# 2

# Administration

2.1 In undertaking its review of the administration of the intelligence agencies for the 2013–14 financial year, the Committee asked agencies to provide submissions addressing:

- strategic direction and priorities,
- legislative changes (if any) that have impacted on administration,
- involvement (if any) in litigation matters,
- human resource management,
- changes (if any) to the structure of the organisation,
- security issues,
- security clearances, and
- public relations and/or public reporting.

2.2 In their submissions, agencies outlined significant developments and relevant aspects of administration for 2013–14. Much of the evidence received was classified, however, and accordingly has not been authorised for publication. The Committee scrutinised all material provided and followed up several issues at classified hearings. This chapter reports the Committee's findings on administration of the agencies. In some areas the discussion is necessarily general due to security needs.

## Legislative changes

2.3 Agencies were asked to identify any legislative changes that impacted on administration in 2013–14, including information on:

- the frequency and nature of the use of powers,
- staffing implications,
- training,

- the role of legal officers,
- the need for specialist staff, and
- relationships with outside agencies such as police or the judiciary.

2.4 The majority of agencies noted work undertaken during the reporting period in support of the Government's national security reforms,[1] which followed the Committee's 2012–13 inquiry into potential reforms of Australia's national security legislation.[2] ASIO, for example, advised that it had worked with the Attorney-General's Department during the reporting period to inform the Government's response to the Committee's report and to support the preparation of the National Security Legislation Amendment Bill (No. 1) 2014.[3] The Bill was introduced into the Senate on 16 July 2014 (outside the reporting period) and included a range of measures impacting on the legislative framework for ASIO, ASIS and the other agencies operating under the *Intelligence Services Act 2001* (IS Act).

2.5 Several agencies noted the commencement of the *Public Interest Disclosure Act 2013* (PID Act) on 15 January 2014. The PID Act aims to promote integrity and accountability in the Commonwealth public sector by encouraging and facilitating the disclosure of suspected wrongdoing, protecting disclosers from adverse consequences, and ensuring disclosures are properly investigated and dealt with.[4] Agencies prepared for the commencement of the PID Act by establishing internal procedures, appointing officers authorised to receive disclosures, liaising with the IGIS and providing training to staff on the changes.[5]

2.6 Some agencies also highlighted work undertaken to prepare for the commencement of the *Performance, Governance and Public Accountability Act 2013* (PGPA Act) on 1 July 2014.[6] The PGPA Act replaced the *Financial Management and Accountability Act 1997* (FMA Act) and the *Commonwealth Authorities and Companies Act 1997* (CAC Act) to be 'the primary piece of Commonwealth resource management legislation'.[7] ONA noted that ensuring compliance with the PGPA Act required a considerable amount

[1] ASIO, *Submission 6.1*, p. 28; ASD, *Submission 3.1*, p. 6; DIO, *Submission 3.2*, p. 6; AGO, *Submission 3.3*, p. 6; ASIS, *Submission 5*, p. 30.

[2] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, June 2013.

[3] ASIO, *Submission 6.1*, p. 28.

[4] Commonwealth Ombudsman, 'About the PID Scheme', <www.ombudsman.gov.au/pages/pid/about-the-pid-scheme> viewed 27 April 2015.

[5] ASIO, *Submission 6.1*, p. 31; AGO, *Submission 3.3*, p. 6; ONA, *Submission 2.1*, p. 11.

[6] ONA, *Submission 2.1*, p. 12; ASIS, *Submission 5*, p. 30.

[7] Department of Finance, 'PGPA Act legislation and associated instruments', <www.finance.gov.au/resource-management/pgpa-legislation> viewed 27 April 2015.

of work, including re-writing chief executive instructions and updating financial delegations.[8]

2.7 ASIO referred to several other pieces of legislation that had impacted on its administration in 2013–14:

- The *Migration Amendment Bill 2013*, which came into effect on 2 June 2014. This Bill amended the *Migration Act 1958* so that a protection visa cannot be granted to an applicant who has received an adverse security assessment (other than under the Minister's discretionary powers) and confirmed limitations on the appeal rights of applicants,
- The *Information Privacy Act 2014 (ACT)*, which, following submissions from ASIO, was amended to allow Australian Capital Territory public sector agencies to disclose to ASIO personal information in connection with the performance of ASIO's functions, and
- Amendments pursued by ASIO to legislation in the Australian Capital Territory, New South Wales and Victoria to support the issue of evidence to ASIO of assumed identities (such as birth certificates).[9]

## Litigation

2.8 ASIO advised that it was involved in more than 50 litigation matters in 2013–14, 'primarily criminal prosecutions, including for terrorism and foreign incursion offences, and judicial and administrative reviews of ASIO security assessments'.[10] The Administrative Appeals Tribunal (AAT) reviewed and upheld three of ASIO's security assessments; a number of complex matters were subject to judicial review in the Federal and High Courts of Australia; and one matter was heard by the International Court of Justice in The Hague.[11] ASIO also provided information to support various criminal prosecutions, including at least three prosecutions under the *Crimes (Foreign Incursions and Recruitment) Act 1978*.[12]

2.9 ASIO noted that the protection of sensitive national security information was an important consideration in its litigation matters:

> The Office of Legal Counsel, a Division of ASIO, works closely with ASIO operational areas and external stakeholders and legal representatives to balance protection of ASIO investigations, capabilities, methodologies, officer and source identities and

[8] ONA, *Submission 2.1*, p. 12.

[9] ASIO, *Submission 6.1*, pp. 28–30.

[10] ASIO, *Submission 6.1*, p. 32.

[11] ASIO, *Submission 6.1*, p. 32.

[12] ASIO, *Submission 6.1*, p. 33.

> foreign liaison relationships with court requirements and the principles of open justice.[13]

2.10 ONA appeared before the AAT to defend the exemption of ONA material on two Department of Foreign Affairs and Trade files requested by an academic. ONA provided classified evidence and unclassified sworn affidavits in support of the formal respondent, the National Archives of Australia (NAA).[14]

### Use of ASIO's special powers

2.11 ASIO reports each year on the use of its special powers under the *Australian Security Intelligence Organisation Act 1979 (*ASIO Act) and the *Telecommunications (Interception and Access) Act 1979* to use methods of investigation such as telecommunications interception and access; use of surveillance devices; entry and search of premises; computer access; and the examination of postal and delivery service articles. The use of these powers is subject to a warrant approved by the Attorney-General.[15]

2.12 Further, the ASIO Act enables ASIO, with the Attorney-General's consent, to seek warrants from an independent issuing authority (a federal magistrate or judge) for questioning, or questioning and detention, of individuals.[16]

2.13 The number of warrants approved by the Attorney-General in 2013–14 is classified and cannot be reported by the Committee. However, the Committee notes there has been an increase in the number of warrants sought and issued. No administrative issues were brought to the Committee's attention in regard to these warrants. Additionally, the Committee made enquiries at the public hearing regarding the number of warrants that were applied for but not approved by the Attorney-General in the reporting period.[17]

## Strategic direction and organisational structure

2.14 The Committee requested agencies to report on their organisation's strategic direction and priorities. The Committee also requested information on any changes to the structure of each organisation,

[13] ASIO, *Submission 6.1*, p. 32.

[14] ONA, *Submission 2.1*, p. 12.

[15] ASIO, *Submission 6.1*, p. 31.

[16] ASIO, *Submission 6.1*, p. 31.

[17] *Classified Committee Hansard*, 25 March 2015, pp. 23–24; ASIO, *Submission 6.2*, pp. 6–7.

including the distribution of staff across different areas of the organisation; the ratio of field and operation staff to administrative staff; the ratio of executive to middle and lower level staff; and the ratio of central office to outlying staff.

2.15 While much of the information provided to the Committee was classified, where possible, the strategic direction and organisational structure of each agency is discussed below.

