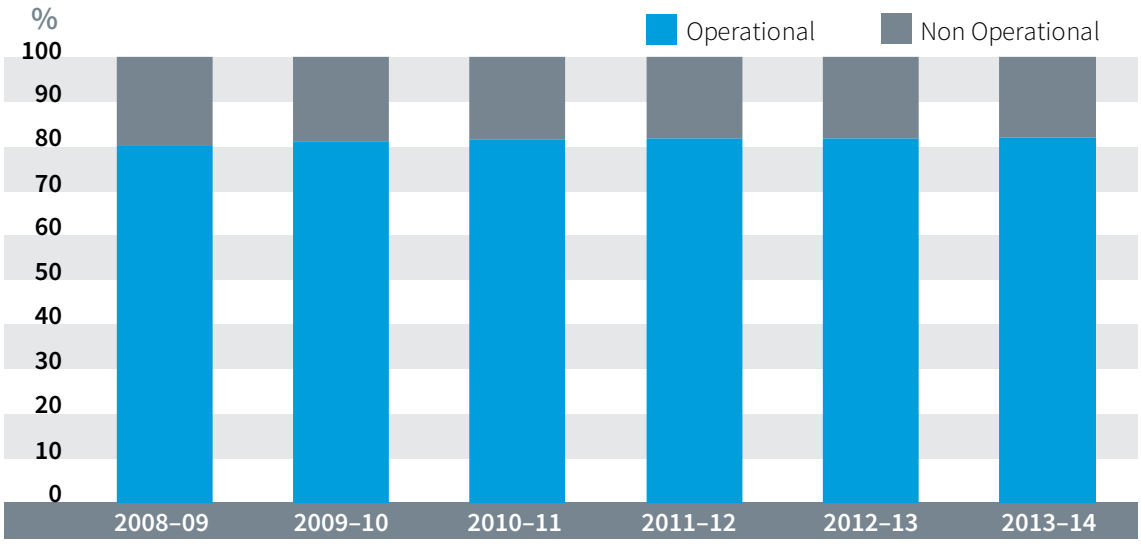
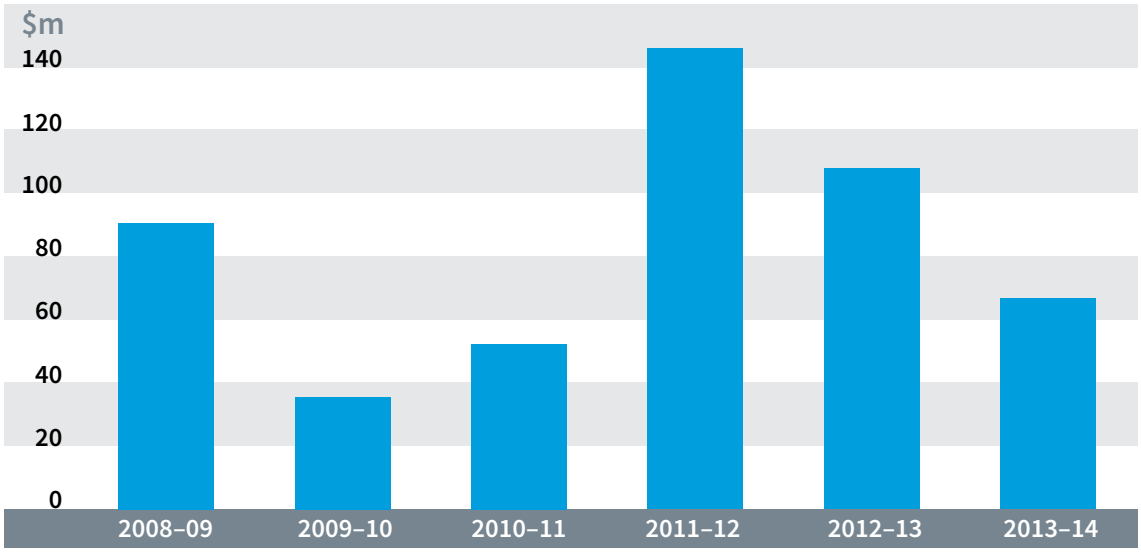


Figure 4: Purchase of capital items



Financial management and internal controls

Over the reporting period ASIO prepared annual financial statements in accordance with provisions of section 49 of the *Financial Management and Accountability Act 1997* (FMA Act) and the Finance Minister's Orders. 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 2013–14 ASIO did not receive any adverse audit qualifications from the ANAO as part of its independent audit reporting to Parliament. There were two 'C' findings, issues that pose a low business or financial management risk to the entity, which have been addressed.

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.

Structure of the Organisation

Organisational structure

ASIO maintained its eight division structure following the 23 percent reduction in the Senior Executive Service during the previous reporting period.

ASIO further refined its organisational structure in this reporting period by combining its operational and support functions into two groups under each Deputy Director-General.

Counter-Espionage and Interference, Information, Technical Capabilities and Corporate Security Divisions are structured under one Deputy Director-General; and Operational Capabilities, Office of Legal Counsel, Security Advice and Assessments and Counter-Terrorism Divisions report to the second Deputy Director-General.

The number of branches within the divisional structure has remained relatively stable, with the creation of one new branch, Data Exploitation Projects, within Technical Capabilities Division.

Figure 5: ASIO organisational structure at 30 June 2013

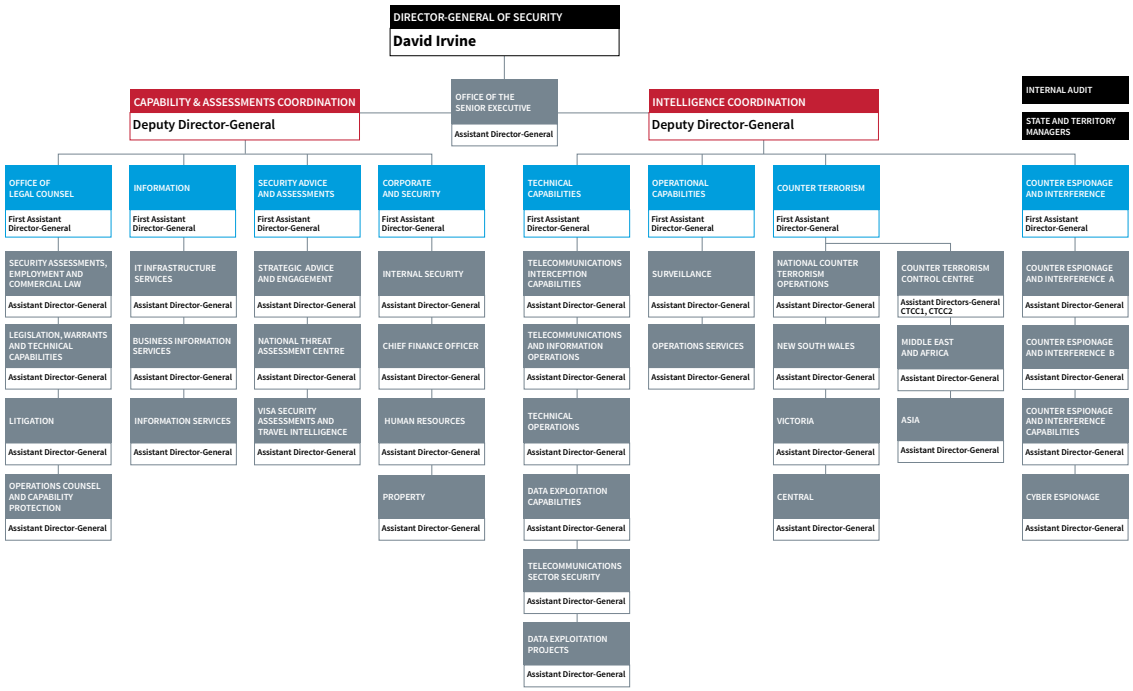
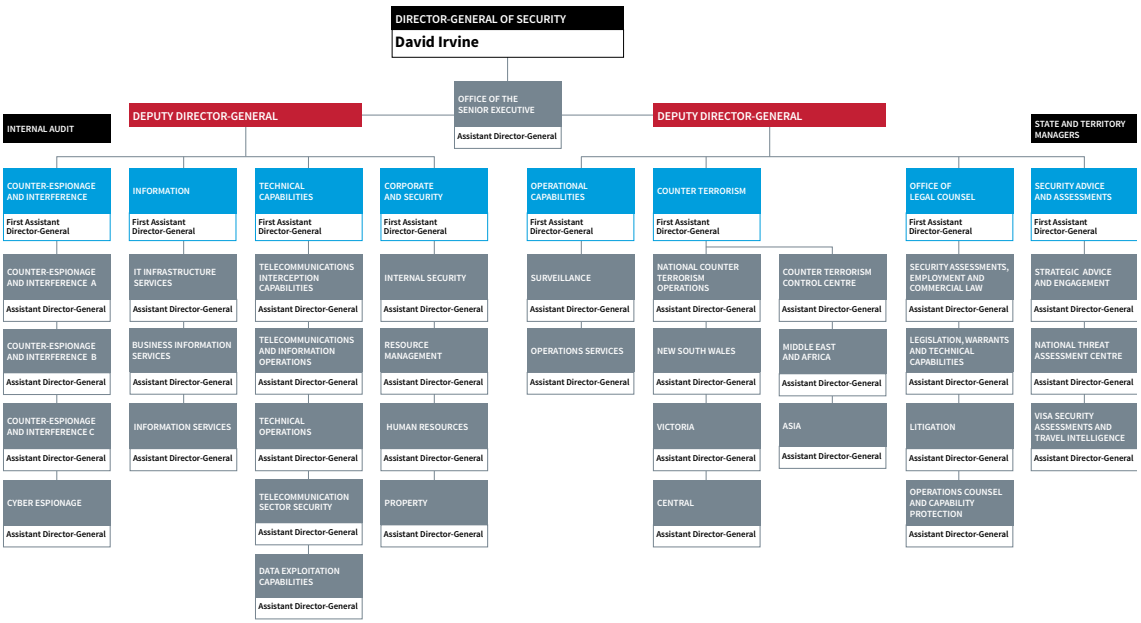


