# 2

# Administration

2.1 In undertaking its review of the administration of the intelligence agencies for the 2011-12 and 2012-13 financial years, the Committee asked agencies to provide submissions addressing:

- any legislative changes that have impacted on administration,
- human resource management,
- the structure of the organisation and distribution of staff,
- pressures and management of expansion, where applicable,
- security issues, including the status of security clearances and any security breaches,
- public relations and/or public reporting, where applicable,
- strategic direction/planning, and
- performance management and evaluation.

2.2 In their submissions, agencies outlined significant developments and relevant aspects of administration for each financial year. 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 both 2011-12 and 2012-13, including information on:

- the frequency and nature of the use of powers,

- the amount of time expended on particular areas,
- staffing implications,
- training,
- the role of legal officers,
- the need for specialist staff, and
- relationships with outside agencies such as police or the judiciary.

## 2011-12

2.4 In 2011-12, a number of changes were made to the legislative framework governing the operations of ASIO, ASD, AGO and ASIS through amendments to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act).

*2.5* The (then) Government determined that legislative amendments to the IS Act and ASIO Act should be considered in three tranches. The first and second set of amendments occurred in 2011-12 with enactment of the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* and *Intelligence Services Legislation Amendment Act 2011*.[1]

2.6 AGO advised that amendments to the IS Act affected administration of the organisation. Legislative changes included:

- inclusion of a section clarifying AGO's function to support the ADF through military operations and cooperate with the ADF on intelligence matters,[2]
- a new ground for obtaining a Ministerial Authorisation for the purpose of producing intelligence on an Australian person, where the Minister is satisfied that person is involved in, or likely to be involved in, activities related to a contravention of a United Nations sanctioned enforcement law,[3] and
- an amendment to ensure that the immunity provisions in Section 14 of the IS Act cannot be limited inadvertently.[4]

2.7 Commencing in March 2011, amendments to the IS Act and ASIO Act enabled greater collaboration between the intelligence agencies in the performance of their respective functions.[5] Under the changes, such

1 DIGO (AGO) (Review No. 11), *Submission 3*, p. 7.
2 DIGO (AGO) (Review No. 11), *Submission 3*, p. 7; *Intelligence Services Act 2001*, s 6B(g).
3 DIGO (AGO) (Review No. 11), *Submission 3*, pp. 7-8.
4 DIGO (AGO) (Review No. 11), *Submission 3*, p. 8.
5 DSD (ASD) (Review No. 11), *Submission 5*, p. 3. See also DIO (Review No. 12), *Submission 4*, p. 7.

cooperation could include providing staff and other resources to ASIO or another specified agency.[6]

2.8 DIO is the only agency to not fall with the scope of these legislative amendments. DIO noted that as a member of the AIC the changes would affect how it interacted with other agencies.[7]

## Proposed legislative reform

2.9 The (then) Government approved referral of the third tranche of amendments to national security legislation on 16 April 2012.[8] In May 2012, the then Attorney-General, the Hon Nicola Roxon MP asked the Parliamentary Joint Committee on Intelligence and Security to inquire into potential reforms to Australia's national security legislation.[9]

2.10 Detailed discussion of these proposed reforms can be found in the Committee's report for that inquiry, which was tabled in June 2013.[10] Each intelligence agency made submissions to the inquiry and provided information in private hearings.[11]

2.11 ASIO outlined these reforms as follows:

- reform of the *Telecommunications (Interception and Access) Act 1979*, including proposals that modernise lawful access to communications and associated communications data;
- amendments to the *Telecommunications Act 1997* and other relevant legislation to strengthen measures to mitigate the national security risks posed to Australia's telecommunications infrastructure; and
- amendments to the ASIO Act and *Intelligence Services Act 2001* which seek to improve the operational capabilities of intelligence agencies, as well as making some technical and administrative amendments.[12]

2.12 ASIO submitted that these legislative amendments were necessary to equip intelligence agencies to meet the challenges posed by current and emerging technologies.[13] The reforms would enable ASIO and other

---

6 DSD (ASD) (Review No. 11), *Submission 5*, p. 3; *Intelligence Services Act 2001*, s 7(f), s 13A.

7 DIO (Review No. 12), *Submission 4*, p. 7.

8 DIGO (AGO) (Review No. 11), *Submission 3*, p. 8.

9 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, <www.aph.gov.au/pjcis>.

10 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, <www.aph.gov.au/pjcis>.

11 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 24 June 2013, <www.aph.gov.au/pjcis>.

12 ASIO (Review No. 11), *Submission 7*, p. 34.

13 ASIO (Review No. 11), *Submission 7*, p. 34.

agencies to operate effectively into the future while maintaining the appropriately stringent accountability regime existing across the intelligence and law enforcement agencies.[14]

2.13 Similarly, AGO submitted that:

> This package of legislative amendments seeks to ensure that the statutory powers accorded to Australia's intelligence and law enforcement agencies remain effective in the current and future national security environment.[15]

## 2012-13

2.14 The Committee's inquiry into potential reforms of Australia's national security legislation continued into the 2012-13 financial year. In their submissions, agencies noted that they continued to collaborate on the proposed amendments to ensure that the legislative framework supported agency functions and capabilities.[16]

2.15 Commenting on telecommunications reforms, ASIO submitted that it strongly supported legislative change:

> ASIO believes reform of the legislation governing interception and access to telecommunications data is required to create a regime that is sufficiently robust and technologically neutral so as not to require revision with each new technological or business development.[17]

2.16 The Committee agrees that the agencies of the Australian Intelligence Community need to be able to meet the challenges posed by current and emerging technologies.