## ASIO

2.16 ASIO referred the Committee to the vision, mission and goals outlined in its *Strategic Plan 2013–16*. It noted that the goals in its strategic plan emphasised capability building of 'both the workforce and technology required of a security agency'.[18] These goals were to:

- deliver high-quality security intelligence collection, analysis, assessment and advice in support of ASIO's mission,
- continue to enhance ASIO's strategic impact and reputation,
- evaluate, evolve and strengthen ASIO's capabilities and business practices, and
- attract, develop and retain a professional and highly competent workforce.[19]

2.17 ASIO advised that its strategic plan was incorporated into its business planning cycle to ensure that the identified goals were reflected in the business priorities of all parts of the organisation.[20]

2.18 For 2013–14, ASIO's strategic plan prioritised the work of its governance committees, which it considered particularly important following introduction of the PGPA Act, and the implementation of a risk management policy. In light of this, ASIO established an additional committee, the ASIO Combined Committee, during the reporting period to ensure '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'.[21]

2.19 ASIO maintained its eight division structure during the reporting period, following a 23 per cent reduction in its Senior Executive Service (SES) in the previous reporting period. The number of branches within ASIO's

[18] ASIO, *Submission 6.1*, p. 16.

[19] ASIO, *Strategic Plan 2013–16*, p. 3: <www.asio.gov.au/Publications/Strategic-Plan.html> viewed 1 May 2015.

[20] ASIO, *Submission 6.1*, p. 16.

[21] ASIO, *Submission 6.1*, p. 16.

divisions 'remained relatively stable', with one new branch—Data Exploitation Projects—being created under the Technical Capabilities Division.[22]

2.20 ASIO also combined its operations 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.[23]

2.21 Also of interest to the Committee was ASIO's risk management framework. The Committee obtained additional information from ASIO about this framework during the private hearing.[24]

## ONA

2.22 ONA's structure remained the same in 2013–14. ONA was led by its Director-General, supported by two Deputy Director-Generals, and consisted of ten branches with liaison offices in Washington and London.[25] ONA reported its strategic direction and priorities to the Committee in classified evidence.[26]

## Defence Intelligence Agencies

2.23 In 2013–14, the Defence Intelligence Agencies (DIAs) contributed to the development of the next Defence White paper, the Force Structure Review and the First Principles Review of Defence.[27]

2.24 ASD prepared for the transition of the Information Security Registered Assessors Program (IRAP) into a new framework. The IRAP 'endorses qualified ICT professionals to provide cyber-security assessment services for Australian Government agencies'. Under the new framework, it was intended that IRAP services would be expanded, providing the Government with additional ASD-endorsed capability. All administration functions were returned to ASD and a new entry examination developed. Mandatory annual online refresher training was also introduced for all

[22] ASIO, *Submission 6.1*, p. 14.

[23] ASIO, *Submission 6.1*, p. 14.

[24] *Classified Committee Hansard,* 25 March 2015, pp. 10–11.

[25] ONA, *Submission 2.1*, p. 3.

[26] ONA, *Submission 2.1*, pp. 5–6.

[27] *Classified Committee Hansard,* 26 March 2015, p. 28.

IRAP assessors as a cost saving measure, replacing a former face-to-face training.[28]

2.25 ASD reported that:

> The revitalisation of IRAP has been positively received by IRAP assessors and customers, and has seen ASD develop and support IRAP relationships in an effort to increase the cyber security posture of Australian Government networks. ASD is now working on expanding IRAP to include Penetration Testing and Incident Response services.[29]

2.26 No changes to ASD's organisational structure were reported.

2.27 AGO's mission to provide geospatial intelligence from imagery and other sources in support of Australia's defence and national interests remained unchanged in 2013–14.[30] AGO released its *AGO Strategy 2014–18* in December 2013 and commenced a five year Capability Improvement Program, designed to ensure AGO meets its strategic goals and objectives. AGO provided additional information about its priorities and capability development to the Committee in classified evidence.[31]

2.28 AGO advised that progress continued in the reporting period towards a coordinated and integrated Defence geospatial capability. This included Phase One of the Defence Geospatial Enterprise Review, which AGO advised had identified a number of challenges and remediation actions.[32]

2.29 Several changes to AGO's organisational structure were also reported to the Committee.[33]

2.30 DIO advised the Committee of its strategic priorities, engagement with stakeholders, and contribution to Defence policy and capability development in classified evidence.[34]

## Pathway to Change

2.31 The *Pathway to Change: Evolving Defence Culture and Employment Pathways for APS Women in the Department of Defence* (Pathway to Change) strategy was announced in March 2012 in response to a number of reviews into Defence culture. The strategy aims to 'shape Defence's attitudes, systems and behaviours to improve capability and ensure the continued support of

[28] ASD, *Submission 3.1*, p. 6.

[29] ASD, *Submission 3.1*, p. 6.

[30] AGO, *Submission 3.3*, p. 2.

[31] AGO, *Submission 3.3*, pp. 2–4.

[32] AGO, *Submission 3.3*, p. 4.

[33] AGO, *Submission 3.3*, p. 7.

[34] DIO, *Submission 3.2*, pp. 2–5.

the Australian public'.[35] Each of the DIA's updated the Committee on their activities under the Pathway to Change strategy during 2013–14.

2.32 ASD's key initiative during the reporting period was continued growth of its mentoring culture. Specific activities undertaken during the year included a guest speaker leadership series; tradecraft mentoring; promoting better understanding of working hours; developing and delivering 'Early Parenting Years' outreach sessions; and implementing a communications strategy to inform ASD staff of Defence's culture reform initiatives and show leadership support of the values and behaviours expected of all employees. ASD also formalised a collaboration with AGO, the Defence Security Authority and the Chief Information Office Group of Defence by officially launching a joint mentoring program.[36]

2.33 AGO's Pathway to Change initiatives during 2013–14 included developing online courses for the joint mentoring program; improving the accessibility of its mentoring program resources; reporting on Pathway to Change activities and events in internal publications; attendance of staff at women's networking events; and staff participation in outreach sessions run by ASD.[37]

## Human resource management

2.34 The Committee requested agencies to provide an update on human resource management, including information on the following issues:

- staffing numbers,
- recruitment and retention strategies,
- training and development,
- performance management,
- workplace diversity,
- language skills,
- staff complaints,
- separation rates, and
- accommodation.

[35] AGO, *Submission 3.3*, p. 3.

[36] ASD, *Submission 3.1*, p. 5.

[37] AGO, *Submission 3.3*, p. 3.

2.35 Information provided to the Committee regarding each agency's staffing arrangements was largely classified. Nevertheless, where possible, human resource management issues relating to each agency are discussed below.

## Staffing demographics

2.36 ASIO advised it had continued downsizing activities during 2013–14.[38] There were 34 Executive Level voluntary redundancies and four SES voluntary redundancies during the period.[39]

2.37 As at 30 June 2014, ASIO had at total of 1 795 staff, including 44 SES officers, 488 ASIO Executive Officer 1 and 2 officers, and 1 263 other officers. Of these, 791 staff (44 per cent) were women; 98 staff came from a non-English speaking background; eight staff identified as Aboriginal or Torres Strait Islander; and 19 staff had a disability.[40] Graphs provided in ASIO's submission indicated an increase in the age of ASIO's workforce over recent years, with a marked decrease in the proportion of staff under 35 years old. Approximately two thirds of staff had lengths of service of more than five years, and 22 per cent more than ten years.[41]

2.38 ONA also reduced its staffing levels during the reporting period. As at 30 June 2014, it had 146 staff (excluding the Director-General), down from 153 in 2013. This included 20 non-ongoing staff, 15 part-time staff and seven overseas-based staff. Approximately 41 per cent of ONA's staff were women. 30 per cent of staff were under 35 years old, and 16 per cent were over 55 years old.[42] One staff member was identified as having a disability.[43]

2.39 ASD had over 1 500 employees as at 30 June 2014. During 2013–14, ASD's staffing level declined slightly. Approximately 93 per cent were operational staff and seven percent were administrative staff. ASD advised that it had reclassified positions in its workforce to 'more accurately reflect job families in Defence'. Accordingly, ASD's Corporate and Business Management structure was retired, with occupation profiles being realigned into five new job families: Administration and Corporate Communications, Auditing and Assurance, Communication and Stakeholder Management, Customer Service and Information Knowledge Management.[44]

[38] ASIO, *Submission 6.1*, p. 21.

[39] ASIO, *Submission 6.1*, p. 26.

[40] ASIO, *Submission 6.1*, p. 24.

[41] ASIO, *Submission 6.1*, Figures 11 and 12, p. 25.

[42] ONA, *Submission 2.1*, p. 18.

[43] ONA, *Submission 2.1*, p. 21.