Figure 6: ASIO organisational structure at 30 June 2014



Corporate direction and strategic planning

ASIO strategic planning

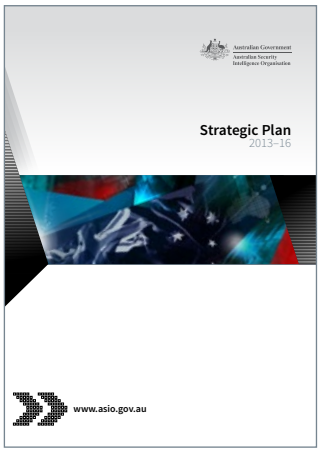
ASIO's *Strategic Plan 2013–16* provides direction on ASIO's vision, mission and goals, ensuring ASIO's activities are directed against identified priorities for the period. It also enables ASIO to respond with agility and resilience to challenges as they emerge in the security environment.

In setting out ASIO's strategic goals, consideration was given to the current priorities, while also recognising that ASIO must consider the capabilities required for the future. This has resulted in goals that rightly place emphasis on capability building of both the workforce and technology required of a security agency.

ASIO's business planning cycle incorporates the strategic plan, ensuring that the identified goals are reflected in the many business priorities of ASIO's divisions and branches.

For 2013–14, the strategic plan prioritised the work of ASIO's governance committees. This has been particularly important with the introduction of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the development and implementation of ASIO's Risk Management Policy.

The strategic plan sets ASIO's direction and forms the basis for much of ASIO's corporate governance arrangements. The plan provides a keystone for people working in ASIO to understand how they contribute to ASIO's mission and the Australian Government's national security strategy—ultimately illustrating the importance of each role in ASIO in working for a more secure Australia.



Corporate governance

The implementation of the PGPA Act brings to focus the importance of ASIO's governance arrangements and the need to ensure that appropriate attention is given to the reporting and evaluation of ASIO's performance.

Over the reporting period an additional committee was established, the ASIO Combined Committee. The Committee ensures comprehensive consideration of ASIO's investment program, and a shared understanding across ASIO's governance committees of events and issues that impact ASIO on a Whole-of-Organisation level.

The addition of the ASIO Combined Committee has resulted in the structure outlined in Figure 7.

Figure 7: ASIO Governance Committee Framework

Director-General of Security

The Director-General of Security is ASIO's executive officer and is responsible for ensuring that ASIO achieves its mission.

Though enacted outside of the reporting period, the PGPA Act determines the Director-General is ASIO's accountable authority and carries those responsibilities set out in the Act. These are:

- The duty to govern the Commonwealth entity;
- The duty to establish and maintain systems relating to risk control;
- The duty to encourage cooperation with others;
- The duty in relation to requirements imposed on others; and
- The duty to keep the responsible Minister and Finance Minister informed.

ASIO's governance structure supports the Director-General in his responsibilities. This includes the provision of reporting and advice on ASIO's budget, Investment Program and corporate risk.

ASIO Executive Board

ASIO's Executive Board is chaired by the Director-General and comprises both Deputy Directors-General and an external member, Ms Jenet Connell, the Chief Operating Officer of the Department of Finance. The role of the external member has been of considerable value over the reporting period, particularly with continued focus on the Government's Public Management Reform Agenda.

The focus of the Executive Board over the period has included reporting on the domestic security implications of the conflict in Syria, the progress on and move to the Ben Chifley Building and the resourcing of ASIO's programs.

The implementation of measures for ASIO's compliance with the PGPA Act will also require Executive Board focus over the 2014–15 period. This includes the roll out of integrated performance and risk reporting across both corporate and intelligence functions.

Intelligence Coordination Committee

The Intelligence Coordination Committee (ICC) provides coordination of ASIO's investigative and assessment priorities and allocation of resources. The ICC also performs the functions of a program board and provides governance for intelligence and related investment projects in ASIO.

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

Workforce Capability Committee

The Workforce Capability Committee (WCC) considers issues relevant to the human resources of ASIO. In doing so, it primarily considers the recruitment, retention, training and education of ASIO's workforce. The WCC also provides a point for escalation of matters arising from the Work Health and Safety Committee.

The WCC is chaired by a Deputy Director-General and is comprised of SES Band 1 and 2 representatives from across ASIO's structure.

Over the reporting period, focus has been given to the recruitment and retention of staff, training of staff, staff safety, and the negotiation of ASIO's 10th Workplace Agreement.

ASIO Security Committee

Security governance in ASIO is overseen by the ASIO Security Committee, where senior executive-level representatives consider and recommend actions for the secure conduct of ASIO business to the ASIO Executive Board.

Finance Committee

The Finance Committee provides assurance to the Executive Board regarding ASIO's financial performance. This includes across ASIO's Investment Program, which is a program of projects, many of which are aimed at ensuring ASIO has the capabilities required to perform its function.

The New Building Committee is a subcommittee of the Finance Committee and provides guidance on the ongoing transition to the Ben Chifley Building.

Audit and Risk Committee

The Audit and Risk Committee (ARC) is a senior corporate committee, comprising three internal and two external members. The ARC provides advice on ASIO's risk management, a range of internal controls and legislative and policy compliance.

In 2012, the Director-General appointed an independent chair to the ARC, underpinning the committee's role in providing independent assurance and advice to the ASIO executive on a range of governance and compliance matters. The independent chair is Ms Lynelle Briggs AO, a distinguished former public servant whose experience includes serving as the Australian Public Service Commissioner and the Chief Executive of Medicare Australia.

The ARC also includes a second external agency member position, occupied during the reporting period by Mr Roman Quaedvlieg, Chief Executive Officer of Australian Customs and Border Protection Service. The attendance of ANAO observers at each meeting further reinforces the independence of the committee.

Consistent with the ANAO's *Better Practice* guide on audit committees, ASIO conducted a biennial performance review of the ARC. Overall, the review found that the committee's performance was sound. Recommendations centred on enhancing committee administration and member induction and training, as well as incorporating changes relating to the introduction of the Public Governance, Performance and Accountability rules. The ARC endorsed the review findings and ASIO implemented all recommendations.

The ARC oversaw the development of a risk management policy that covers the corporate and operational functions of ASIO and was near completion in the reporting period. The ARC expects the policy to be integrated into the existing risk management framework, augmenting existing risk management guidance documentation.

The ARC has considered all audits undertaken by ASIO's Internal Audit Directorate during the period. The committee has monitored and reviewed ASIO's response and action in relation to recommendations or significant issues raised in internal or external audit and review reports and *Better Practice* guides. For further information on the audits and reviews considered by the committee, see following 'Audit and Evaluation'.

Audit and evaluation

ASIO's Internal Audit (IA) Directorate undertakes audits of business areas and processes to improve ASIO performance and ensure the Organisation is meeting legislative, regulation and policy requirements. In 2012–13, the IA Directorate audited ASIO's compliance with the requirements of the *Work Health and Safety Act 2011*. The audit recommended that a follow-up audit be conducted to assess the outcomes of a number of projects underway at the time. IA Directorate conducted the follow-up audit in the reporting period and found ASIO had:

- made improvements in the area of work health and safety policy development and guidance material;
- expanded the Health and Safety Representative role; and
- implemented a health and safety inspection program.

During the reporting period, the Directorate also evaluated whether decision-making responsibilities are delegated to the appropriate level to meet both legislative and operational requirements. The audit confirmed that ASIO's corporate governance structures support the reporting and accountability of decision making, and ensure that the Executive Board maintain awareness of the strategic and operational information required. Recommendations were made to support agility in decision making while continuing to meet the need for demonstrable controls.

In 2013–14, ASIO continued to conduct compliance audits to ensure the Organisation conformed to privacy requirements and agreements made with external partners. ASIO also continued to formalise existing informal arrangements in order to promote a better compliance framework and provide accountability for, and assurance of, internal controls.

In the reporting period ASIO introduced an additional annual compliance audit. This audit focused on ASIO's Rehabilitation Management System and arose from new requirements in the *Safety Rehabilitation and Compensation Act 1988*. The audit sought to establish whether ASIO was using the framework of the legislation and the *Guidelines for Rehabilitation Authorities 2012* to manage the return to work of its injured employees. The audit found ASIO was meeting the requirements of the framework and the guidelines.