### Recommendation 1

**The Committee recommends that the Australian Government consider the legislative and other reforms necessary to equip the Australian Intelligence Community to meet the challenges posed by current and emerging technologies.**

---

14 ASIO (Review No. 11), *Submission 7*, p. 34.

15 DIGO (AGO) (Review No. 11), *Submission 3*, p. 8.

16 See for example, AGO (Review No. 12), *Submission 3*, p. 5. The Committee notes that outside the reporting period, the Senate Legal and Constitutional Affairs References Committee commenced an inquiry into the *Telecommunications (Interception and Access) Act 1979.*

17 ASIO (Review No. 12), *Submission 7*, p. 30.

2.17 Also in 2012-13, the *Foreign Affairs Portfolio Miscellaneous Measures Act 2013* amended the *Workplace Health and Safety Act 2011* to enable the Director-General of ASIS to declare that the provisions of the Act would not apply in certain circumstances. This provided consistency with provisions already applying to ASIO and the ADF.[18] Amendments to the IS Act also provided a mechanism for ASIS employees employed under the IS Act to voluntarily transfer between APS agencies.[19]

2.18 AGO sought amendments to section 6B(e) of the IS Act to clarify its functions so as to:

- remove any doubt that the AGO is enabled to provide Commonwealth and State authorities (and other approved bodies) assistance in the production and use of geospatial products,[20] and
- include express reference to specialised imagery and geospatial technologies as a function.[21]

2.19 Legislation to enact the change of name for AGO and ASD was drafted during 2012-13.[22]

## Litigation

2.20 The trend of increased ASIO involvement in legal and judicial matters continued during 2011-12. ASIO was involved in 58 litigation matters in this period, including criminal (particularly terrorism) prosecutions, judicial and administrative reviews of security assessments, and a range of civil actions.[23]

2.21 ASIO stated that the scope and diverse nature of its involvement in legal proceedings placed a strain on the organisation's legal, operational and administrative resources in preparing appropriate support and input, while maintaining appropriate protection of security classified information.[24]

2.22 In 2012-13, ASIO advised that it was involved in approximately 50 litigation matters, including terrorism, other criminal prosecutions and

18 ASIS (Review No. 12), *Submission 6*, p. 29.
19 ASIS (Review No. 12), *Submission 6*, p. 29.
20 AGO (Review No. 12), *Submission 3*, p. 5.
21 AGO (Review No. 12), *Submission 3*, p. 6.
22 AGO (Review No. 12), *Submission 3*, p. 6.
23 ASIO (Review No. 11), *Submission 7*, p. 35.
24 ASIO (Review No. 11), *Submission 7*, p. 35.

civil matters. Civil matters largely related to judicial and administrative review of ASIO security assessments.[25]

2.23 ASIO submitted that ASIO's involvement in litigation was expected to continue due to the continued upward trend in merits and judicial review of adverse security assessments and the recent surge in criminal prosecutions that required ASIO's intelligence as evidence.[26]

### Use of ASIO's special powers

2.24 ASIO reports each year on the use of its special powers under the ASIO Act and the *Telecommunications (Interception and Access) Act 1979* to use methods of investigation such as telecommunications interception and access, listening devices, entry and search of premises, computer access, tracking devices and examination of postal and delivery service articles. The use of these powers is subject to a warrant approved by the Attorney-General.[27]

2.25 Further, the ASIO Act enables ASIO, with the Attorney-General's consent, to seek warrants from an independent issuing authority (a judge) for questioning, or questioning and detention, of individuals.[28]

2.26 The number of warrants approved by the Attorney-General in 2011-12 and 2012-13 is classified and cannot be reported by the Committee. However, the Committee reviewed the number of warrants approved by the Attorney-General across the two reporting periods, as reported by warrant type.

## Strategic direction and organisational structure

2.27 The Committee requested agencies to report on any changes made to the structure and strategic direction of their organisation, including developments in staffing arrangements, during the reporting periods.

### ASIO

2.28 ASIO restructured and refined its organisational structure in 2011-12 in response to current and anticipated budgetary constraints. This included

25 ASIO (Review No. 12), *Submission 7*, p. 31.
26 ASIO (Review No. 12), *Submission 7*, p. 31.
27 ASIO (Review No. 12), *Submission 7*, p. 32.
28 ASIO (Review No. 12), *Submission 7*, p. 32.

reducing its 11 divisions to eight.[29] ASIO considered the restructure would:

- align like functions;
- reinforce the ASIO mission and the way each Division contributes to the mission; and
- maximise the impact of outreach through consolidated Divisional engagement.[30]

2.29 ASIO informed the Committee that the organisation had moved from a period of growth to a period of consolidation.[31] ASIO's reform and modernisation program had enabled agility in the face of a complex security environment, and allowed for the maintenance of Australia's nationally important security intelligence capability, while also finding efficiencies in undertaking its work.[32]

2.30 In 2011-12, ASIO also deferred the program of growth recommended by Mr Allan Taylor AM in the 2005 Review of ASIO Resourcing (the Taylor Review).

2.31 The Taylor Review recommended that ASIO have 1 860 full time staff by 2012-13.[33] In 2010-11, ASIO increased its staffing level to 1 769 staff. However, following an internal review, ASIO reduced its approved staffing target to 1 760 in February 2012. Subsequently, in light of its then budget, ASIO decided to maintain a level of 1 730 full-time equivalent staff.[34]

2.32 In 2012-13, ASIO's new *Strategic Plan 2013-16* recognised that many of ASIO's broad strategic objectives remained. The four goals identified in the new Strategic Plan were:

- 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.[35]

---

29 ASIO (Review No. 11), *Submission 7*, p. 19.

30 ASIO (Review No. 12), *Submission 7*, p. 16.

31 ASIO (Review No. 11), *Submission 7*, p. 22.

32 ASIO (Review No. 11), *Submission 7*, p. 22.

33 ASIO (Review No. 11), *Submission 1,* p. 28. See also, *Review of Administration and Expenditure: No. 10 – Australian Intelligence Agencies*, May 2013, Canberra, pp. 8-9.