[44] ASD, *Submission 3.1*, p. 11.

## Recruitment and retention strategies

2.40 In the context of its continued downsizing, ASIO informed the Committee that recruitment action during the reporting period had been limited to the 'difficult-to-fill roles' of intelligence officer, technical officer and security assessor.[45] ASIO implemented a new advertising strategy for intelligence officers during the period, with one recruitment campaign attracting 1 049 applicants, an increase of 40 per cent from the previous campaign. ASIO also introduced a new technical officer graduate program designed to attract and develop entry-level staff in specialist areas.[46]

2.41 At the hearing, ASIO advised the Committee of its current recruitment processes and the timeframes and resources involved in recruiting, vetting and training new staff. ASIO also explained its rebalancing of the organisation to meet ongoing capability needs.[47]

2.42 Defence commented that the reduction of recruitment activities for each of its agencies since the last reporting period had raised a number of challenges, and that agencies were seeking to broaden and deepen their analytical and technical expertise.[48]

2.43 ASD informed the Committee that it had used a number of strategies in 2013–14 to recruit talented staff, including both generic and specialised recruitment rounds, transfers at level and the Defence-wide graduate program. However, ASD also noted that it had recruited only 75 new staff in the period, down from 175 in 2012–13 and 226 in 2011–12. In 2013–14, 63 per cent of all ASD's new arrivals came from its graduate program. The majority of direct entrants to ASD in 2013–14 came from the broader Defence portfolio, with only seven per cent coming from the private sector. This was in contrast to previous years in which the majority of direct entrants were typically from the private sector.[49] ASD recruited no cadets through the Australian Government Information Management Office ICT Entry Level Programs in 2013–14.[50]

2.44 This significant decrease in recruitment activity was reflected across other agencies, with budgetary pressures and broader Australian Public Service (APS) recruitment policy identified as partial reasons for this. However, one agency reported an increase in recruitment, partly as a result of an

[45] ASIO, *Submission 6.1*, p. 21.

[46] ASIO, *Submission 6.1*, p. 21.

[47] *Classified Committee Hansard,* 25 March 2015, pp. 14–15.

[48] *Classified Committee Hansard,* 26 March 2015, p. 28.

[49] ASD, *Submission 3.1*, pp. 15–16.

[50] ASD, *Submission 3.1*, p. 17.

increased availability of candidates associated with a general decline in the Canberra employment market.

2.45 ASIS highlighted the marketing material produced for its Technologist Recruitment Campaign. This campaign involved the launch of a YouTube video, a presence on major online job websites, and presenting the video in selected cinemas and digital light boards at major domestic airports in February 2014. ASIS used similar methods for its 'IQ+EQ=ASIS' recruitment campaign in March and April 2014, in addition to advertisements in both print media and online news websites. ASIS reported that both campaigns had been well received.[51]

2.46 In regard to retention strategies, ONA noted that prospective employees were attracted to its interesting and challenging work, together with flexible working arrangements and appropriate remuneration. ONA advised that it provided its new staff with a tailored program covering their development needs, both at a job-specific and an organisational awareness level.[52]

2.47 ASD referred the Committee to its 'Unified Structure' corporate initiative, which aims to retain staff by providing them with an opportunity to advance to the next level within a broadband, if they can successfully demonstrate that they have been working at the higher level for a reasonable amount of time and will continue to perform at that level as a result of their skills.[53]

2.48 Defence noted that the Intelligence and Security Group had actively sought to increase the recruitment of Indigenous employees throughout 2013–14, with additional employees obtaining security clearances in the reporting period and more expected for the following financial year.[54]

## Separation rates

2.49 The average separation rate across the APS for 2013–14 was 7.6 per cent.[55] Of these separations, 41.5 per cent were attributed to retrenchments (up from 27.8 per cent in 2012–13) and 53.5 per cent were attributed to resignations and age retirements (down from 66.1 per cent in 2012–13).[56]

[51] ASIS, *Submission 5*, pp. 14–15.

[52] ONA, *Submission 2.1*, p. 19.

[53] ASD, *Submission 3.1*, p. 18.

[54] *Classified Committee Hansard,* 26 March 2015, p. 28.

[55] Based on 11 131 separations as a proportion of a total of 145 891 ongoing APS employees at 30 June 2014. See Australian Public Service Commission, *State of the Service Report 2013–14*, p. 175.

[56] Australian Public Service Commission, *State of the Service Report 2013–14*, p. 175.

2.50 In contrast to previous years, the separation rates provided by AIC agencies in their submissions were all given classifications or Dissemination Limiting Markers and cannot be included in this report.

2.51 Separation rates varied between agencies. Most agencies reported rates that were either steady or lower compared in previous years. ONA was an exception to this, with an increased separation rate attributed to a number of retirements in the reporting period, with 21 per cent of staff who left in the period having worked for more than 10 years in ONA.[57]

2.52 The separation rates reported by some agencies were also affected by voluntary redundancies, including those in ASIO as noted above. ASIO reported that 58 per cent of its separations were due to resignations or age retirements, with the remaining 42 per cent due to 'other' reasons.[58]

2.53 The Committee obtained further information from agencies during the hearings to clarify trends in separations.[59]

## Individual performance management

2.54 All agencies reported on their arrangements for managing the performance of employees.

2.55 ASIO noted that its performance management framework—Enhancing Performance—aimed 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.[60]

2.56 ASIO reported that four of its employees had participated in its formal underperformance management process in 2013–14. ASIO also completed nine misconduct investigations during the period, all resulting in a charge of misconduct. The most common allegation of misconduct (eight instances) was for 'contravening or failing to behave in a way that upholds ASIO's Values or the Code of Conduct'.[61]

2.57 ONA advised that its approach to performance management was outlined in its performance development framework:

> All employees are required to participate in the program, which requires them to meet regularly with their managers to discuss, set, document and review work priorities and development

[57] ONA, *Submission 2.1*, p. 19; *Classified Committee Hansard,* 26 March 2015, pp. 25–26.

[58] ASIO, *Submission 6.1*, p. 31.

[59] *Classified Committee Hansard,* 25 March 2015, pp. 11–12; *Classified Committee Hansard,* 26 March 2015, pp. 25, 34.

[60] ASIO, *Submission 6.1*, p. 27.

[61] ASIO, *Submission 6.1*, p. 27.

> expectations. Pay-point advancement within broad banded classification was available to eligible staff at the end of the financial year.[62]

2.58 ONA noted that the ethical behaviour expected of its employees was promoted in its corporate documents, and that it had implemented and promoted the revised APS Code of Conduct and APS Values to all staff during the reporting period. It advised that there had been no code of conduct breaches or investigations during 2013–14.[63]

2.59 ONA also referred the Committee to its recognition of high performing employees through AIC and ONA Australia Day awards programs.[64]

2.60 ASD advised that the performance of its employees was assessed twice annually as part of the Defence Performance Feedback and Development Scheme, which is linked to performance progression payments. ASD reported that approximately 90 per cent of employees had their performance progression approved in 2013–14. Of those denied progression, 11 were due to non-completion of mandatory training, one was due to work performance being rated as not effective, and one was due to the employee refusing to participate.[65] The remaining employees were ineligible for progression due to a range of reasons. The other DIA's reported a similar proportion of employees being denied performance progression.[66]

2.61 Supervisors in ASD were additionally encouraged to 'provide informal, timely and accurate feedback to their employees on a regular basis'.[67]

2.62 As part of its individual performance management framework, one organisation reported that it awarded performance bonus payments to staff at the top of their salary range who received appropriate performance ratings.

## Training and development

2.63 All agencies reported on specific training and development activities undertaken during the reporting period, encompassing both corporate and operational aspects. Training areas identified across the agencies included:

- intelligence tradecraft,

[62] ONA, *Submission 2.1*, p. 21.

[63] ONA, *Submission 2.1*, p. 20.

[64] ONA, *Submission 2.1*, p. 21.

[65] ASD, *Submission 3.1*, p. 27.

[66] DIO, *Submission 3.2*, p. 16; AGO, *Submission 3.3*, p. 24.

[67] ASD, *Submission 3.1*, p. 26.

- agency-specific legislation,
- language capabilities,
- induction courses,
- graduate development programs,
- leadership and management,
- ethics and fraud,
- workplace health and safety,
- workplace behaviour,
- information technology,
- finance management and procurement, and
- security awareness.