Fraud control

In preparation for the introduction of the *Public Governance, Performance and Accountability Act 2013* and associated rules on 1 July 2014, ASIO reviewed its fraud policies and guidance documents. In the reporting period, IA Directorate also developed the *ASIO Fraud Management Guidelines* to provide staff with specific guidance on the Commonwealth fraud control policy framework, ASIO's fraud control and management arrangements and fraud allegation reporting procedures. ASIO received one allegation of fraud, which was dealt with through the *Public Interest Disclosure Act 2013*, investigative process. ASIO provides fraud awareness training for all new employees and contractors. All staff must complete an e-learning training module on fraud awareness every three years.

Communication and leadership meetings

Senior Executive Meeting

The Senior Executive Meeting is a weekly meeting attended by officers at the SES Band 2 and above to discuss emerging issues. It is chaired by the Director-General of Security.

Senior Executive Service Meeting

The monthly Senior Executive Service Meeting provides a forum for officers at the SES Band 1 and above to discuss key strategic issues affecting ASIO and ensure messages are communicated.

ASIO Consultative Council

The ASIO Consultative Council was established to enable management and staff of the Organisation to meet regularly in a structured way to discuss and resolve issues of interest and concern.
Over the reporting period the ASIO Consultative Council received updates regarding

- the Australian Government Employment Bargaining Framework
- ASIO's first consolidated Determination of Terms and Conditions of Employment
- the ASIO staff survey.

Human resource management

Recruitment

In 2013–14, ASIO continued with downsizing activities, a result of recommendations from the internal *Review of the Staffing and Resource Allocation (2012–13).* The focus for recruitment for the reporting period was limited to the difficult-to-fill roles of intelligence officer, technical officer and security assessor positions. There was no recruitment action for roles other than these. ASIO implemented a new advertising strategy for intelligence officers during 2013–14, attracting 1049 applications for one recruitment campaign, an increase of approximately 40 percent on the previous campaign. Applicants progress through a number of selection processes including assessments centres, individual interview and security vetting to ascertain suitability.

ASIO also introduced a new technical officer graduate program to attract and develop entry-level staff in specialist areas. The program will provide graduates with skills and knowledge required for roles in ASIO's technical areas.

Training and development

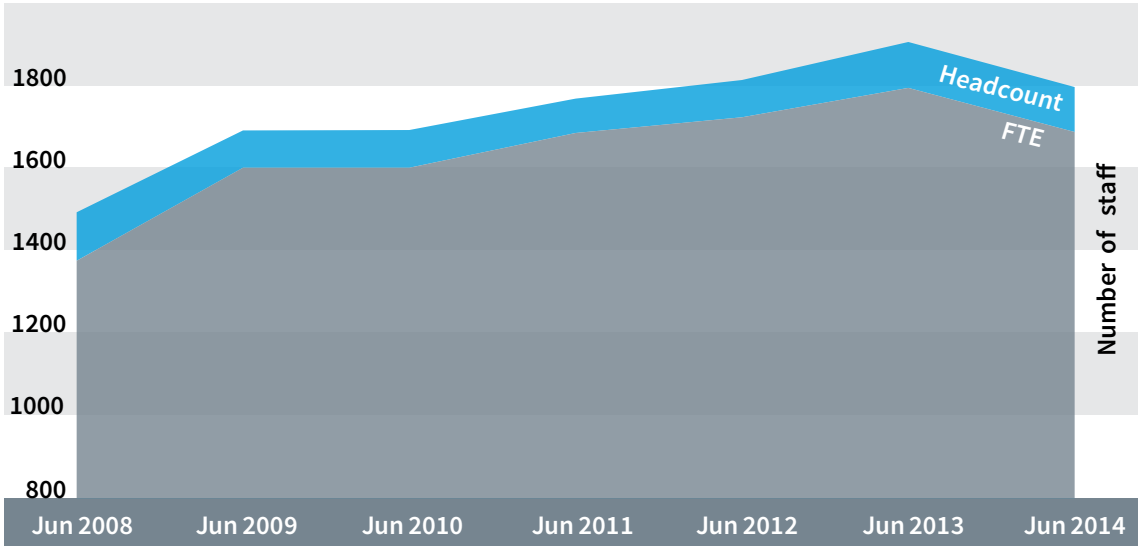
ASIO established a new Training Branch in July 2014 to better service the Organisation's growing training needs. The structure of the Branch has been designed to enhance ASIO's existing training and the associated foundational policy and doctrine.

Intelligence training

Two Intelligence Development Programs (IDPs) were conducted over the reporting period. An important feature of ASIO's intelligence training is the provision of specific training modules to officers who identify a need in order to perform aspects of their role. ASIO provided an additional 102 instances of analytical and operational training to these officers of between five days and three weeks duration over the period.

Significant planning was also undertaken in September/October 2014 to remodel the existing IDP to cater for an anticipated increase in intelligence officer intakes. The new IDP model will form the basis of the January 2015 IDP intake.

Figure 8: Staffing growth



Additionally, the Training Branch is also focused on the provision of further specialised training to intelligence officers in a range of analytical and operational roles in the workplace. These additional training opportunities are currently under development for delivery in 2014–15.

Corporate training

ASIO provides training and development opportunities throughout an officer's career. These programs can be specific to an officer's role or Organisation-wide mandatory training to ensure standard level of training. Corporate training activities include:

- an induction program for all new starters to explain ASIO's role and functions, the nature of the security environment and the standard of behaviour expected of ASIO officers;
- administrative training including contract and finance management, procurement, and communication;
- information technology training, including training on ASIO's various systems and databases;
- mandatory training, including security awareness, ethics and accountability, public interest disclosure, work health and safety, and workplace behaviour, to ensure all ASIO officers behave in accordance with the key principles and standards of the Australian Public Service and ASIO; and
- discipline-specific courses including social, cultural, political and religious history and influences.

In light of the heightened counter terrorism threat environment, significant investment has also been made into the design, development and delivery of a Whole of Organisation officer safety and security training program. The program provides a tiered training approach linked to officers' roles, functions and specific operating environment. At the base of the program is a new *Personal Safety and Security Workshop* for all staff to provide an updated appreciation of the threat environment, revision of ASIO's security protocols and procedures including physical security measures and situational awareness principles to manage personal safety and security.

Management and leadership skills

In 2013–14, ASIO began implementing the *Management and Leadership in Security Intelligence Strategy (2013-16)*. The strategy focuses on the management and leadership behaviours and skills required of current and future ASIO leaders, providing a framework for talent management and succession planning.

As part of the strategy, ASIO has introduced three management programs, two of which are run with Australian Intelligence Community agency partners. The Introduction to Management Program is aimed at high performing first time managers and ASIO Executive Officer (AEO) 1 officers and focuses on the introductory fundamentals of management responsibilities, principles and practices. ASIO has run three programs in the reporting period.
The Mastering Management Program is targeted at high potential and high performing AEO2 and AEO3 officers and is designed to develop capabilities required to effectively manage self and others in the current and future working environment.
ASIO ran one program in the reporting period.

Language training

Maintaining and improving ASIO's language capabilities is crucial to its ability to conduct effective counter-terrorism, counter-espionage and foreign intelligence operations.

In addition to its linguist capability, ASIO also utilises the language skills of its officers working in other disciplines. To this end, ASIO's Language Skills Development Program provides support to officers interested in enhancing their language skills in operationally relevant languages. In the current reporting period the program provided support to 55 officers (which has risen from 26 during the last reporting period) across a range of languages.

e-learning

ASIO's suite of e-learning modules provides a convenient and effective way to deliver training to ASIO officers across a range of disciplines, including work health and safety, workplace behaviour, ethics and other mandatory training requirements. ASIO's e-learning modules continue to be updated as required to ensure currency and maintain best practice.

ASIO reviewed the current catalogue and removed out of date courses and updated the content on others. The redevelopment of key mandatory modules is currently underway.

Study Support Program

ASIO's Study Support Program assists officers in their endeavours to undertake further professional development in disciplines relevant to their roles in ASIO and broader government.

The program continues to be well subscribed. In 2013–14, 166 officers participated in ASIO's Study Support Program over the course of the year. Fields of study include business management and strategic studies, security and policy, engineering, commerce, project management and information technology.

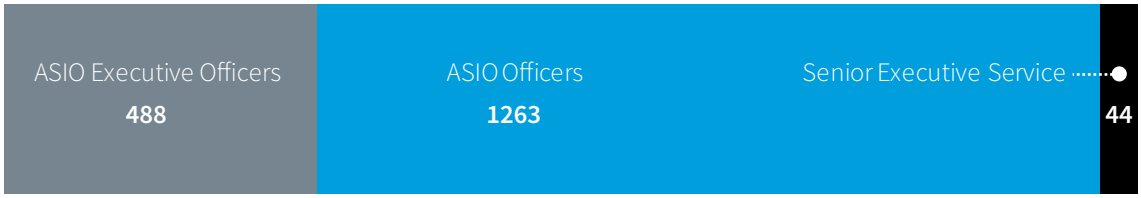
National Intelligence Community training

ASIO considers shared training opportunities within the National Intelligence Community (NIC) to be a valuable way to improve understanding of and cooperation between NIC agencies. During the reporting period, ASIO continued to actively contribute to NIC training as a presenter and a participant.