34 ASIO (Review No. 11), *Submission 1,* p. 28.

35 ASIO (Review No. 12), *Submission 7*, p. 19.

## ONA

2.33 ONA also restructured its organisation in mid-June 2012. This saw the dissolution of one of its 11 branches, the Atlantic Branch, with its personnel and responsibilities distributed across other branches. The restructure resulted in the saving of one SES position.[36]

## Defence Intelligence Agencies

2.34 In late 2011, AGO's *Strategic Plan 2011-2021* was published, with the three key themes of knowledge, collaboration, and people.[37]

2.35 The six enduring strategic priorities of the organisation remained:

- adapting data acquisition and management for an information-rich environment,
- delivering products and services critical to customers' decision-making,
- unlocking unique information and intelligence and innovation,
- leading the growth of geospatial intelligence (GEOINT) capability within Defence and the Australian Government,
- creating a team to lead and succeed through continuous change, and
- achieving best practice in governance, compliance and security.[38]

2.36 AGO reported several changes to its organisational structure (which also affected the other DIAs) during 2011-2012, including:

- disbanding the Joint Fusion Development Directorate, a joint team formed in 2008 with ASD to develop analytic tools, techniques, processes and business practices, as it had achieved its objectives,
- formation of the Defence Intelligence Counter-Proliferation Team with ASD and DIO in late 2011, which is to provide intelligence to help prevent, or disrupt, the proliferation of weapons of mass destruction,
- creation of the Asian Security Developments Directorate from the previous Asia and Pacific Developments Directorate, with a primary focus on the production of GEOINT and technical intelligence on regional defence capabilities and security issues in countries across South-East Asia, and
- postponement of the Geospatial Technician Training Program that had been due to commence training in October 2012.[39]

---

36 ONA (Review No. 11), *Submission 6*, pp. 14-15.

37 DIGO (AGO) (Review No. 11), *Submission 3*, p. 2.

38 DIGO (AGO) (Review No. 11), *Submission 3*, p. 2.

39 DIGO (AGO) (Review No. 11), *Submission 3*, pp. 8-9.

## Australian Cyber Security Centre

2.37 In 2012-13, the then Prime Minister, the Hon Julia Gillard MP, announced establishment of the Australian Cyber Security Centre (ACSC), as part of the National Security Strategy. The ACSC was to enable stronger understanding of the new cyber threat and facilitate faster and more effective responses to cyber security incidents.[40]

2.38 In a significant structural change within the intelligence agencies, all cyber security capabilities of Defence (ASD, DIO, Cyber Security Operations Centre), the Attorney-General's Department, ASIO, Australian Federal Police and Australian Crime Commission would be co-located in the ACSC.[41]

## Pathways to Change

2.39 Within Defence as a whole, the *Pathway to Change: Evolving Defence Culture* (Pathway to Change) strategy was released in March 2012 in response to a number of reviews into Defence and ADF culture.[42] The strategy is to shape Defence's attitudes, systems and behaviours to improve capability and ensure the continued support of the Australian public.[43]

2.40 In response to Pathway to Change, AGO has been involved in a number of initiatives, including holding all-staff briefings in November 2012, a broadening of ASD's outreach program to include AGO, and keeping staff on long-term leave connected with the workforce.[44]

2.41 The other DIAs also developed and implemented initiatives to assist in providing a fairer and more inclusive workplace in support of the retention of its employees.

2.42 ASD submitted:

> The Intelligence and Security Group is committed to Pathway to Change and to building on our strengths. ASD recognises that some cultural changes are needed to clearly demonstrate that we are 'trusted to defend, proven to deliver and respectful always'. In 2012-13, ASD delivered agency-specific initiatives to continue the organisation's commitment to implementing the recommendations that were included in the cultural reviews.[45]

---

40 ASD (Review No. 12), *Submission 5*, p. 10.

41 ASD (Review No. 12), *Submission 5*, p. 10.

42 AGO (Review No. 12), *Submission 3*, p. 2; ASD (Review No. 12), *Submission 5*, p. 3.

43 AGO (Review No. 12), *Submission 3*, p. 2.

44 AGO (Review No. 12), *Submission 3*, p. 2.

45 ASD (Review No. 12), *Submission 5*, p. 3.

2.43 ASD's aim in its *Pathway to Change Strategy* for 2012-13 was to shape ASD's attitudes, systems and behaviours to improve capability. A key initiative in 2012-13 was to embed a mentoring culture in ASD. In doing this, ASD commenced an internal mentoring program which included a guest speaker leadership series, development of a new entrant mentoring framework, social media training and the creation of a senior female advisory group.[46]

## Human resource management

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

- recruitment and retention,
- separation rates,
- training,
- workplace diversity,
- language skills,
- staff complaints, and
- accommodation.

2.45 Information provided to the Committee regarding each agency's staffing arrangements was largely classified. Nevertheless, where possible, the human resource management of each agency is discussed below.