2.64 Agencies also reported on continued staff engagement in training courses facilitated by the National Intelligence Community's Training Secretariat and the National Security College.

## Defence Intelligence Agencies

2.65 ASD participated in the development and presentation of the Defence Intelligence and Security Group Orientation Program, which is offered to new employees. Eleven ASD staff attended the program in 2013–14.[68]

2.66 ASD also invested in the Executive Leadership Development Program and the Middle Management Development Program for Intelligence and Security Group staff, with a total of 62 employees attending the two programs. Fifty-three ASD employees attended the 'Stepping Stones' program, which aims to equip staff in middle management positions with the skills and tools to respond and adapt to rapid organisational change.[69]

2.67 The Committee was informed that all Defence staff were required to undertake and maintain proficiency in a range of mandatory training courses, including Work Health and Safety awareness, Fraud and Ethics awareness, Equity and Diversity awareness and Security Awareness.[70]

2.68 ASD advised that all new employees in a DIA were required to attend a 'Day One Security Brief' and attend an 'Introduction to Defence Intelligence Security' course within the first four weeks, with an annual Security Refresher thereafter. Under the Defence Enterprise Collective

[68] ASD, *Submission 3.1*, p. 21.

[69] ASD, *Submission 3.1*, p. 22.

[70] ASD, *Submission 3.1*, pp. 23, 24.

Agreement, all APS staff are also required to undertake one of two 'Essentials' courses for either employees or supervisors, as appropriate.[71]

2.69 The DIAs each reported on the percentage of their staff attending the mandatory courses. These figures indicated that a significant majority, but not all, staff in each agency had completed the mandatory training.[72]

## ONA

2.70 ONA provided an overview of its learning and development program for 2013–14, led by its Director of Professional Analysis and Development. ONA noted that its Open Source Centre had led a review of web research skills training, which led to the introduction of a new social media training course aimed at 'lifting national intelligence community agency capability in the exploitation of open source material'.[73]

2.71 ONA advised that, although it did not have a graduate recruitment program of its own, it had again participated in the Australian Public Service Commission's small agency graduate development program. ONA also noted that it had sponsored two staff to complete postgraduate programs at the National Security College.[74]

## ASIO

2.72 ASIO reported that it had conducted two Intelligence Development Programs for new intelligence officers in 2013–14. ASIO established a new Training Branch in July 2014, outside the reporting period, and had undertaken significant planning in October–November 2014 to remodel the existing Intelligence Development Program.[75]

2.73 ASIO reported on a range of corporate training and development activities that had taken place during the reporting period. This included:

- induction programs for new starters,
- administrative training including contract and finance management, procurement and communication,
- information technology training,
- mandatory training on security awareness, ethics and accountability, public interest disclosure, work health and safety and workplace behaviour, and

[71] ASD, *Submission 3.1*, p. 23.

[72] ASD, *Submission 3.1*, p. 24; DIO, *Submission 3.2*, p. 15; AGO, *Submission 3.3*, p. 21.

[73] ONA, *Submission 2.1*, p. 22.

[74] ONA, *Submission 2.1*, p. 23.

[75] ASIO, *Submission 6.1*, p. 21.

- discipline specific courses, including social, cultural, political and religious history and influences.[76]

2.74 In light of the heightened counter terrorism threat environment, ASIO also delivered a whole-of-organisation officer safety and security training program, underpinned by a Personal Safety and Security Workshop.[77]

2.75 ASIO informed the Committee that it had begun implementing its *Management and Leadership in Security Intelligence Strategy (2013–16)* during the reporting period. This included three management programs, two of which were run with AIC partner agencies.[78]

2.76 Other training and development activities identified by ASIO included:

- language training, across a range of languages, provided to 55 officers as part of its Language Skills Development Program (rising from 26 officers in 2012–13),
- a suite of e-learning modules across a range of disciplines,
- the participation of 166 officers in ASIO's Study Support Program, and
- enabling staff to participate in courses run by the National Security College.[79]

2.77 ASIO noted that it had actively contributed to the shared National Intelligence Community training activities, and had made places available in its training courses to other agencies. ASIO also ran the ASIO Partnership Forum to 'provide a greater understanding of ASIO's work to individuals within the [National Intelligence Community] who work on a regular or semi-regular basis with ASIO'.[80]

2.78 In evidence, ASIO noted that it had a significant focus on leadership and management training and commented:

> We are seeing significant benefits over a number of years from a high-quality leadership and management training regime. [81]

## Workplace diversity

2.79 ASIO advised the Committee that it had broadened its policy work in support of equity and diversity in 2013–14. It had also expanded and revitalised its Harassment and Discrimination Advisor Network,

[76] ASIO, *Submission 6.1*, p. 22.

[77] ASIO, *Submission 6.1*, p. 22.

[78] ASIO, *Submission 6.1*, p. 22.

[79] ASIO, *Submission 6.1*, pp. 22–23.

[80] ASIO, *Submission 6.1*, p. 23.

[81] *Classified Committee Hansard*, 25 March 2015, p. 17.

providing training to all advisors and developing staff and manager guides.[82]

2.80 ONA noted that it complied with the relevant anti-discrimination legislation, and that it 'continued to support the needs of people with disabilities through inclusive staff selection procedures that reflect merit, fairness and freedom from discrimination'.[83]

### Gender

2.81 In June 2014, 57.6 per cent of ongoing APS employees were female, compared with 57.5 per cent in June 2013.[84] The proportion of women to men in the intelligence agencies, however, is lower that the APS average.

2.82 As noted above, women comprised approximately 44 per cent of ASIO's total workforce in 2013–14, which was stable compared to previous years. Consistent with patterns across the broader APS, the gender gap was most pronounced at senior levels, with only 25 per cent of SES and 38 per cent of Senior Officers being women, compared to 50 per cent of grade 1–5 ASIO Officers.[85]

2.83 The proportion of females within ONA in 2013–14 was approximately 41 per cent, a fall of three per cent on the previous year.[86]

2.84 The proportion of women in the DIAs remained particularly low, especially the proportion of female Australian Defence Force personnel in these organisations. The percentage of women in two of the three DIAs increased slightly from 2012–13 to 2013–14, with the figure reducing slightly in the third agency.[87] The Committee heard that the DIA's were

> continuing to identify initiatives that will encourage increased representation of women in our workforce across all APS levels and job families with the agencies.[88]

## Staff feedback and complaints

2.85 The DIAs each reported on their complaint handling processes and mechanisms by which staff could provide feedback.

[82] ASIO, *Submission 6.1*, p. 24.

[83] ONA, *Submission 2.1*, p. 20.

[84] Australian Public Service Commission, *State of the Service Report: State of the Service Series 2013–14*, p. 179; Australian Public Service Commission, *State of the Service Report: State of the Service Series 2011–12*, p. 246.

[85] ASIO, *Submission 6.1*, p. 24.

[86] ONA, *Submission 2.1*, p. 18.

[87] ASD, *Submission 3.1*, p. 12; DIO, *Submission 3.2*, p. 8; AGO, *Submission 3.3*, pp. 7-8.

[88] *Classified Committee Hansard*, 26 March 2015, p. 28.

2.86 ASD noted that it had several mechanisms that employees could use to provide feedback on the work environment, including the Joint Staff Consultative Group, exit interviews, Director's suggestion box, and various organisational blogs.[89]

2.87 All complaints of unacceptable behaviour involving Defence personnel are required to be reported by the manager of the complainant on the 'ComTrack Self-Service' database for monitoring. ASD reported that it had recorded eight complaints of unacceptable behaviour in the database in 2013–14, with six cases closed during the reporting period in accordance with the Defence complaint management process.[90]

2.88 The IGIS received two complaints regarding ASD in 2013–14, both of which were resolved administratively by her office.[91]

2.89 The PID Act replaced the Defence Whistleblower Scheme on 15 January 2014. ASD reported that it had received one disclosure under the PID Act during 2013, which was referred to the Australian Federal Police for action. There had been no complaints made under the previous scheme during the reporting period.[92]

2.90 Non-SES APS staff within Defence can also request a 'Review of Action', enabling them to seek redress if they believed an action taken by another APS employee or Agency Head was unfair or unreasonable. No Review of Action applications were made by ASD employees during the reporting period.[93]

2.91 ONA noted that it had specifically trained Workplace Harassment Contact Officers to support its culture of intolerance of bullying or harassing behaviour. It reported no formal complaints during the period, noting that any complaints or inappropriate behaviour would be 'rapidly dealt with in accordance with ONA's personnel policies'.[94]

### Staff complaints to the Inspector-General of Intelligence and Security

2.92 Under the *Inspector-General of Intelligence and Security Act 1986*, the Inspector-General of Intelligence and Security (IGIS) has limited jurisdiction in relation to employment related grievances within ASD, AGO, DIO and ONA. The IGIS does, however, investigate ASIO and ASIS related employment matters

[89] ASD, *Submission 3.1*, p. 27–28.