ASIO makes available places for other agencies to participate in ASIO training courses and holds the ASIO Partnership Forum to provide a greater understanding of ASIO's work to individuals within the NIC (and more broadly) who work on a regular or semi-regular basis with ASIO.

ASIO also enables officers to participate in courses offered by the Australian National University's National Security College to develop a deeper understanding of national security challenges and provide an opportunity for further executive and professional development.

Figure 9: Ratio of staff



Workforce

At the end of the reporting period, 30 June 2014, ASIO had 44 Senior Executive Service (SES) officers, 488 AEO 1, 2 and 3 officers and 1263 other officers at APS 1–6 equivalent.

Equity and diversity

ASIO recognises that positive outcomes are achieved by a workplace with a diverse range of skills, cultural perspectives and backgrounds. In 2013–14, ASIO broadened its policy work in support of equity and diversity, and revitalised its Harassment and Discrimination Advisor (HaDA) Network including expanding the network and providing training to all advisors; and the development of staff and manager guides. In September 2014, ASIO conducted a Gender Equity staff survey, the outcomes of which will inform further work in 2014–15.

ASIO's diversity statistics are reflected in the table below.

Table 1: 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)	44	11	0	0	1	44
Senior Officers [3]	488	185	16	2	6	488
AO5 [4]	646	323	51	3	7	639
AO1 – 4 [5]	516	258	26	2	2	509
Information Technology Officers Grades 1 and 2	93	14	5	1	3	93
Engineers Grades 1 and 2	8	0	0	0	0	8
Total	**1,795**	**791**	**98**	**8**	**19**	**1,781**

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 Officer grade 5 group translates to APS Level 6.*
5 *Translates to span the APS 1 to 5 classification levels.*

Figure 10: The gender breakdown of ASIO staff by classification level

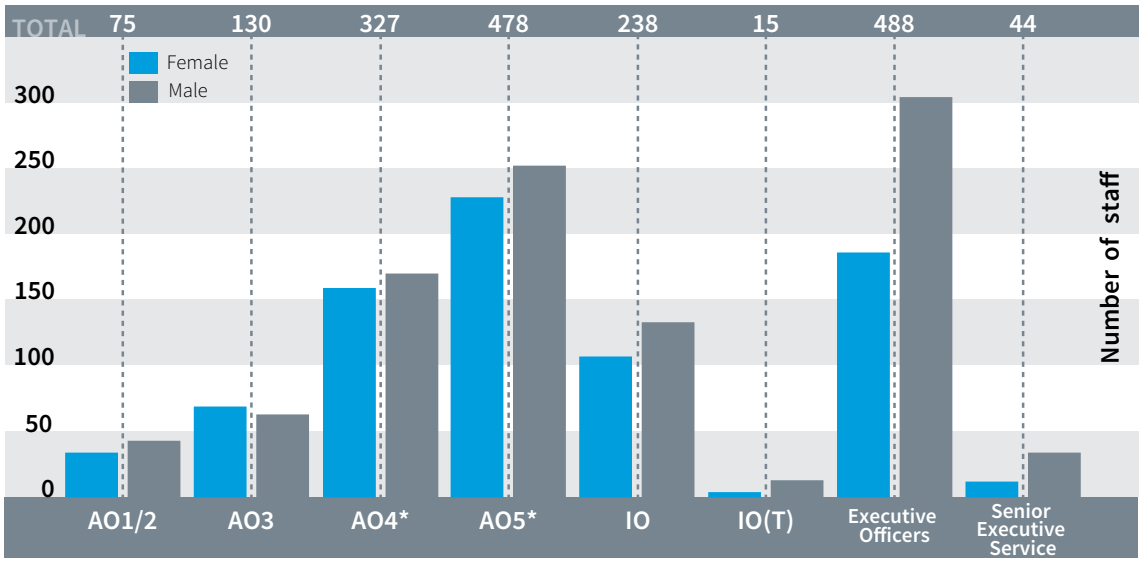


Figure 11: The age profile and tenure of ASIO staff

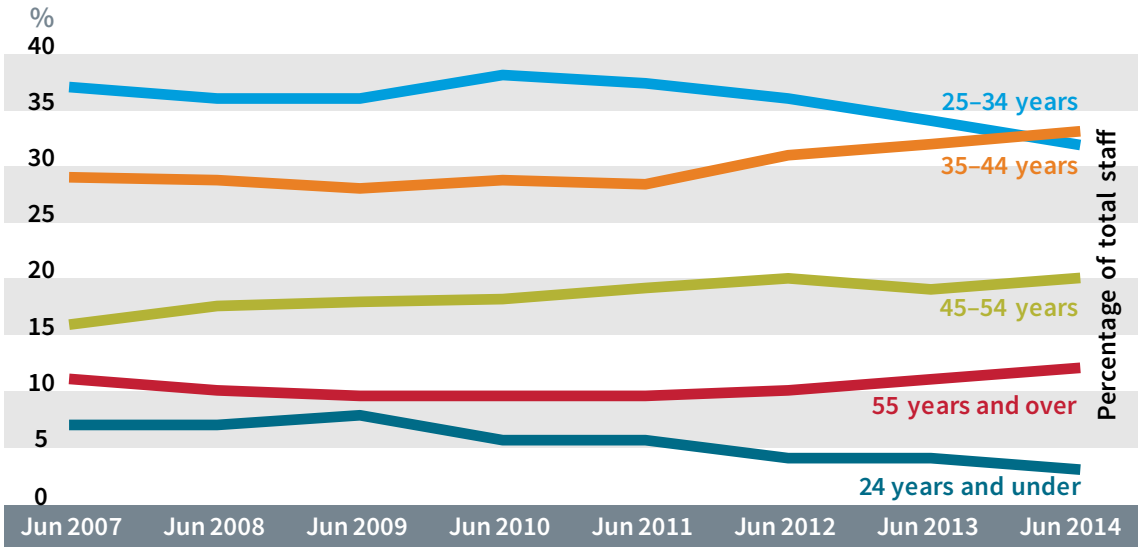


Figure 12: Staff length of service

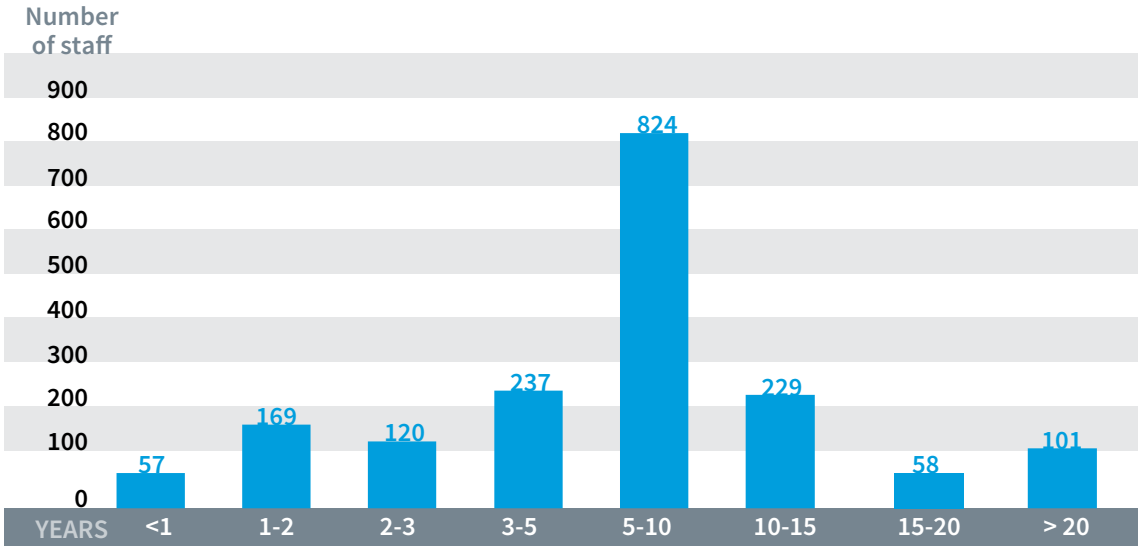


Figure 13: Separation by reason

Redundancies

In 2013–14, a voluntary redundancy program was initiated as part of a workforce reshaping and rebalancing strategy. There were 34 Executive Level voluntary redundancies as well as four Senior Executive Service voluntary redundancies.

Attachments

During the reporting period ASIO remained 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
- Western Australia Police.

In determining potential secondments, ASIO identifies opportunities to mutually enhance strategic and operational outcomes.

Staffing and personnel matters

In 2010 ASIO appointed its first external Ombudsman. The Ombudsman's goal is to seek to resolve disputes impartially, informally and quickly through advice, consultation and mediation.

In 2013–14, Human Resources Branch managed 118 formal personnel matters including support for injured workers (including compensation cases), misconduct matters and under performance processes.