### Staffing demographics

2.46 ASIO advised that as at 30 June 2012, there were 60 Senior Executive Service (SES) officers, 500 Executive Level 1 and 2 officers, and 1 252 other officers within the organisation.[47]

2.47 As at 30 June 2013, there were 45 SES officers, 517 Executive Officers and 1 342 other officers.[48]

2.48 In addition to its organisational restructure, ASIO had reduced the number of SES officers by 25 per cent through a voluntary redundancy program. 15 SES officers left the organisation as a result of this program.[49]

---

46 ASD (Review No. 12), *Submission 5*, p. 4.

47 ASIO (Review No. 11), *Submission 7*, p. 29.

48 ASIO (Review No. 12), *Submission 7*, p. 25.

49 ASIO (Review No. 12), *Submission 7,* p. 28.

2.49 Within ONA, there were 156 staff members at 30 June 2012, including 59 staff at APS level 3-6 (there were no officers at APS levels 1-2), 74 Executive Level 1 and 2 officers, and 14 Band 1 and 2 SES officers.[50]

2.50 As at 30 June 2013, there were 153 staff members in ONA, comprising 85 males and 68 females. This included 60 staff between APS levels 1-6, 77 officers at Executive Level 1 and 2, and 13 Band 1 and 2 SES officers.[51]

2.51 ONA also reported changes to its staff numbers over the two reporting periods. In 2011-12, 35 new staff arrived and 28 left. In 2012-13, 16 new staff arrived and 21 left.[52]

## Recruitment

2.52 Agencies commented on the challenges faced in developing recruitment strategies that effectively target the technical specialists needed in their organisations. ASIO considered that the specialist requirements of its recruitment efforts required innovative ways to attract suitable applicants:

> These include more specific sourcing strategies that limit advertising, for example, to online media or specialised publications. Selection and assessment activities are better aligned to the specific skills and capabilities required for individual roles.[53]

2.53 The DIAs indicated that the staffing challenges they faced included attracting and recruiting people with the right skills. Agencies also face the challenge that many staff with specialist skills are highly sought by non-government organisations that are able to offer significantly higher salaries.[54]

2.54 Recruitment and organisational growth also continued to be affected by budget constraints in both the 2011-12 and 2012-13 financial years.

2.55 Some agencies reduced recruitment as a direct result of budget outcomes, or cited other reasons for the reduction, including competition in the market for specialists, or the need for candidates to satisfy rigorous security clearance requirements.

2.56 Other agencies reported a slight increase in new arrivals on previous years, although this was not the norm across the intelligence community.

2.57 In 2011-12, ASIO advised that despite deferring its overall staff growth, it would continue to recruit new intelligence professionals and technical

50 ONA (Review No. 11), *Submission 6*, p. 28.

51 ONA (Review No. 12), *Submission 6*, p. 26.

52 ONA (Review No. 11), *Submission 6*, p. 31; ONA (Review No. 12), *Submission 2*, p. 28.

53 ASIO (Review No. 11), *Submission 7*, p. 25.

54 *Classified transcript,* 15 May 2014, p. 28.

officers within budget allocations and increase the skill-set of existing officers to meet the challenges of Australia's security environment.[55]

2.58 During 2012-13, ASIO focussed on recruiting intelligence professionals, technical officers and security assessors, and strengthening its strategies to attract and develop entry-level staff and existing staff across the breadth of ASIO's activities.[56]

## Separation rates

2.59 The average separation rate across the APS for 2011-12 was 6.6 per cent.[57] In 2012-13, this rate decreased to 6.3 per cent.[58] Separation rates within the AIC varied between agencies and were affected by voluntary redundancy programs offered by some agencies.

2.60 ASIO reported that its separation rate had decreased from 5.8 per cent in 2010-11 to 4.7 per cent in 2011-12, increasing again in 2012-13 to 5.7 per cent as a result of voluntary redundancies.[59]

2.61 ONA's separation rate was 17.9 per cent in 2011-12, an increase of 0.9 per cent on the previous year. There was one retiree and 10 transfers to other APS agencies. 17 staff resigned or came to the end of their contracts.[60] ONA advised that it aimed to maintain a separation rate of around 18 per cent as:

> This level of turnover provides ONA with a balance of continuity and change and is an important factor in ONA's workforce planning and associated budgetary arrangements.[61]

2.62 ONA's separation rate for 2011-12 was affected by the loss of staff who had been engaged to provide security services on the 2 National Circuit building site prior to ONA's occupation.[62]

2.63 In 2012-13, ONA's separation rate was 13.8 per cent.[63]

2.64 There were varying trends regarding separation rates within the Defence Intelligence agencies over both reporting periods.[64]

---

55 ASIO (Review No. 11), *Submission 7,* p. 25.

56 ASIO (Review No. 12), *Submission 7*, p. 22.

57 Australian Public Service Commission, *State of the Service Report 2011-12*, p. 174.

58 Australian Public Service Commission, *State of the Service Report 2012-13*, p. 247.

59 ASIO (Review No. 11), *Submission 7*, p. 32; ASIO (Review No. 12) *Submission 7,* p. 28.

60 ONA (Review No. 11), *Submission 6*, p. 31.

61 ONA (Review No. 11), *Submission 6*, p. 31.

62 ONA (Review No. 12), *Submission 2*, p. 28.

63 ONA (Review No. 12), *Submission 2*, p. 28.

64 DIGO (AGO) (Review No. 11), *Submission 3,* pp. 17-19; DIO (Review No. 11) *Submission 4*, pp. 11-12; DSD (ASD) (Review No. 11), *Submission 5*, pp. 16-17; AGO (Review No. 12), *Submission*

2.65 Outside the reporting period, it was noted that separation rates had generally decreased, consistent with more recent trends across the APS.

## Retention strategies

2.66 Agencies are developing strategies to retain staff, including providing meaningful training opportunities and career pathways, and opportunities for flexible working arrangements, career diversity or specialisation.

2.67 In classified evidence all the DIAs reported on the various strategies employed to attract and retain staff.[65]

2.68 Other agencies reported on career management and employee mobility over the reporting periods, including the development of comprehensive leadership development frameworks and collaboration between agencies including joint recruitment and exchange programs to provide additional opportunities for staff.

## Training and development

2.69 All agencies reported on specific training and development activities undertaken during the reporting period.

2.70 Training and development included opportunities to expand skills, as well as mandatory training required to maintain core skills. Training was provided in the areas of:

- tradecraft,
- intelligence,
- corporate,
- leadership and management development, and
- language.