[90] ASD, *Submission 3.1*, p. 27; Intelligence and Security Group, Department of Defence, *Submission 3.4*, p. 1.

[91] ASD, *Submission 3.1*, p. 28.

[92] ASD, *Submission 3.1*, p. 28.

[93] ASD, *Submission 3.1*, p. 28.

[94] ONA, *Submission 2.1*, p. 20.

2.93 The IGIS received 17 non-visa related complaints in 2013–14, mostly related to employment matters. The IGIS explained that these complaints were largely from current or former intelligence officers and concerned the revocation of security clearances and subsequent termination of employment. A small number of complaints were also received from individuals who had their 'arrangements' with ASIS terminated.[95]

2.94 Other activities conducted by the IGIS over the reporting period are discussed later in this chapter.

## Accommodation

2.95 AGO noted that it had conducted an accommodation review in 2013–14 that led to the reorganisation of staff within its building to achieve greater efficiencies. A refresh of facilities, including staff lounges and outdoor areas, as well as refurbishment of some offices and work areas was also commenced.[96]

2.96 ONA advised that its property expenses for 2013–14 totalled $5.5 million, equating to $1 047 per square metre. ONA reported that the occupational density of its building—the Robert Marsden Hope Building in Barton—was 18.5 square metre per occupied work point. It noted, however, that the building had been leased on a 15 year term commencing in 2011, prior to the introduction of whole-of-government occupational density targets. ONA also noted that its energy consumption in 2013–14 was 9.83 per cent lower than the previous year and the lowest on record since energy measurement was introduced in 2004–05.[97]

### Relocation of ASIO's central office

2.97 ASIO's new central office, the Ben Chifley Building, was officially opened by the then Prime Minister, the Hon Kevin Rudd MP, on 23 July 2013.

2.98 The building is described as

> a special purpose, high-security building, designed with the capacity and flexibility to meet national security needs now and in the future. Located at 70 Constitution Avenue, Parkes ACT, the building will offer 45 000m$^2$ of net lettable area, accommodate up to 1800 people and operate 24 hours per day.[98]

[95] IGIS, *Submission 4*, pp. 21, 22.

[96] AGO, *Submission 3.3*, p. 25.

[97] ONA, *Submission 2.1*, p. 23.

[98] ASIO, *Ben Chifley Building*, <www.asio.gov.au/About-ASIO/Ben-Chifley-Building.html> viewed 3 June 2015.

2.99 ASIO was originally expected to take possession of the Ben Chifley building by mid-2012, with the main relocation of ASIO staff to commence from late 2012.[99]

2.100 In its previous report on Administration and Expenditure, the Committee noted ASIO's advice that delays in the commissioning and testing essential building services in the building had led to slippages in the dates of handover. ASIO was, at the time of that report, scheduled to take possession of the building in May 2014, with operational capability by late 2014.[100] This was reconfirmed when the Committee inspected the building on 7 March 2014.

2.101 The building remained unoccupied by ASIO staff for the remainder of 2013–14. ASIO took possession of the building on 7 August 2014, outside the reporting period.[101]

## Committee comment

2.102 During the hearings, the Committee discussed with agencies the impact of the operational environment on their workforce, including the impact on staff leave and professional development and training. The Committee also explored current and future staffing needs with some agencies.

2.103 The Committee notes agencies' reporting about recruitment practices in 2013–14 and some of the changes to the vetting of potential staff that were implemented by ASIO. The Committee is interested to obtain a longitudinal picture as to the impact of changed recruitment practices on matters within the scope of its review, such as misconduct and separation rates. The Committee accepts that it is too early to evaluate the impact of these changes in this review and will examine this matter again in 2014-15.

2.104 In its previous review, the Committee recognised the increasing focus on developing and delivering dedicated leadership development and management programs across the intelligence agencies during the 2011–12 and 2012–13 reporting periods. This focus continued in 2013–14.

2.105 Agencies also continued their collaboration within the AIC and with Allied partners to expand training and development opportunities for staff. The Committee agrees that training and development should remain a high priority for all agencies.

[99] Parliamentary Joint Committee on Intelligence and Security, *Review of Administration and Expenditure: No. 10 – Australian Intelligence Agencies*, Canberra, May 2013, p. 19.

[100] Parliamentary Joint Committee on Intelligence and Security, *Review of Administration and Expenditure: No. 11 and No. 12 – Australian Intelligence Agencies*, Canberra, September 2014, pp. 27–28.

[101] ASIO, *Ben Chifley Building*, < www.asio.gov.au/About-ASIO/Ben-Chifley-Building.html> viewed 11 May 2015.

2.106 The Committee reiterates its previous comments that in light of the threat to national security posed by unauthorised disclosure by a 'trusted insider', it is essential that intelligence agencies provide an environment where staff complaints or concerns are investigated thoroughly, both internally and externally, and with independence if necessary.

## Security matters

2.107 The Committee's review of security matters within each agency included:

- changes to security policies and procedures,
- security training,
- security breaches,
- e-security arrangements, and
- security clearances, including current procedures, timelines, delays and any associated outsourcing arrangements.

2.108 Over 2013–14, agencies focussed on reviewing and enhancing policies to mitigate the 'trusted' or 'malicious' insider threat.

2.109 Another issue of focus for intelligence agencies was addressing the cyber security threat.

2.110 Much of the evidence on security matters was classified. The Committee provides an unclassified discussion of security matters below.

### Security policies and procedures

2.111 Agencies reported that they continued to apply robust and effective security arrangements to protect officers, premises, information and assets, by adhering to the Australian Government's Protective Security Policy Framework. Agencies also employed internal security policies and procedures specific to their unique security environment.[102]

2.112 ASIO reported that its security governance was overseen by the ASIO Security Committee, comprising SES representatives, who recommended actions for the secure conduct of ASIO business to the ASIO Executive Board.[103]

2.113 ASIO submitted that its policies and procedures were constantly reviewed to ensure they remained current and relevant. Any changes to policies or

[102] ASIO, *Submission 6.1*, p. 34; ONA, *Submission 2.1*, p. 25.

[103] ASIO, *Submission 6.1*, p. 34.

procedures were communicated to staff via security education and awareness campaigns.[104]

2.114 ASIO advised that it continued to work closely with other government agencies to provide advice to both government and private sector to mitigate threats to security.[105]

2.115 ONA submitted that it participated in inter-agency security forums and committees to assist in the identification and implementation of security best practice.[106]

## The 'trusted' or 'malicious' insider

2.116 Over 2013–14, agencies reviewed and enhanced policies to mitigate the 'trusted' or 'malicious' insider threat. ASIO described 'malicious insiders' as

> trusted employees and contractors who deliberately and wilfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.[107]

2.117 Over the reporting period, ASIO increased its engagement with the Australian Government, both at executive levels and with agency security advisors, to raise awareness of the malicious insider threat.[108]

2.118 Specifically, ASIO worked with key agencies, including the Attorney-General's Department, the Department of the Prime Minister and Cabinet (PM&C) and the Department of Defence, on personnel security policy reforms and associated policy initiatives, with a view to addressing:

- 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.[109]

2.119 ASIO submitted:

> 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

[104] ASIO, *Submission 6.1*, p. 34.

[105] ASIO, *Submission 6.1*, p. 34.

[106] ONA, *Submission 2.1*, p. 25.

[107] ASIO, *Submission 6.1*, p. 34.

[108] ASIO, *Submission 6.1*, p. 34.

[109] ASIO, *Submission 6.1*, p. 34.