Table 2: Formal personnel matters

Case category	Number of cases
Early intervention support for workers with non-work-related injuries/illnesses	42
Early intervention support for workers with work-related injuries/illnesses (did not proceed to workers' compensation claim)	23
Workers' compensation	36
Administrative Appeals Tribunal	4
Misconduct	9
Underperformance	4

Table 3: Misconduct

Specific element [1]	Number
Contravened or failed to comply with a term or condition of employment, including the ASIO Values or the Code of Conduct	8
Been inefficient or lacks diligence in the performance of his or her duties	5
Been negligent or careless in the performance of his or her duties	4
Engaged in dishonest or misleading behaviour	0
Engaged in conduct that adversely affects the performance of his or her duties or has the potential to bring the Organisation into disrepute	4
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

Performance management

ASIO's performance management framework —Enhancing Performance—aims to create 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.

During 2013–14 a total of four employees participated in the Organisation's formal underperformance management process.

Misconduct

During 2013–14, ASIO completed a total of nine misconduct investigations all resulting in a charge of misconduct. This represents approximately half of one percent of all staff.[2]

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

2 Based on an average headcount for 2013–14 of 1844.

Legislation

Legislative amendments

Throughout 2013–14 ASIO worked collaboratively with other Australian Government agencies to advocate for amendments to Australia's legislative framework that would support ASIO's functions and capabilities within a Whole-of-Government agenda. Legislative reform of relevance to ASIO and progressed during the reporting period is detailed below.

Review of national security legislation

During the reporting period, ASIO worked with the Attorney-General's Department (AGD) to inform the Australian Government's response to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of national security legislation. ASIO undertook a significant amount of work during the reporting period as part of preparation of the National Security Legislation Amendment Bill (No.1) 2014. The Bill was introduced by the Attorney-General on 16 July 2014, outside of the reporting period.

The Bill gives effect to important recommendations in Chapter 4 of the PJCIS's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

The Bill was referred back to the PJCIS to scrutinise whether it appropriately implemented the Committee's recommendations and to assess the balance of national security and safeguards proposed in the Bill. Outside the reporting period, ASIO provided a written submission to the PJCIS inquiry in relation to the Bill, assisted AGD to prepare supplementary submissions to the PJCIS inquiry and appeared before the PJCIS inquiry in both a public hearing on 15 August 2014 and closed hearing on 18 August 2014.

The Bill received Royal Assent on 2 October 2014, outside the reporting period. The measures of the Bill directly affecting ASIO commenced on 30 October 2014. The key amendments intend to:

- improve the scope and effectiveness of ASIO's special powers;
- modernise ASIO's employment provisions;
- introduce a special intelligence operations scheme;
- enhance cooperation between ASIO and Australian Secret Intelligence Service (ASIS) overseas; and
- create and update secrecy offences in the ASIO Act and *Intelligence Services Act 2001*.

ASIO believes this legislative reform is critical to ensuring ASIO is equipped to carry out its mandate in the face of rapidly changing security environments.

Migration Amendment Bill 2013 inquiry

On 12 December 2013, the Senate referred the Migration Amendment Bill 2013 to the Legal and Constitutional Affairs Legislation Committee for inquiry and report. The Director-General of Security provided evidence at a confidential hearing of the inquiry on 4 February 2014, addressing questions from committee members relating to ASIO's security assessments for protection visa applicants, caseload numbers, internal reviews of security assessments, and the Independent Reviewer of Adverse Security Assessments.

The Bill was passed by Parliament, and the *Migration Amendment Act 2014* came into effect on 2 June 2014. This Act:

- amends the *Migration Act 1958* so that a protection visa can be issued only where the applicant is not the subject of an adverse security assessment (other than under the Minister's discretionary powers);
- confirms that an individual who has had their visa application refused due to an adverse security assessment is unable to appeal to the Refugee Review Tribunal, the Migration Review Tribunal or the Administrative Appeals Tribunal (AAT);
- does not affect a visa applicant's right to seek judicial review of an adverse security assessment under the original jurisdiction of the High Court of Australia; and
- does not remove the discretionary power of the Minister for Immigration and Border Protection to issue a visa to any person in immigration detention, regardless of whether ASIO has issued an adverse security assessment.

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

In December 2013, the Senate referred a comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to the Legal and Constitutional Affairs References Committee. The inquiry is focusing on previous recommendations relating to the TIA Act made by the Australian Law Reform Commission in its 2008 review of Australian privacy law and practice; and those made by the PJCIS in its *Report of the inquiry into potential reforms of Australia's national security legislation*.

During the reporting period, ASIO made an unclassified submission to the inquiry, highlighting the importance of telecommunications interception and data to ASIO's activities and the growing challenges ASIO faces in maintaining access to this information. Outside of the reporting period, ASIO appeared before the Committee and the Committee also accepted ASIO's offer of a classified briefing.

Information Privacy Act 2014 (ACT)

The Information Privacy Bill 2014 (ACT) was passed by the Legislative Assembly of the Australian Capital Territory (ACT) on 3 June 2014. It was introduced to regulate the handling of personal information (other than personal health information) by public sector agencies in the ACT.

During the reporting period, ASIO advised the ACT Government that the Bill, as it was first presented to the Assembly, would in many circumstances prevent ACT public sector agencies disclosing to ASIO personal information relevant to security that would assist in the collection of security intelligence. ASIO argued that the Bill should be amended to better enable ACT public sector agencies to disclose personal information to ASIO for the purposes of ASIO performing its function of collecting intelligence relevant to security. As a result of submissions by ASIO, the ACT Government proposed amendments to the Bill to allow ASIO appropriate access to personal information in connection with ASIO's functions. The *Information Privacy Act 2014* (ACT) now includes provisions under which public sector agencies can disclose personal information to ASIO in connection with the performance of ASIO's functions.

Legislation on assumed identities

With the support of AGD, ASIO has been pursuing amendments to state and territory legislation on assumed identities (AI) to enable ASIO to acquire evidence of AIs (e.g. birth certificates) where such evidence is administered by State and Territory agencies (e.g. Births, Deaths and Marriages (BDM) registers). In particular, although ASIO obtains authority to acquire evidence of, and use, AIs under Commonwealth legislation, ASIO needs to rely on State and Territory AI laws to support the issue of evidence of AIs where such evidence is administered by State and Territory agencies. During the reporting period, submissions by ASIO resulted in amendments to NSW, ACT and Victorian legislation on AIs.

New South Wales

The *Law Enforcement and National Security (Assumed Identities) Act 2010* (NSW) was amended on 23 August 2013 to allow the Director-General of Security to apply for an order for entry of an AI in the NSW BDM register. The legislative amendments also ensure that sensitive information is protected by requiring that the applications be heard in chambers and not in open court.

Australian Capital Territory

The *Crimes (Assumed Identities) Act 2009* (ACT) was amended on 10 December 2013 to allow the Director-General of Security to apply for an order for entry of an AI in the ACT BDM register.

Victoria

The *Crimes (Assumed Identities) Regulations 2006* (VIC) was amended on 15 July 2013, declaring Part IAC of the *Crimes Act 1914* (Cwlth) a corresponding law. This means ASIO can rely on the *Crimes (Assumed Identities) Act 2004* (VIC) to apply for orders for entry, or cancellation of entry, of an AI acquired under a Commonwealth AI authority in the Victorian BDM register, and to support the acquisition/cancellation of other evidence of an AI authorised by a Commonwealth AI authority.

These amendments represent a significant outcome for ASIO in the protection of the identity of its employees and people.

Independent National Security Legislation Monitor

The Office of the Independent National Security Legislation Monitor (INSLM) was established by the *Independent National Security Legislation Monitor Act 2010* to assist ministers in ensuring Australia's counter-terrorism 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.

During the reporting period the INSLM's third and fourth annual reports were tabled in Parliament, on 12 December 2013 and 18 June 2014 respectively. The reports include detail of the outcomes of the INSLM's examinations of the legislation which is designed to:

- counter-terrorism financing and prevent Australians participating in offshore conflicts
- address issues in the existing legislation that may adversely affect the investigation and prosecution of terrorism offences or the identification and investigation of security threats.

ASIO provided submissions and evidence in private hearings to the INSLM on these matters, and the INSLM's reports made several recommendations relating to ASIO's activities:

- amending ASIO's questioning powers to include offences against the *Charter of the United Nations Act 1945*
- introducing the ability for an interim passport suspension to be approved by the Director-General of Security, including suspending the capacity to use a foreign passport
- introducing a legislative 'special intelligence operation' scheme where ASIO officers and human sources are protected from criminal and civil liability for certain conduct in the course of intelligence operations
- amending the *Intelligence Services Act 2001* to streamline intelligence cooperation between ASIO and ASIS—that is, not requiring a ministerial authorisation for requests to ASIS, Australian Signals Directorate and Australian Geospatial-Intelligence Organisation where it is at the request of the Director-General of Security and is for the purpose of assisting ASIO in the performance of its functions
- introducing a power for the Minister for Immigration and Border Protection to revoke the citizenship of Australians on security grounds, where to do so would not render the individual stateless
- amending the name or alias of a proscribed terrorist organisation without having to conduct the proscription process from the beginning.

The PJCIS separately considered several of these issues, and shortly after the reporting period the Australian Government introduced the National Security Legislation Amendment Bill (No. 1) 2014 into Parliament to amend Australia's national security legislation.

Public Interest Disclosure Act 2013

The *Public Interest Disclosure Act 2013* (PID Act) came into effect on 15 January 2014 and provides agencies and whistleblowers with procedures to follow in making a 'public interest disclosure', and protections for those who make such disclosures in accordance with the scheme.