2.71 Training delivered over the reporting period included training targeted at new starters and ongoing staff, and management and leadership training for senior staff.

2.72 Agencies also outlined a number of shared training opportunities across the AIC, which aimed to foster a collaborative approach and mutual understanding of the role of each AIC agency. Training was conducted in tradecraft, leadership and operational development. Agencies also reported on continued staff engagement in training courses facilitated by

*3*, pp. 15-16; DIO (Review No. 12), *Submission 4*, pp. 12-13; ASD (Review No. 12), *Submission 5*, pp. 18-19.

65 DIGO (AGO) (Review No. 11), *Submission 3*, p. 20; DIO (Review No. 11), *Submission 4*, p. 10; DSD (ASD) (Review No. 11), *Submission 5*, pp. 15-16.

the National Intelligence Community's Training Secretariat and the National Security College.

## DIO

2.73 In 2011-12, DIO undertook significant development and review of its tradecraft training opportunities for staff. These developments included:

- consolidating its foundational tradecraft training program designed to build analysts' principal tradecraft skills,
- assessing its *Fundamentals of Intelligence Analysis* and *Military Analysis* courses to ensure they met the DIO mandate,
- using tradecraft instructors to facilitate *Structured Analytic Technique* sessions, and
- working with the Allied community on tradecraft training opportunities, including collaborating with the National Intelligence Community Training Secretariat to establish the *Denial and Deception Advanced Studies Program* in partnership with the US Office of National Intelligence and National Intelligence University.[66]

2.74 In 2013, DIO launched a pilot Continuing Professional Development program targeting EL1 and O5 staff, focussed on leadership, management and analytic tradecraft.[67]

2.75 In evidence to the Committee, the DIAs emphasised the high value placed on training within their organisations. Representatives pointed out that each agency has a training academy and that training is often delivered by expert staff within the organisation. In some cases during the reporting period, expenditure on training had increased.[68]

## ONA

2.76 ONA continued to offer a range of public service and specialist training opportunities to all staff, consistent with the APS Integrated Leadership System.[69] ONA provided approximately $410 000 in both 2011-12 and 2012-13 to learning and development, including studies assistance programs and language training.[70]

66 DIO (Review No. 11), *Submission 4*, p. 12.

67 DIO (Review No. 12), *Submission 4*, p. 14.

68 *Classified transcript*, 15 May 2014, p. 23.

69 ONA (Review No. 11), *Submission 6*, p. 35.

70 ONA (Review No. 11), *Submission 6*, p. 35; ONA (Review No. 12), *Submission 6*, p. 33.

2.77 In 2011-12, ONA stated that it had identified the competencies its analysts should possess and was establishing procedures to ensure new analysts were prepared with the appropriate suite of skills and techniques.[71]

2.78 Throughout 2011-12 and 2012-13, ONA participated in intelligence community training, including attending and presenting at National Security College courses. Most notably, ONA worked with the National Intelligence Open Source Committee to expand the delivery of open-source training for NIC members.[72]

## ASIO

2.79 A number of training and development programs took place in ASIO in both 2011-12 and 2012-13. In 2011-12, this included:

- a dedicated training unit offering specialist courses for ASIO's case officers and analysts,[73]
- programs to build management and leadership skills,[74]
- expansion of ASIO's Language Skills Development Program,[75]
- e-learning opportunities,[76]
- studies assistance,[77] and
- shared training opportunities across the AIC.[78]

2.80 ASIO offers specific training modules to officers as part of its intelligence training. In 2012-13, analytical and operational training was provided to officers on 51 occasions.[79]

2.81 In 2013, ASIO implemented a new Management and Leadership in Security Intelligence strategy aimed at officers at the AO5 to SES Band 2 level with a renewed focus on building and reinforcing fundamental management skills.[80]

2.82 ASIO explained that the strategy:

---

71 ONA (Review No. 11), *Submission 6*, p. 35.
72 ONA (Review No. 11), *Submission 6*, p. 35; ONA (Review No. 12), *Submission 6*, p. 33.
73 ASIO (Review No. 11), *Submission 7,* p. 26.
74 ASIO (Review No. 11), *Submission 7*, p. 27.
75 ASIO (Review No. 11), *Submission 7*, p. 27.
76 ASIO (Review No. 11), *Submission 7*, p. 27.
77 ASIO (Review No. 11), *Submission 7*, p. 27.
78 ASIO (Review No. 11), *Submission 7*, p. 27.
79 ASIO (Review No. 12), *Submission 7*, p. 22.
80 ASIO (Review No. 12), *Submission 7*, p. 23.

> … places value and emphasis on developing management and leadership skills, operational and investigative excellence, intellectual rigour and positioning ASIO for the future…[81]

### Committee comment

2.83 The Committee recognises the increasing focus on developing and delivering dedicated leadership development and management programs across the intelligence agencies. This was notable over the two reporting periods.

2.84 Agencies are also collaborating within the AIC and with Allied partners, to expand training and development opportunities for staff. The Committee welcomes this continued collaboration and the flow-on benefits of sharing skills and knowledge among the intelligence community.

2.85 The Committee notes that despite budget constraints, agencies have continued to prioritise training and development opportunities for staff. The Committee agrees that where intelligence agencies require staff with highly specialised skills and training, training and development should remain a high priority.

2.86 In discussions with the DIAs, the Committee expressed concern about the percentage of staff with outstanding mandatory training requirements. The Committee considers it is essential that mandatory training be completed within required timeframes.