> awareness of the potential threat to the security and integrity of government business.[110]

2.120 ONA advised that it monitored staff attitudes to security through specific security related questions in the State of the Service Survey:

> Our most recent survey results are very positive. They show a high level of acceptance and understanding of ONA's requirements for security and staff feel very well supported by the Security Team.[111]

## E-security and the cyber security threat

2.121 ASIO considered that the threat posed by malicious activity conducted by cyber means continued to increase over 2013–14:

> 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 principles.[112]

2.122 ASIO advised that over the reporting period, it provided industry partners with security advice and defensive briefings on the threat posed by cyber espionage to sensitive information and intellectual property.[113]

2.123 ASIO advised that it continually modified and enhanced its e-security capabilities to ensure its information technology systems were adequately protected from both accidental and malicious activity. The agency employed a range of policies and practices to avoid or identify vulnerabilities in its ICT systems.[114]

2.124 ASIO expected that the establishment of the Australian Cyber Security Centre in late 2014 would deliver substantial dividends and momentum on cyber security issues, not least ensuring coordinated and targeted industry outreach.[115]

2.125 The Defence Intelligence and Security Group submitted that the Cyber Security Operations Centre, hosted at the Australian Signals Directorate, continued to work closely within Defence and other government agencies to ensure Australia was protected against emerging cyber threats and

[110] ASIO, *Submission 6.1*, p. 34.

[111] ONA, *Submission 2.1*, p. 26.

[112] ASIO, *Submission 6.1*, p. 9.

[113] ASIO, *Submission 6.1*, p. 4.

[114] ASIO, *Submission 6.1*, p. 35.

[115] ASIO, *Submission 6.1*, p. 9.

adequately positioned to meet the Government's requirement to implement the Top 4 Strategies to Mitigate Targeted Cyber Intrusions — a new mandatory requirement in 2013 under the FMA Act.[116]

2.126 ASD established a dedicated team to engage with Commonwealth, state and territory governments, to enhance cyber security posture through threat assessments, security alerts, and guidance and defensive measures; the revision of the *Australian Government Information Security Manual* (ISM) and vulnerability assessments.[117]

2.127 ONA reported on the actions it took during the reporting period to strengthen its ICT systems and manage the threat posed by an external attacker or trusted insider.[118]

## Security training

2.128 Agencies continued to require that staff undertake mandatory training and maintain proficiency in security awareness.[119]

2.129 During 2013–14, agencies updated or enhanced security training programs in line with the current security environment and security risks.

2.130 In light of the heightened counter terrorism threat environment, ASIO made a significant investment into the design, development and delivery of a whole-of-organisation officer safety and security training program over the reporting period. The program provides:

- a tiered training approach linked to officers' roles, functions and specific operating environment, and
- 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.[120]

2.131 Agencies also reported on mandatory training packages delivered during the reporting period, which focussed on the risks associated with using social media.[121]

[116] Intelligence and Security Group, Department of Defence, *Submission* 3. The FMA Act was replaced with the PGPA Act on 1 July 2014.

[117] Intelligence and Security Group, Department of Defence, *Submission* 3.

[118] ONA, *Submission 2.1*, p. 26.

[119] ASD, *Submission 3.1*, p. 23.

[120] ASIO, *Submission 6.1*, p. 22.

[121] ASD, *Submission 3.1*, p. 30; ONA, *Submission 2.1*, p. 25.

## Security breaches

2.132 There are strict policies and guidelines in place to ensure intelligence agency staff actively and conscientiously take responsibility for classified information and equipment.

2.133 Agencies reported to the Committee on the number and nature of security breaches reported during 2013–14, including any action taken as a result of the breach(es). Agencies also reported on internal and external risk mitigation strategies employed to protect information of national security significance.

2.134 Much of the evidence provided to the Committee regarding security breaches is classified and cannot be discussed in this report.

2.135 ASIO noted that it was 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 were notified of breaches within their branch or division to enable proactive management of each occurrence.[122]

2.136 The DIAs reported on the range of internal and external mitigation strategies agencies employed to protect information and reduce costs and resource overheads associated with management and clean-up of data spills. Defence Intelligence Security, on behalf of the DIAs, invested heavily in external customer liaison and security briefings, to assist customers in developing and implementing tailored mitigation strategies to reduce the likelihood of recurrence.[123]

## Security clearances

2.137 Personnel across the AIC are required to secure and maintain an appropriate security clearance to perform their roles.

2.138 As part of its review, the Committee sought evidence from agencies regarding the processing times and outcomes of security clearances undertaken over each reporting period.

2.139 Much of the evidence provided to the Committee regarding security clearances is classified and cannot be discussed in this report.

2.140 ASIO reported on the continued pressures on its initial vetting and revalidation of security clearances, and advised that it was proactively seeking ways to become more efficient in security vetting processes, without compromising its high standards of security practices.[124] ASIO

[122] ASIO, *Submission 6.1*, p. 35.

[123] ASD, *Submission 3.1*, pp. 32–33; AGO, *Submission 3.3*, pp. 30–31.

[124] ASIO, *Submission 6.1*, p. 35.

outlined the specific changes it had made to vetting practices to achieve efficiencies in classified evidence to the Committee.

### Committee comment

2.141 On the basis of evidence provided, the Committee is satisfied that agencies have robust procedures and guidelines in place to protect their people, premises, assets and information. The Committee is encouraged to see that agencies are adapting their policies and procedures to meet emerging and increasing threats, including the trusted/malicious insider threat and the cyber security threat.

## Oversight and accountability

2.142 There are a number of internal and external oversight and accountability mechanisms in place for each of the intelligence agencies to provide assurance to the Australian public of the legality and propriety of their activities. These mechanisms include:

- internal reviews,
- Ministerial and Parliamentary accountability,
- the IGIS, and
- for ASIO, the Independent Reviewer of Adverse Security Assessments.

2.143 Agencies also regularly undertake, or are subject to, a formal assessment of their performance.[125] The performance of collection agencies is evaluated against the National Intelligence Priorities on a rolling cycle. ONA, for example, undertakes a bi-annual review of its assessments to provide internal quality assurance.[126] ASD periodically conducts a Sigint Services Performance Review, with input from its customers, to assess its performance against strategic goals.[127]

2.144 DIO commented that, arising from the 2011 Independent Review of the Intelligence Community, it was subject to a performance review by the Defence Strategic Policy Division. DIO advised the Committee of the findings of the review conducted in the reporting period.[128]

[125] ASIS, *Submission 5*, p. 28.

[126] ONA, *Submission 2.1*, p. 10.

[127] ASD, *Submission 3.1*, p. 39.

[128] *Classified Committee Hansard*, 26 March 2015, p. 31.

2.145 ONA and ASIS noted that they are subject to reviews of their performance by PM&C.[129]

2.146 ONA also undertakes two broader evaluations. First, ONA undertakes annual performance evaluations of ASD, AGO and ASIS's foreign intelligence collection activities, which, with the evaluations of ONA and ASIO by PM&C, are provided in an annual report to the National Security Committee of Cabinet.[130] Secondly, ONA undertakes special-purpose evaluations of foreign intelligence activities. The Committee heard that these evaluations examine agency activities but also look at the question of measurable outcomes.[131] One agency head informed the Committee that the reports provided the government with a 'very clear understanding and appraisal of how the money is being spent and the successes, weaknesses and failures'.[132]

2.147 Agencies also reported in their submissions on their interaction with Ministers and the Parliament.[133]

## Inspector-General of Intelligence and Security

2.148 The IGIS is an independent statutory office holder with responsibility for reviewing the activities of the AIC agencies. The IGIS's purpose is to ensure that

> each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and is consistent with human rights.[134]

2.149 The IGIS can also, at the request of the Prime Minister, inquire into an intelligence or security matter relating to any Commonwealth agency.

2.150 The Committee sought a submission from the IGIS on any issues of administration and expenditure arising during IGIS's inspection and inquiry activities in the reporting period. The IGIS also appeared at a private hearing, during which the Committee sought additional information on inquiries and other inspections conducted during the reporting period.

[129] ONA, *Submission 2.1,* p. 10; ASIS, *Submission 5,* p. 28.

[130] ONA, *Submission 2.1,* p. 9; *Classified Committee Hansard,* 26 March 2015, pp. 21–22, 30. Like ONA, ASIO is evaluated by PM&C.