ASIO undertook a large amount of work in reviewing draft legislation, briefing other departments on the practical application of proposed provisions in an intelligence context, and advising relevant ministers and departments of potential issues associated with the enactment of particular provisions.

ASIO has developed an internal framework for the implementation of ASIO's PID Act obligations. This includes chairing a regular meeting of intelligence agencies to address the particular implementation issues in an intelligence context and liaising closely with the IGIS to ensure ASIO's compliance with both the letter and the spirit of the law. ASIO also developed internal PID related policy and procedures, provided training for all staff on the PID Act and the processes within ASIO, and provided specific training for authorised officers about their role in receiving PIDs. Comment from the Office of the IGIS has been that the implementation of the PID Act in ASIO has been very positive.

During the reporting period, two disclosures were received and allocated to an investigating authority. One of the allocated disclosures was withdrawn by the discloser prior to investigation, and the second resulted in an investigation reviewing internal processes. The completed public interest disclosure investigation produced recommendations aimed at improving organisational effectiveness and increasing overall accountability.

Use of ASIO special powers

In the performance of its functions it is sometimes necessary for ASIO to use highly intrusive methods of investigation, these include: telecommunications interception and access; use of surveillance devices; entry and search of premises; computer access; and the examination of postal and delivery service articles. All of these activities require a warrant issued by the Attorney-General.

These activities are authorised under and must satisfy the strict thresholds in the ASIO Act or the *Telecommunications (Interception and Access) Act 1979*. The ASIO Act also enables ASIO, with the Attorney-General's consent, to seek warrants from an independent 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.

All ASIO warrants must also comply with the *Attorney-General's Guidelines*, and in particular follow the principles 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

In 2013–14, ASIO was involved in over 50 litigation matters, primarily criminal prosecutions, including for terrorism and foreign incursion offences, and judicial and administrative reviews of ASIO security assessments. The Administrative Appeals Tribunal (AAT) reviewed three ASIO security assessments, along with the consequential administrative decisions by other agencies. All since have been upheld. Judicial review included a number of complex matters involving various Commonwealth agencies in the Federal and High Courts of Australia. One matter was heard by the International Court of Justice in the Hague.

An important ASIO consideration remained the protection of sensitive national security information sought as evidence or required to be disclosed to defendants and applicants, while facilitating its disclosure as required by law and the interests of justice. The Office of Legal Counsel, a Division of ASIO, worked closely with ASIO operational areas and external stakeholders and legal representatives to balance protection of ASIO investigations, capabilities, methodologies, officer and source identities, and foreign liaison relationships with court requirements and the principles of open justice.

Key matters

BLBS, AAT Melbourne

ASIO assessed BLBS, a dual Australian/Lebanese citizen intercepted while attempting to travel to Yemen to engage in militant jihad, as a threat to security. The Minister for Foreign Affairs canceled his Australian passport and ordered surrender of his Lebanese travel document. On 28 November 2013, the AAT affirmed ASIO's security assessment, finding reasonable grounds to suspect BLBS would be likely to engage in conduct which might prejudice the security of a foreign country were he allowed to travel abroad.

CXQY, AAT Sydney

CXQY, a Jordanian national with a permanent spousal visa, sought review of his adverse security assessment recommending the Minister for Immigration refuse his application for Australian citizenship. ASIO assessed that CXQY intended to travel overseas, using an Australian passport once he obtained it, to undertake militant training and engage in acts of politically motivated violence in Israel. On 16 December 2013, the AAT upheld ASIO's assessment.

MYVC, AAT Sydney

ASIO assessed that MYVC was engaged in organised people smuggling. On 28 July 2014, the AAT affirmed ASIO's security assessment and the Minister for Foreign Affairs' passport cancellation decision. It found that organised people smuggling poses a serious threat to Australia's border integrity and therefore falls within the definition of 'security' in the ASIO Act. Following the reporting period MYVC unsuccessfully appealed in the Federal Court of Australia.

Sayed Akbar Jaffarie, Full Federal Court

Mr Jaffarie challenged ASIO's assessment that he was engaged in organised people smuggling, along with the constitutional validity, scope and meaning of the border protection head of security in section 4 of the ASIO Act. After the reporting period, on 18 August 2014, the Full Federal Court of Australia dismissed Mr Jaffarie's application and found that ASIO had not denied him procedural fairness. He sought leave to appeal in the High Court of Australia.

Milad al-Ahmadzai and others (various criminal prosecutions)

In 2013, a number of ASIO investigative targets were charged with criminal offences. Although the offences did not all relate to national security, sensitive ASIO information was sought and provided as part of the briefs of evidence.

- Milad al-Ahmadzai was arrested and charged with *Criminal Code* offences in relation to threats made over the telephone to an ASIO officer and a NSW Police officer. He pleaded guilty and was convicted and sentenced to eight months (commencing 20 March 2014 and expiring 19 November 2014) in respect of the threat to cause serious harm to a Commonwealth officer, and three months (commencing 20 February 2014 and expiring 17 May 2014) in respect of using a carriage service to menace/harass.
- Mr al-Ahmadzai and Fadi Alameddine were charged with attempting aggravated break and enter with intent to steal, and taking a conveyance without consent, under the *Crimes Act 1900 (NSW)*. The charges related to their alleged involvement in the attempted theft of an automated teller machine. The trial is listed for September 2015.
- Mr al-Ahmadzai, Mr Alameddine, Wesam Hamze and Osama Toffic were charged with various offences under the *Crimes Act 1900 (NSW)* relating to a shooting outside Aarows club, including shooting with intent to kill and shooting with intent to cause grievous bodily harm (both carrying a maximum 25 year sentence).

Foreign incursions prosecutions

ASIO information has been provided for use in each prosecution under the *Crimes (Foreign Incursions and Recruitment) Act 1978*. ASIO information has been provided for use in each prosecution.

- On 3 December 2013, Hamdi Alqudsi was charged with seven counts of promoting/supporting the entry of persons into Syria.
- On 23 January 2014, Mohamed Ali Baryalei was charged with engaging in hostile activity in a foreign state, and a warrant was issued for his arrest.
- On 27 March 2014, Mostafa Mahamed Farag was charged with engaging in hostile activity in a foreign state, and a warrant was issued for his arrest.

Timor-Leste v Australia, International Court of Justice (Legal-in-Confidence)

On 17 December 2013, Timor-Leste instituted proceedings against Australia claiming that ASIO's removal of documents and data from lawyer Bernard Collaery's premises under warrant on 3 December violated Timor-Leste's sovereignty and property and other rights under international law. It also sought interim 'provisional measures' that Australia return the material uncopied and unexamined, and apologise.

The International Court of Justice (ICJ) on 3 March 2014 provisionally ruled that Australia must:

- ensure the content of the seized material not be used to the disadvantage of Timor-Leste until conclusion of this case
- keep the seized material under seal until further decision of the ICJ
- not interfere in any way in communications between Timor-Leste and its legal advisers in connection with the arbitration between Timor-Leste and Australia, any future bilateral negotiations concerning maritime delimitation, or any other related bilateral procedure including the present case.

ASIO contributed to AGD's handling of the provisional measures hearing, and the subsequent preparation of and response to submissions for the substantive hearing. That was scheduled for 18-25 September 2014 but deferred on the basis of negotiations between the Foreign Ministers of Australia and Timor-Leste.

Security of ASIO

A strong security culture underpins ASIO's ability to carry out its mission to protect Australia, its people and its interests and is essential to the Organisation effectively meeting its obligations. Sensitive information must be protected so that it cannot be accessed by those who wish to do Australia harm. Our allied partners and members of the public would be less willing to communicate information to ASIO if these strong security practices were not in place.

ASIO is committed to protecting ASIO officers, premises, information and assets from compromise. This is achieved through adherence to a best practice security model which meets Australian Government requirements and is further strengthened to mitigate the specific risks that face a security intelligence agency. ASIO continually reviews its security policies and procedures to ensure a robust and resilient security culture.

In 2013–14 ASIO continued to work closely with other government agencies to provide advice to both the government and private sector to mitigate threats to security.

ASIO's information and communications technology security program provides assurance that ASIO's information systems are being used in an authorised, secure and appropriate manner, through audits, investigation of IT security incidents and IT security policy and advice.

Security governance and policy

ASIO complies with the Australian Government's Protective Security Policy Framework's (PSPF) requirements for the management and oversight of the Organisation's protective security, and develops policies aligned with this framework. ASIO also has internal security policies and procedures specific to the Organisation's unique security environment.

These policies and procedures are continually reviewed to ensure they remain current and relevant. New or significantly altered policies are communicated to staff via security education and awareness campaigns.

The ASIO Security Committee oversees security governance in ASIO, where SES representatives consider and recommend actions for the secure conduct of ASIO business to the ASIO Executive Board. For further information on committees, see 'Corporate direction and strategic planning' pages 20–25.

ASIO has significantly increased engagement with the Australian Government—at both executive levels and with agency security advisors—to raise awareness of the malicious insider threat. Malicious insiders are trusted employees and contractors who deliberately and wilfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.