## Workplace diversity

2.87 ONA advised that it continued to support the needs of people with disabilities, through inclusive staff selection procedures that reflect merit, fairness and freedom from discrimination. ONA advised:

> Reasonable accommodations to meet the needs of staff with disabilities or acquired injuries have included access to car parking; provision of an office; graduated return to work on reduced hours; and flexible work patterns.[82]

2.88 ASIO also advised that it endeavoured to build on the positive outcomes attainable by a workforce with varied skills, cultural perspectives and backgrounds.[83] ASIO submitted:

---

81 ASIO (Review No. 12), *Submission 7*, p. 23.

82 ONA (Review No. 11), *Submission 6*, p. 33.

83 ASIO (Review No. 11), *Submission 1*, p. 33.

> This is especially true in the security intelligence arena where understanding the intricacies of various cultures, societies and religions is crucial to understanding and addressing the broader security environment.[84]

### Gender

2.89 In 2012-13, 57.9 per cent of the APS workforce was female, compared with 57.6 per cent in 2011-12.[85] The proportion of women to men in the intelligence agencies, however, is lower that the APS average.

2.90 The proportion of women in the DIAs is particularly low, especially the proportion of female ADF personnel in these organisations. The percentage of women in two of the three DIAs increased slightly from 2011-12 to 2012-13, with the figure remaining the same in the third agency.[86]

2.91 Representatives of the DIAs told the Committee:

> … an area that has been a concern of ours for some time is simply the numbers of women within the workforce. It is below the numbers within the Department of Defence on a percentage basis. In essence, it is quite a number below … and we have a number of programs and approaches to try to lift the numbers of females joining the workforce.[87]

2.92 The Committee notes there has been some success to date.

2.93 Women comprised 44 per cent of ASIO's total workforce in both 2011-12 and 2012-13.

2.94 The proportion of females within ONA increased slightly over the two reporting periods, to approximately 44 per cent in 2012-13.[88]

## Staff feedback and complaints

2.95 Three agencies conducted staff surveys during 2011-2012, with another reporting on actions taken to implement a previous staff survey

---

84 ASIO (Review No. 12), *Submission 7*, p. 26.

85 Australian Public Service Commission, *State of the Service Report: State of the Service Series 2012-13*, p. 110; Australian Public Service Commission, *State of the Service Report: State of the Service Series 2011-12*, p. 246.

86 DIGO (AGO) (Review No. 11), *Submission 3*, p. 10; AGO (Review No. 12), *Submission 3*, pp. 7-8; DIO (Review No. 11), *Submission 4*, pp. 8-9; DIO (Review No. 12), *Submission 4*, pp. 9-10; DSD (ASD) (Review No. 11), *Submission 5*, p. 12; ASD (Review No. 12), *Submission 5*, p. 14.

87 *Classified transcript,* 15 May 2014, p. 15.

88 ONA (Review No. 11), *Submission 6*, p. 28; ONA (Review No. 12), *Submission 2*, p. 25.

2.96 ONA engaged independent consultants to conduct its staff survey in February 2012. ONA performed above the Australian government and Australian workforce averages on all survey categories.[89] ONA advised that it would develop an action plan to address the significant issues identified in the survey, including greater emphasis on career development, change management and employment security.[90]

2.97 2011-12 marked the first full year of ASIO's anti-bullying campaign, Silence Hurts. In May 2012, ASIO conducted an organisation-wide staff survey which included questions on working relationships. The survey noted a decrease in the number of staff reporting that they had been subject to harassment or bullying in the prior 12 months. ASIO reported that nine requests were made for support or assistance relating to workplace bullying or harassment.[91]

2.98 In its 2011-12 *Report to Parliament*, ASIO stated:

> In April 2012 ASIO conducted a staff survey to obtain workforce perceptions of, and levels of satisfaction with, a number of key people and cultural indicators. A strong and representative response rate of 72 per cent was achieved. As a consequence of implementing and delivering specific corporate and people management/development initiatives, ASIO has attained results indicating significant areas of improvement since the 2009 survey.[92]

2.99 Other results from the survey included:

- over 98 per cent of ASIO staff supported the organisation's mission,
- over 93 per cent of staff believed that the organisation had a clear set of values in relation to expected behaviours,
- over 89 per cent of staff felt they cooperated to get the job done, and
- over 89 per cent of staff reported they were innovative and were always looking for better ways of doing things.[93]

2.100 ASIO employs an external ombudsman or an ASIO Ombudsman. The Ombudsman acts as an independent arbiter (when external processes are exhausted) for staff who consider they have been treated unfairly.[94] ASIO reported that in 2011-12 the Ombudsman responded to a range of matters including workplace issues, transfer and employment opportunities, and

89 ONA (Review No. 11), *Submission 6*, p. 33.
90 ONA (Review No. 11), *Submission 6*, p. 34.
91 ASIO (Review No. 11), *Submission 7*, p. 32.
92 ASIO, *ASIO Report to Parliament 2011-2012,* p. 59.
93 ASIO, *ASIO Report to Parliament 2011-2012,* p. 59.
94 ASIO, *ASIO Report to Parliament 2011-2012,* p. 66.

conditions of employment.[95] The Ombudsman independently initiated formal reviews into two staff complaints over that period, with no formal complaints referred by the Director-General.[96]

2.101 ASIO undertook significant work to update its strategy for the professional conduct and behaviour of ASIO officers during 2012-13 in recognition of legislative amendments and the impending finalisation of *Safe Work Australia's draft Cost of Practice: Preventing and Responding to Workplace bullying*.[97]

2.102 In 2012-13, the Director-General formally referred seven complaints to the ASIO Ombudsman of which six were finalised during the reporting period.[98] A further two matters were referred, concerning reforms to ASIO's Values and Code of Conduct and a review of the scope of the Ombudsman role within the organisation.[99] The Ombudsman also responded informally to an additional 20 queries from ASIO officers, of which six complaints and 11 queries were in relation to bullying or harassment.[100]

2.103 Within ASD, there are several mechanisms employees can use to provide feedback on the work environment, including the Joint Staff Consultative Group, exit interviews, Director's suggestion box, and various organisational blogs.[101]