[131] *Classified Committee Hansard,* 26 March 2015, p. 22.

[132] *Classified Committee Hansard,* 26 March 2015, p. 11.

[133] *Classified Committee Hansard,* 26 March 2015, p. 11; ONA, *Submission 2.1,* p. 11; ASIO, *Submission 6.1,* pp. 36–37; ASIS, *Submission 5,* p. 28.

[134] IGIS, *Submission 4,* p. 4. The functions of the Inspector-General are prescribed under sections 8, 9 and 9A of the *Inspector-General of Intelligence and Security Act 1986*.

2.151 Agencies informed the Committee about their interaction with the IGIS and her office throughout the reporting period.[135]

2.152 In 2013–14, the IGIS completed three major inquiries relating to:

- the attendance of legal representatives at ASIO interviews,
- the actions of ASIO, the Australian Federal Police and the then Department of Immigration and Citizenship relating to an Egyptian irregular maritime arrival who was placed in immigration detention and was the subject of an Interpol red notice, and
- ASIS's provision of weapons and training in weapons and self-defence to its staff, and the use of weapons and self-defence techniques by ASIS staff.[136]

## Attendance of legal representatives at ASIO interviews

2.153 This inquiry investigated allegations that ASIO officers had made arbitrary decisions regarding the attendance of legal representatives at security assessment interviews.

2.154 While the IGIS determined that ASIO's policy on this issue was sound, she made a number of recommendations to improve practices.[137] ASIO agreed to four recommendations in full and a fifth in part, and had reported to the IGIS on implementation of the recommendations by the end of the reporting period.[138] ASIO noted that it had developed policy to reflect the IGIS' recommendations and that it was conducting appropriate training for new officers.[139]

2.155 ASIO also reported its views to the Committee on the fifth recommendation in its classified submission.[140]

2.156 During the hearing, the Committee discussed the intent of the IGIS's recommendation about migration agents. The IGIS made the following observation:

> My recommendation was not that ASIO should definitely have migration agents present but that they should consider it on a case-by-case basis. Sometimes these people are there to provide support rather than advice, and I feel that ASIO is equipped to

[135] ASIS, *Submission 5,* pp. 28-29; DIO, *Submission 3.2,* p. 23; AGO, *Submission 3.3,* p. 33; ASD, *Submission 3.1,* p. 40; ONA, *Submission 2.1,* p. 11; ASIO, *Submission 6.1,* pp. 37–39.

[136] IGIS, *Submission 4,* p. 6.

[137] IGIS, *Submission 4,* pp. 6–7.

[138] IGIS, *Submission 4,* p. 7.

[139] ASIO, *Submission 6.1,* p. 38.

[140] ASIO, *Submission 6,* p. 45.

> decide on a case-by-case basis, rather than having a blanket refusal.[141]

## Inquiry into the management of the case of Mr E

2.157 This inquiry was initiated at the request of the then Prime Minister. The IGIS examined the handling of a particular asylum seeker with complex security issues as well as the Government's management of complex security cases more generally.

2.158 The IGIS made a number of findings in this case, and noted that significant changes were initiated in ASIO and the Department of Immigration and Border Protection during the inquiry to introduce considerably more robust security checking processes prior to community detention or the issue of bridging visas. ASIO also published guidance for staff on how to do the checks and escalate and resolve concerns, while the Department established a team to identify and oversight national security and serious criminality cases.[142]

2.159 Agencies advised the IGIS at the end of the reporting period on their progress in implementing the inquiry recommendations.[143] ASIO noted in its submission that it had accepted the IGIS's recommendations in full.[144]

## Inquiries into the use of weapons and self-defence techniques in ASIS

2.160 The IGIS commenced her first inquiry in April 2013 and finalised it in November 2013. A second inquiry was commenced in June 2014.

2.161 The first inquiry identified two main concerns relating to delays in providing oleoresin capsicum spray and batons to some overseas stations and controls on the consumption of alcohol.[145] The second inquiry resulted from an incident that occurred overseas that revealed issues relating to adherence to (internal) policies, which are documented in the IGIS's annual report. An (internal)-initiated investigation of the incident highlighted systemic issues, including inaccuracies with the information provided to the IGIS during the course of the 2013 inquiry.[146]

2.162 ASIS advised that it had accepted the IGIS's recommendations resulting from the first inquiry and that it was continuing to consult with the IGIS on improvements to operations and policies. In relation to the second inquiry, ASIS advised that it would work closely with the IGIS to

[141] *Classified Committee Hansard,* 19 March 2015, p. 2.

[142] IGIS, *Submission 4,* p. 8.

[143] IGIS, *Submission 4,* p. 8.

[144] ASIO, *Submission 6.1,* p. 39.

[145] IGIS, *Submission 4,* pp. 8-9.

[146] IGIS, *Submission 4,* p. 9; See also IGIS, *Annual Report 2013–14,* pp. 10–11.

implement the recommendations of this report.[147] The Committee also obtained additional information during the private hearing with the IGIS.[148]

### Other matters

2.163 Throughout 2013–14, the IGIS continued her regular examination of agency records to ensure that agency activities complied with relevant legislative and policy frameworks. The IGIS reported that

> overall the level of compliance in each of the intelligence agencies is very high.[149]

2.164 The IGIS's submission summarised her inspections throughout the reporting period. During the classified hearing, the Committee sought further information from the IGIS on a range of matters relating to human rights considerations, ministerial authorisations, warrants, interaction with foreign agencies and the identification of Australians.[150] The Committee also took the opportunity to discuss compliance more broadly with the IGIS.[151]

2.165 In her submission, the IGIS noted that she had conducted a review of DIO's implementation of the recommendations of the inquiry into analytic independence (2012–13), finding that DIO had made good progress in implementing the recommendations.[152] DIO commented in its submission:

> IGIS regarded DIO's implementation of the Review of Key Judgements process as particularly robust and successful; the process involves the monthly review of two previous DIO products and provides a basis for the systematic identification and review of previous judgements made by DIO analysts. The process also provides a tradecraft benefit, allowing analysts to contest and challenge underlying assumptions and plan for future products.[153]

## Independent Reviewer of Adverse Security Assessments

2.166 Three types of security assessments are issued by ASIO: adverse, qualified and non-prejudicial.[154]

[147] ASIS, *Submission 5,* p. 29.

[148] *Classified Committee Hansard,* 19 March 2015, p. 5.

[149] IGIS, *Submission 4,* p. 5.

[150] *Classified Committee Hansard,* 19 March 2015, pp. 8–12, 15–16.

[151] *Classified Committee Hansard,* 19 March 2015, pp. 12–13.

[152] IGIS, *Submission 4,* p. 9.

[153] DIO, *Submission 3.2,* p. 23.

[154] ASIO, *Submission 6.1,* p. 46.

2.167 The role of the Independent Reviewer of Adverse Security Assessments (the Independent Reviewer) is to

> Review ASIO adverse security assessments (ASAs) given to the Department of Immigration and Border Protection in relation to people who remain in immigration detention and have been found to:
>
> 1. engage Australia's protection obligations under international law, and
> 2. not be eligible for a permanent protection visa, or who have had their permanent protection visa cancelled.[155]

2.168 In performing her role, the Independent Reviewer is required to examine all material relied on by ASIO in making an adverse security assessment, provide an opinion to the Director-General of Security as to whether the adverse security assessment is appropriate, and make recommendations for the Director-General's consideration.[156]

2.169 ASIO advised that 54 cases were before the Independent Reviewer at the start of 2013–14. Subsequently, three assessments were amended to either non-prejudicial or qualified as a result of ASIO's internal review process and 17 reviews were finalised by the Independent Reviewer by the end of the year.[157]

2.170 In relation to these 17 cases, the Independent Reviewer found 15 to be appropriate, one to be inappropriate and provided additional information in the final case that resulted in ASIO issuing a new qualified security assessment. Where ASIO's assessment was found to be inappropriate, ASIO re-examined the case and issued a qualified security assessment.[158]

2.171 During the reporting period, the Independent Reviewer also provided ASIO with new information and draft reports for a further 16 cases.[159]

2.172 During the private hearing, the IGIS commended the work of the Independent Reviewer, noting it had been effective.[160]

[155] Attorney-General's Department, *Independent Reviewer of Adverse Security Assessments,* <www.ag.gov.au> viewed 7 May 2015.