Of note, ASIO has used its investigative and personnel security assessment experience, and that of its allied partners, to inform the development and implementation of robust policy and procedures to strengthen the Australian Government's defence against the malicious insider threat. The Organisation has worked closely with key agencies, including the AGD, the Department of the Prime Minister and Cabinet and the Department of Defence, on personnel security policy reforms and other associated policy initiatives. ASIO's focus has been to simultaneously address:

- access—the suitability of clearance holders and the need for comprehensive and robust vetting, revalidation and clearance maintenance processes
- accessibility—ensuring systems and processes appropriately restrict access to information to a 'need to know' while not inhibiting secure and effective government business processes.

This work will be the focus of continued effort over the next reporting period, but it has already resulted in significant improvements in personnel security outcomes and an increased awareness of the potential threat to the security and integrity of government business.

Security clearances in ASIO

Pressures on ASIO's initial vetting and revalidation continued over the reporting period. ASIO is proactively seeking ways to become more efficient in security vetting processes, without compromising the high standards of ASIO security practices. Initial and ongoing security vetting of ASIO staff provides a critical counter-intelligence function and is conducted in line with Whole-of-Government requirements, security risk management strategies, policies and procedures. As clearance holders, ASIO officers must maintain clearance suitability and proactively report on any matters which may affect their clearance.

Security breaches

ASIO strives to uphold the highest standard of security practice, including the reporting of security breaches. ASIO is required to report annually on its security status, including security breaches, to the Secretaries' Committee on National Security and the National Security Committee of Cabinet.

Relevant senior managers in ASIO are notified of breaches which occur within their branch or division to enable proactive management of each occurrence. Multiple breaches by the same individual within a 12 month period attract more significant consequences, from formal counselling to misconduct sanctions. An ASIO officer's security breach history over the previous twelve month period may also be taken into account when considering the officer's suitability for internal promotion or posting.

ASIO continually modifies and enhances its e-security capabilities to ensure its information technology systems are adequately protected from both accidental and malicious activity. ASIO employs a range of policies and practices in regards to ICT systems to ensure vulnerabilities are avoided where possible and remedied when needed.

Management of relationships and public reporting

Parliamentary oversight

Attorney-General

ASIO is responsible to the Australian Government through the Attorney-General, as outlined in the ASIO Act. ASIO informs the Attorney-General of significant national security developments. During the reporting period, ASIO provided advice to the Attorney-General on a range of issues connected to the security environment, specific investigations and operations, and administrative matters relevant to ASIO, primarily communicated through just under 300 submissions.

In March 2014, ASIO also introduced a weekly written brief for the Attorney-General to capture issues 'for noting' rather than 'for approval'. This primarily forward looking brief, included 61 items throughout the reporting period.

ASIO's operational activity is conducted in accordance with the *Attorney-General's Guidelines*, last updated by the Attorney-General on 10 December 2007 under sections 8A(1) and 8A(2) of the ASIO Act. The guidelines stipulate that ASIO's information collection activities should be conducted in a lawful, timely and efficient manner, using the least intrusion necessary into an individual's privacy and proportionate to the gravity of the threat being investigated.

All ASIO warrants (other than questioning and detention warrants, which are issued and approved by a person as specified under Part III, Division 3 of the ASIO Act) are issued by the Attorney-General after consideration of a request presented by the Director-General of Security. For every warrant raised, ASIO is required to report to the Attorney-General on the extent to which action undertaken in respect of the warrant assisted the Organisation in carrying out its functions.

Report to Parliament

ASIO's *Report to Parliament* contains an account of ASIO's performance across its functions during the previous 12 months. The report provides detail of ASIO's activities during the reporting period, including the nature of the threat environment, details of ASIO's corporate human resources and governance arrangements, and ASIO's financial statements.

ASIO also produces a highly classified annual report outlining ASIO's operational and corporate activities in greater detail. ASIO's 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

Throughout the reporting period ASIO engaged with the PJCIS on a range of matters relevant to the Committee's role, including briefing the Committee on proscription of terrorist organisations and providing a submission and attending a hearing for the PJCIS review of national security legislation and the review of the *Telecommunications (Interception and Access) Act 1979*.

Senate Standing Committee on Legal and Constitutional Affairs

As part of the Attorney-General's portfolio, ASIO appears before the Senate Standing Committee on Legal and Constitutional Affairs to respond to questions on issues of departmental expenditure and operations. The Director-General of Security and Deputy Director-General, Ms. Kerri Hartland appeared at Supplementary Budget Estimates in November 2013, Additional Budget Estimates in February 2014 and Budget Estimates in May 2014.

External oversight mechanisms

Inspector-General of Intelligence and Security

The Office of the IGIS was formally established under the *Inspector-General of Intelligence and Security Act 1986.* The IGIS, Dr Vivienne Thom, is an independent statutory office holder responsible for reviewing the activities of the Australian Intelligence Community to ensure the agencies act legally, with propriety, in compliance with ministerial guidelines and directives, and with due regard for human rights.

The IGIS conducts regular and ongoing inspections and monitoring of ASIO activities with wide-ranging powers similar to those of a royal commission, including access to ASIO records or premises at any time.

ASIO does not wait for an inspection of a case to bring issues or errors to the attention of the IGIS but proactively provides that advice. ASIO also ensures that 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.

Outcomes of IGIS inquiries

During the reporting period, two full IGIS inquiries examined ASIO's role and functions, one stemming from a complaint to the IGIS about ASIO, and the other from a ministerial referral relating to an illegal maritime arrival.

Inquiry into attendance of lawyers at ASIO interviews

In May 2013 the IGIS initiated an inquiry into the attendance of legal representatives at ASIO interviews. The inquiry originated in a complaint, lodged by the Refugee Advisory and Casework Service, alleging inconsistent and arbitrary practices by ASIO in relation to the attendance of legal representatives at security assessment interviews.

The IGIS completed her inquiry during the reporting period, the IGIS stated that ASIO's internal policies were sound and appropriate and that ASIO officers conducted themselves in a professional manner during the interviews. However, the IGIS made five recommendations that would serve to refresh and reinforce ASIO's policies and procedures. Of the five recommendations in the report, ASIO agreed in full to Recommendations 1 to 4 and agreed in part to Recommendation 5. Recommendations were:

1. ASIO should work with the Department of Immigration and Border Protection (DIBP) to ensure that:
   - When making interview arrangements in Australia, visa applicants are specifically asked whether they want to have a legal representative attend
   - The lawyer's personal details are obtained by DIBP and passed to ASIO
   - A decision is made about whether the lawyer may attend and is conveyed prior to the day of interview.

2. ASIO should:
   - Review its training to reinforce that the attendance of a lawyer at a security assessment interview is not to be considered problematic, unless sound reasons exist for deciding otherwise
   - Ensure that decisions about whether a lawyer may attend an interview are considered and recorded on a case-by-case basis
   - Ensure that, in the absence of a specific cause for concern, interviews should commence without efforts by interviewing officers to discourage the attendance of a legal representative.
3. ASIO should:
   - Clarify the status of any person who wants to attend an interview to ascertain whether they are the interviewee's legal representative
   - Further consider whether migration agents should be accorded the same status as lawyers, with their attendance at interviews being addressed on a case-by-case basis.
4. ASIO should:
   - Provide guidance for interviewing officers on when a written or verbal confidentiality undertaking should be requested from a person
   - Provide the template undertaking document to attendees before the interview commences
   - Provide a copy of a written undertaking to the signatory.
5. The details of this recommendation are afforded a national security classification.

ASIO has fully implemented all recommendations to which it agreed.

In the reporting period, ASIO produced policy on visa security assessment interviews which reinforced recommendations from the IGIS Inquiry into the attendance of legal representatives at ASIO interviews. ASIO continues to conduct training for new officers who will be conducting visa security assessment interviews to reinforce this policy.

Inquiry into Egyptian maritime arrival Mr E.

On 5 June 2013, the then Prime Minister, the Hon. Julia Gillard MP, requested that the IGIS conduct an inquiry into the management by Australian Government agencies of people seeking asylum who present complex security issues, with particular reference to an Egyptian illegal maritime arrival who was subject to an Interpol 'red notice'.

The IGIS report noted that, prior to the case becoming a matter of public interest, ASIO had already initiated significant changes addressing a number of the issues raised during the inquiry. The report outlined six recommendations relating to the coordination of agencies on national security alerts, identity resolution processes, risk assessments, record keeping and training.

The three IGIS recommendations relevant to ASIO resulting from the inquiry into the Egyptian maritime arrival were:

- DIBP and ASIO should continue to build on recent improvements in implementing a coordinated approach to resolving potential matches to national security alerts and document agreed procedures. This approach includes mechanisms to:
  - Escalate the priority of requests for information
  - Ensure that request are followed up
  - Access all relevant existing information
- DIBP should review its procedures for conducting risk assessments in cases involving national security to ensure that those undertaking the assessment;
  - have access to relevant information and expertise including from ASIO and AFP
  - have appropriate training and a standard process to follow
  - reference source information
  - ensure that risk assessments become part of corporate records and are linked to the particular client's case.
- DIBP and ASIO should ensure that in the small number of cases where there are potentially national security issues all relevant information is taken into account by DIBP when making immigration detention management decisions. Where such a case also involves issues of serious criminality DIBP should also work with the AFP to ensure relevant AFP information is also obtained and taken into account. This recommendation is not intended to suggest that responsibility for the decision in relation to the level of security for a person in immigration detention should rest with ASIO or the AFP; that decision is ultimately one for DIBP to make based on the best available information and advice.