2.104 Staff are also able to use the following mechanisms:

- the Defence Alternative Resolution and Equity Directorate provides support and advice through mediation and conflict coaching, to assist with resolving complaints and grievances from Defence personnel,
- non-SES APS staff can 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, and
- the Defence Whistleblower Scheme, which receives and investigates complaints relating to misconduct within Defence, including criminal activity or unethical behaviour.[102]

95 ASIO (Review No. 11), *Submission 7*, p. 32.
96 ASIO, *ASIO Report to Parliament 2011-2012,* p. 66.
97 ASIO (Review No. 12), *Submission 7*, p. 28.
98 ASIO (Review No. 12), *Submission 7*, p. 28.
99 ASIO, *ASIO Report to Parliament 2012-2013,* p. 61.
100 ASIO (Review No. 12), *Submission 7*, p. 28.
101 DSD (ASD) (Review No. 11), *Submission 5*, p. 23.
102 DSD (ASD) (Review No. 11), *Submission 5*, p. 23.

2.105 No complaints were made through these mechanisms in 2011-12.[103] In 2012-13, there was one Review of Action application that was still to be finalised as at 30 June 2013.[104]

### Role of the Inspector-General of Intelligence and Security

2.106 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.[105] The IGIS does, however, investigate ASIO and ASIS related employment matters, and undertook a number of investigations in 2011-12 and 2012-13.[106]

2.107 The inquiries and findings of the IGIS over the reporting period are discussed later in this chapter.

### Committee comment

2.108 In its 2012-13 submission to the Committee, ASIO noted that regardless of a person's motives, the unauthorised disclosure(s) of sensitive information by a 'trusted insider' could significantly damage national security.[107]

2.109 Accordingly, the Committee considers that it is essential that intelligence agencies provide an environment in which staff complaints or concerns are investigated thoroughly, both internally and externally, and with independence if necessary.

2.110 The Committee notes that intelligence agencies have a number of mechanisms in place, including access to both internal and external review processes, for the investigation and review of staff complaints. External reviews may also be conducted by the IGIS.

2.111 The Committee is of the view that the mechanisms in place within the intelligence agencies are sufficient to ensure that both former and current staff have avenues for the robust review of their concern or grievance.

## Accommodation

### Relocation of ASIO's central office

2.112 ASIO's new central office, the Ben Chifley Building, is described as follows:

103 DSD (ASD) (Review No. 11), *Submission 5*, p. 23.

104 ASD (Review No. 12), *Submission 5,* p. 24.

105 See IGIS Act 1986, s. 8; IGIS (Review No. 11), *Submission* 9, p. 3; IGIS (Review No. 12), *Submission 8*, p. 2.

106 IGIS (Review No. 11), *Submission* 9, p. 3; IGIS (Review No. 12), *Submission 8*, p. 2.

107 ASIO (Review No. 12), *Submission 7.1*, pp. 11-12.

> … 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 40 000 square metres of net lettable area, accommodate up to 1 800 people and operate 24 hours per day.[108]

2.113 In the Committee's review of administration and expenditure for 2010-11, ASIO reported that construction of its new central office was progressing to allow the building to be handed over to ASIO in mid-2012, with the main relocation of ASIO staff to commence from late 2012.[109]

2.114 In 2011-12, ASIO reported that delays in construction had meant that the expected handover date had slipped, with ASIO expected to take possession of the building in mid-2013. ASIO also reported project overruns of $41.6 million during this period, which equated to seven per cent of the approved budget of $589.2 million set in 2008. ASIO's contribution to cost overruns was $24.3 million, which was being met within existing budgets.[110]

2.115 ASIO further explained the delays in construction in its 2011-12 *Report to Parliament*:

> The work program continued throughout 2011-12, with the majority of construction works scheduled for completion in late 2012. In May 2012, the project schedule was revised on advice from the Managing Contractor, resulting in the date from which ASIO is expected to take possession being adjusted from late 2012 to April 2013.[111]

2.116 ASIO argued:

> It is important to consider these budgetary pressures and scheduling delays in the context of the complexity and tenure of the project, given the approved budget and construction schedule was approved in 2008.[112]

2.117 In 2012-13, ASIO again submitted that delays in the commissioning and testing of essential building systems in the building had led to further

---

108 ASIO, *Ben Chifley Building*, <https://www.asio.gov.au/About-ASIO/Ben-Chifley-Building.html> viewed 4 March 2014.

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

110 ASIO (Review No. 11), *Submission 7*, p. 33.

111 ASIO, *ASIO Report to Parliament 2011-12*, p. 67.

112 ASIO (Review No. 11), *Submission 7*, p. 33.

slippages in the dates of handover. At the time of its submission, ASIO was scheduled to take possession of the building in May 2014.[113]

2.118 ASIO submitted:

> To the end of June 2013 the project has experienced overruns of $44 million, which equates to 7.5 per cent of the approved budget of the approved budget of $589 million set in 2008. ASIO's contribution to cost overruns is $24 million which has been met within existing budgets.[114]

2.119 The Ben Chifley Building was officially opened on 23 July 2013, when completion was expected to occur in August 2013. The opening was timed to enable greater access, including by media, to the ASIO building, prior to staff and technical equipment occupying the building.[115]

2.120 ASIO also reported that in June 2013, the Government agreed to accommodate the Australian Cyber Security Centre (ACSC) within the Ben Chifley Building. The design and construction of the ACSC was executed as a $14.6 million variation to the Ben Chifley Building project and it is expected to have an operational capability by late 2014.[116] This was reconfirmed when the Committee visited the building in March 2014.