[156] ASIO, *Submission 6.1,* p. 39.

[157] ASIO, *Submission 6.1,* p. 39. See also p. 40 for an explanation of ASIO's internal review process.

[158] ASIO, *Submission 6.1,* p. 39.

[159] ASIO, *Submission 6.1,* pp. 39–40.

[160] *Classified Committee Hansard,* 19 March 2015, p. 7.

## Independent National Security Legislation Monitor

2.173 The Independent National Security Legislation Monitor (INSLM) is appointed under the *Independent National Security Legislation Monitor Act 2010* on a part time basis for a three year term. The INSLM's role is to:

> Review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation on an ongoing basis. This includes considering whether the laws contain appropriate safeguards for protecting the rights of individuals, remain proportionate to any threat of terrorism or threat to national security or both, and remain necessary.[161]

2.174 Mr Bret Walker AO held the position for a three year term until April 2014, following which it remained vacant until December 2014 when the Hon Roger Gyles AO QC was appointed on an acting basis, pending a permanent appointment.[162]

2.175 During the reporting period, the INSLM's third and fourth annual reports were provided to the Prime Minister on 8 November 2013 and 28 March 2014, and subsequently tabled in Parliament.

2.176 ASIO reported in its submission on a number of recommendations of the INSLM that were relevant to ASIO's activities. Matters addressed by the INSLM included:

- ASIO's questioning powers,
- interim passport suspension,
- introduction of a 'special intelligence operation' scheme,
- streamlining cooperation between ASIO and ASIS,
- revocation of citizenship on security grounds, and
- amending the name or alias of a proscribed terrorist organisation.[163]

2.177 The Committee notes that some of these matters were addressed in legislative amendments reviewed by the Committee outside the reporting period.

## Committee comment

2.178 The Committee sought information from agencies during the hearings about the assessment of their performance and the evaluation of

[161] PM&C, *Independent National Security Legislation Monitor,* <www.dmpc.gov.au> viewed 8 May 2015.

[162] PM&C, *Independent National Security Legislation Monitor,* <www.dmpc.gov.au> viewed 8 May 2015.

[163] ASIO, *Submission 6.1,* pp. 30-31.

measurable outcomes in what was a tight fiscal environment. The Committee considers the performance framework for the AIC agencies to be an important accountability mechanism.

2.179 The Committee took the opportunity during hearings with the IGIS to obtain additional information about some of the key oversight matters arising in 2013–14. The Committee acknowledges that those matters raised by the IGIS represent a small proportion of the work carried out by the AIC agencies. In particular, the Committee notes the IGIS's comment that agencies are 'doing things right most of the time' with only a 'handful' of errors identified each year.[164]

2.180 Outside the reporting period, legislation to amend and broaden the powers of the intelligence agencies was passed by the Parliament. The Committee will continue to monitor the oversight and accountability arrangements of the AIC agencies in light of this changed legislative environment in its future reviews.

## Public relations

2.181 Where possible, agencies have endeavoured to engage with the public through their unclassified public websites and/or public statements and speeches made via their agency head.

2.182 ASIO noted that the Director-General continued to engage with the public through statements and speeches on matters including the security environment in Syria, cyber threats, the Ben Chifley Building and ASIO's new strategic plan. ASIO makes transcripts of speeches, public submissions, its *Report to Parliament*, and other information available on its website.[165]

2.183 ONA similarly makes a range of information available on its website, contributes to publications, and responds to Senate Orders and parliamentary questions.[166] ONA also coordinated AIC responses to media inquiries on disclosures by former NSA contractor, Edward Snowden.[167]

2.184 DIO noted that it had published its Defence Economic Trends in the Asia-Pacific in 2014 on the Defence website.[168]

[164] *Classified Committee Hansard,* 19 March 2015, p. 10.

[165] ASIO, *Submission 6.1,* p. 40.

[166] ONA, *Submission 2.1,* p. 11.

[167] ONA, *Submission 2.1,* p. 2.

[168] DIO, *Submission 3.2,* p. 23.

2.185 AGO's engagement with the media in 2013–14 related to the search for missing Malaysian Airlines passenger aircraft MH370.[169]

2.186 ASD undertook considerable work in response to the disclosures by Edward Snowden.[170] Throughout the year, ASD also contributed to responses to media queries on a range of issues.[171]

2.187 ASD participated in a number of public cyber security forums, workshops and presentations, and published articles relating to ICT security issues. This included a major update in August 2013 to the ISM Controls Manual, as well as cyber security advice, published on OnSecure, ASD's central online community for cyber security professionals within the Australian government and critical infrastructure agencies. A number of products were also published on ASD's public website.[172]

## Requests for access to public records

2.188 Agencies continued to cooperate with requests for public access to agency records, balancing the right to access public records with the need to protect certain information from disclosure.

2.189 ASIO noted an increasing number of requests for access to records in 2013–14, with a 75 percent increase in applications. ASIO commented that

> [d]espite permanently allocating a significant number of officers to service public requests, ASIO faces challenges in meeting the 90 day legislated turnaround time.[173]

2.190 In 2013–14, 82 percent of requests were overdue. ASIO attributed this to several factors:

- a high number of requests, with 773 in 2013–14,
- the time required to process each request – with current staffing levels, ASIO estimates that current requests will take five to six years to process, and
- the reduced closed period from 30 to 20 years.[174]

2.191 ASIO noted in particular that

> [c]urrently 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

[169] AGO, *Submission 3.3,* p. 32.

[170] ASD, *Submission 3.1,* pp. 35–36.

[171] ASD, *Submission 3.1,* p. 36.

[172] ASD, *Submission 3.1,* p. 38.

[173] ASIO, *Submission 6.1,* p. 42.

[174] ASIO, *Submission 6.1,* p. 42.

> 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.[175]

2.192 Other agencies also responded to public access requests.[176] In 2013–14, DIO processed and completed 27 referrals.[177] ASD received 11 requests, with one remaining outstanding at the end of the year.[178] AGO received no requests in the reporting period.[179]

2.193 DIO noted that

> the consolidation of improved business and information-sharing processes between DIO and the Directorate of Records Management and Access continued to increase DIO's expertise in resolving complex cases and reducing processing times for referrals.[180]

2.194 During the hearings, one agency head commented on the resourcing implications in managing public access requests, including the cumulative impact of small pieces of sensitive information being made available.[181]

2.195 Agencies were also involved in the National Archives of Australia Annual Cabinet Release.[182]

## Committee comment

2.196 The Committee notes the resource implications for agencies arising from requests for public access to records and the concerns raised by some agencies. This matter was also raised in the Committee's 2011–12 and 2012–13 reviews. The Committee will continue to monitor the issue.

[175] ASIO, *Submission 6.1,* p. 42.

[176] ONA, *Submission 2.1,* pp. 12–13.

[177] DIO, *Submission 3.2,* p. 23.

[178] ASD, *Submission 3.1,* p. 37.

[179] AGO, *Submission 3.3,* p. 32.

[180] DIO, *Submission 3.2,* p. 23.

[181] *Classified Committee Hansard,* 26 March 2015, p. 18.

[182] ASIO, *Submission 6.1,* p. 42; ONA, *Submission 2.1,* pp.12-13; DIO, *Submission 3.2,* p. 23; ASD, *Submission 3.1,* p. 37;

## Concluding comments

2.197 The Committee has conducted a thorough review of the administration of the six intelligence agencies for the 2013–14 financial year and is satisfied that agencies are overseeing their administrative functions effectively.

2.198 The Committee notes that agency priorities in 2013–14 continued to adapt to the operational environment at that time, which, with the budgetary situation, impacted on many of the administrative matters considered in this review.

2.199 Agencies managed staffing numbers within a constrained budgetary environment. Agencies also continued to address the challenges faced in recruiting staff with the skills needed in their organisations as well as developing effective strategies to retain and develop existing staff.

2.200 The Committee heard that training and development continues to be prioritised. The Committee supports the development and maintenance of those skills essential to each agency's capabilities.

2.201 A number of matters have been investigated by the IGIS or in other internal or external reviews over the reporting period. The Committee accepts that the actions arising from these reviews are being or have been addressed.

2.202 Overall, the Committee has not identified any areas of concern and considers that the administration of the six intelligence agencies is conducted appropriately.