ASIO accepted the three recommendations in full. During the reporting period, ASIO worked with DIBP to implement the recommendations, with consequent changes to ASIO processes, training and guidance to staff.

Further to improvements to the resolution of national security alerts introduced in 2013, ASIO — in consultation with DIBP — issued a procedural document relating to security assessments for illegal maritime arrivals for whom DIBP is considering the grant or re-grant of a bridging visa, or for those being considered for placement in community detention. This provides formal guidance for officers in ASIO and DIBP for handling referrals which potentially match national security alerts.

Independent Reviewer of Adverse Security Assessments

The Independent Reviewer conducts reviews of ASIO adverse security assessments in relation to individuals who remain in immigration detention, after being found by the Department of Immigration and Border Protection to be:

- refugees; and
- ineligible for a permanent protection visa, or who have had their permanent protection visa cancelled, because they are the subject of an adverse security assessment.

The Independent Reviewer is required to:

- examine all material relied on by ASIO in making the adverse security assessment;
- provide an opinion to the Director-General of Security as to whether the adverse security assessment is an appropriate outcome based on that and other relevant material; and
- make recommendations accordingly, for the Director-General of Security's consideration.

ASIO issues three types of security assessments:

- *Adverse Security Assessments* – ASIO recommends that a particular action be taken or not taken, which would be prejudicial to the interests of the person, such as the refusal of a visa or cancellation of a passport;
- *Qualified* – ASIO has information, an opinion or advice that is or could be prejudicial to the interests of the person; and
- *Non-prejudicial* – ASIO does not have security concerns about the proposed action.

At the start of the reporting period, the Independent Reviewer had a caseload of 54. This was reduced to 51 as a result of ASIO's internal review process when ASIO independently issued new non-prejudicial or qualified assessments for three individuals. During the reporting period, the Independent Reviewer finalised 17 reviews.

Table 4: Independent Reviewer findings 2013–14

ASIO's assessment appropriate	15	These are now subject to periodic review. This includes one case where ASIO issued a new adverse security assessment taking into account new information referred by the Independent Reviewer. The Independent Reviewer found the new adverse security assessment to be an appropriate outcome.
ASIO's assessment not appropriate	1	ASIO re-examined the case and issued a qualified security assessment.
Reviewer provided new information to ASIO resulting in new assessments being issued	1	ASIO issued a new qualified security assessment.
Total	**17**	

During the reporting period, the Independent Reviewer referred new information in the form of draft reports concerning three cases to ASIO. The draft reports summarised all the information before her but did not include any recommendations. ASIO was still considering the new information in these three cases at the end of the reporting period. Under the terms of reference, the review process remains on hold until ASIO concludes its consideration of the new information.

In a further two cases, the Independent Reviewer submitted draft reports concluding that the original assessments were not an appropriate outcome. ASIO was still considering these cases at the end of the reporting period.

In addition to the primary reviews that were either finalised or referred to ASIO, the Independent Reviewer had prepared advanced drafts of a further 11 reports. A number of these reviews were finalised just after the end of the reporting period.

The Independent Reviewer's terms of reference require her to conduct a periodic review of adverse security assessments for eligible persons every 12 months. In June 2014, the Independent Reviewer commenced periodic reviews of two cases. These reviews were ongoing at the end of the reporting period.

ASIO Internal Review of Security Assessments

Over the passage of time, new information can become available to ASIO on an individual undergoing a security assessment. Where ASIO receives new information, ASIO reviews it to determine whether it might have a bearing on an extant security assessment.

New information can include additional information supplied by the applicant, DIBP, information obtained through ASIO investigation, or a new strategic assessment which may change ASIO's evaluation of previous information. Where new information is deemed relevant to security ASIO may re-interview the subject of an adverse security assessment.

Public statements

Throughout the reporting period, ASIO continued to engage with the public through a variety of statements and speeches by the Director-General of Security. The Director-General made public comment on a range of matters, including the security environment in Syria, cyber threats, the Ben Chifley Building and ASIO's new strategic plan. The Director-General addressed a variety of forums, including the 2013 Sir Zelman Cowen Oration at the Australian Institute of International Affairs and the 25th Security in Government Conference in 2013.

Transcripts of these speeches can be found on ASIO's website, as well as copies of ASIO's public submissions to inquiries and answers to frequently asked questions. ASIO's *Report to Parliament* is also available on the website and provides a significant body of information to inform the public about ASIO's activities. ASIO updates its website to ensure the most contemporary information is available to the public.

ASIO's domestic relationships

ASIO's ability to protect Australia, its people and its interests relies on maintaining effective networks and productive relationships with domestic partners, including government agencies, industry and the general public. These relationships contribute to ASIO's mission and in part seek to ensure threats to security are identified and mitigated appropriately.

During the reporting period, ASIO continued to broaden and deepen its engagement with government agencies, including through regular ASIO Partnership Forums. These forums provide information to senior officers of government partners to help them better understand the security challenges faced by Australia, ASIO's approach to dealing with these challenges, and the role and functions of the Organisation and the framework it works within.

ASIO surveys key stakeholders in the Australian Government and states and territories each year. The survey seeks to capture feedback on the quality of ASIO advice, the effectiveness of its capabilities and people and the value ASIO adds through cooperation and collaboration.

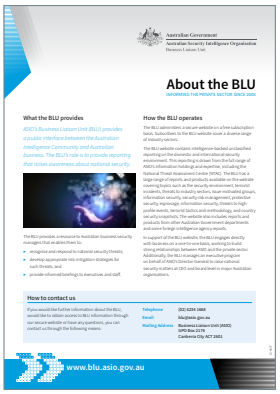
Business Liaison Unit

ASIO works in partnership with the private sector to protect Australian interests, including national critical infrastructure. The Business Liaison Unit (BLU) provides an interface between ASIO and Australia's private sector. The BLU distributes unclassified security reporting drawn from intelligence holdings on a broad range of security topics to businesses in Australia to enable them to better understand the security environment and the threats they face, and to provide them with a basis for security planning. These include domestic and international threat environments, terrorist tactics, malicious activity indicators, cyber security, protective security, and espionage. The BLU also publishes reports prepared by other Australian Government agencies and international partners on its independent website.

The BLU also administers the Register of Australian Interests Overseas, which enables ASIO to provide time-critical advice to subscribed companies in the event of an imminent and credible threat to businesses who register the details of their operations throughout the world.

In 2013–14 the BLU conducted 233 separate meetings with corporate security and risk managers across Australia, published 157 reports on its subscriber-based website (including 77 reports from foreign liaison counterparts and 14 reports from other Australian Government agencies) and hosted four dedicated security briefing days for corporate security managers from the defence industry security program, the energy and resources sector, the banking and finance sector, and a multi-sector security program.

The number of subscribers to the BLU website has steadily increased over the last five years. Last year the number of subscribers increased by 38 percent, from 1555 to 2150. The BLU is not corporately funded or sponsored.



ASIO's international relationships

ASIO's mission relies on fostering and maintaining strong international relationships. ASIO engages with and receives support from a number of international partners.

Over the reporting period there has been a high level of liaison with international partners particularly with regard to protecting Australia from the threat posed by foreign fighters returning from conflicts in the Middle East.

ASIO engages with partners through liaison meetings, exchanges of information and reporting, international visits, joint training and capability development initiatives, formal secondments and staff exchanges.

At the end of the reporting period, the Attorney-General had authorised ASIO to liaise with 346 authorities in 129 countries.

Public access to ASIO records

The *Archives Act 1983* (the Act) requires the National Archives of Australia (NAA) to respond to requests for records under Section 40 of the Act within 90 days from the date of receipt. This timing includes NAA processes, the processes of the agency concerned and any referrals for opinion to third party agencies.

Due to the increasing number of requests for access to records and despite permanently allocating a significant number of officers to service public requests, ASIO faces challenges in meeting the 90 day legislated turnaround time. In 2013–14, there was a 75 percent increase in the number of applications submitted for access to records. In recent years, ASIO has completed 60–70 percent of requests within the 90-day legislative requirement, however currently 82 percent of requests are overdue. This is due to a range of factors including:

- The high number of requests, 773 in 2013–14
- On average, each volume takes two weeks to be assessed to ensure no release of national security information, in accordance with Section 33 of the Act. Utilising existing staffing levels current requests will take five to six years to process.
- The Open Period as specified in the Act currently covers all records created in, or before 1987. In accordance with changes to the Act in 2010 the Open Period is currently transitioning from 30 to 20 years. The reduced closed period equates to more records for assessment and greater sensitivities.

There are no limits to the number of requests an applicant may submit and no mechanism to refuse a request or to charge fees for the requests. Currently 23 percent of ASIO's public research workload supports requests from one researcher. This researcher has a current AAT appeal against deemed refusal of ASIO records. At the request of the NAA, ASIO has allocated extra resources to respond to this case. ASIO estimates this researcher's current requests would take two full-time officers approximately six years to complete.

ASIO is also involved in assessing the proactive release of Cabinet records.