## Relocation of ONA

2.121 Having previously been co-located with ASIO in Russell, ONA occupied its new premises, the Robert Marsden Hope Building in Barton in October 2011. The building is a heritage listed building, opened in 1941 as the Patents Office. ONA had worked with the building's landlord, Industry Superannuation Property Trust, to refurbish and modernise the building sympathetically since 2009.[117]

2.122 ONA said of the relocation:

> Relocating the Office of National Assessments from the Russell Precinct to the Parliamentary Triangle in October 2012 has broadened opportunities to build and expand relationships within Parliament House, and with ONA's broader client base. The Robert Marsden Hope building has been renovated, with ONA occupying a space that since 1941 has been at the heart of Australian government.[118]

---

113 ASIO (Review No. 12), *Submission 7*, p. 29.
114 ASIO (Review No. 12), *Submission 7*, p. 29.
115 ASIO (Review No. 12), *Submission 7*, p. 29.
116 ASIO (Review No. 12), *Submission 7*, p. 29.
117 ONA (Review No. 11), *Submission 6*, p. 20.
118 ONA (Review No. 11), *Submission 6*, p. 20.

2.123 In addition to its proximity to the Department of Prime Minister and Cabinet and other client agencies, ONA advised that it had designed the offices using an open plan layout to improve staff collaboration.[119]

2.124 2012-13 was the first full year of occupancy in the new building. ONA reported that during that time, a number of defects were rectified to comply with the tenancy agreement, with the last of these works completed in February 2013. The lease was formally executed in April 2013 and the Facilities Maintenance Agreement was executed in June 2013.[120]

## Security issues

2.125 The Committee's review of security matters included:

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

2.126 Much of the evidence on security matters was classified. Where possible, however, issues arising in the reporting period are discussed below.

### Security policy and training

2.127 Agencies recognise that they must have in place a strong security culture, to ensure their organisation is able to carry out its objectives, without compromising its people, premises and information.[121] Agencies' security policies and practices must also comply with the Australian Government's Protective Security Policy Framework (PSPF).[122]

#### ONA

2.128 ONA reported on its ongoing goal of maintaining and fostering a strong security culture in areas such as personnel, physical and information technology security.[123]

---

119 ONA (Review No. 11), *Submission 6*, pp. 20-21.

120 ONA (Review No. 12), *Submission 2*, p. 20.

121 See, for example, ASIO (Review No. 12), *Submission 7*, p. 33.

122 ASIO (Review No. 12), *Submission 7*, p. 33.

123 ONA (Review No. 11), *Submission 6*, p. 38.

2.129 ONA explained the importance of effective security arrangements:

> ONA's assessment, foreign liaison and coordination functions and reputation require and rely on robust and effective security arrangements. These are aimed at preventing accidental or deliberate compromise of classified information including that provided by the AIC, allies and other intelligence partners.[124]

2.130 ONA also outlined the high level of security awareness required by staff:

> ONA staff, as a condition of employment, must maintain a very high level of security awareness and report significant changes to their personal circumstances. Strong executive leadership, staff awareness, clear policies and procedures and application of risk assessment and security incident management frameworks supported ONA's security culture.[125]

2.131 In addition to holding regular internal staff training and briefings in the reporting period, ONA participated in inter-agency security forums and committees, not only within the AIC, but also across wider government.[126]

2.132 ONA reported that it had partially implemented the new Australian Government Security Classification Scheme during 2012-13. It also completed IT system updates with the new classifications in 2012-13 and expected another update in 2013-14.[127]

2.133 ONA held security awareness presentations on insider threats for staff. Staff training also included practical tools to assist in the mitigation of phishing and management of staff members' on-line presence.[128]

## ASIO

2.134 ASIO submitted that a strong security culture underpinned its ability to carry out its mission to protect Australia, its people and its interests, stating that:

> This requires strong security policies, practices and technologies. These standards serve to protect the Organisation's people, premises and information from compromise and ensure ASIO can carry out its mission. Without strong security practice, sensitive information could be accessed by those who wish to do Australia

124 ONA (Review No. 12), *Submission 2*, p. 36.
125 ONA (Review No. 12), *Submission 2*, p. 36.
126 ONA (Review No. 11), *Submission* 6, p. 38; ONA (Review No. 12), *Submission 2*, p. 36.
127 ONA (Review No. 12), *Submission 2*, p. 36.
128 ONA (Review No. 11), *Submission 6*, p. 38.

> harm, and allied partners and members of the public would be less willing to communicate information to ASIO.[129]

2.135 2011-12 marked the first full year of ASIO operating within the Government's new PSPF, and saw revision of the Sensitive Material Security Management Protocol. This protocol provides detailed policy guidance for agencies operating in a Top Secret environment.[130]

2.136 During 2012-13, ASIO established the Counter Intelligence and Security Review Committee (CISRC) to provide guidance and direction in respect of security policy for the organisation. The CISRC is chaired by the Director-General and is attended by both Deputy Directors-General and other ASIO senior executive officers.[131]

2.137 The ASIO Security Committee, which previously oversaw ASIO's security, now operates as a subcommittee of the CISRC and comprises SES-level representatives who provide advice and recommendations to the CISRC for consideration and action.[132]

## Security clearances

2.138 Personnel across the AIC are required to secure and maintain an appropriate security clearance in order to perform their roles. Agencies told the Committee that the processes for obtaining and revalidating security clearances are time consuming, with some agencies experiencing high caseloads. The Committee recognises that agencies are continually seeking to improve the efficiency of these processes while also maintaining the standards required by the Government.

2.139 The Committee also heard that agencies are working together to either recognise clearances under a reciprocal arrangement, or to adopt common vetting practices.

2.140 In evidence to the Committee, it was noted that some delays in the vetting process were out of the control of the agencies, as timely vetting remained reliant on a number of factors, including the responsiveness and availability of the applicant and/or their referees.

---

129 ASIO (Review No. 12), *Submission 7*, p. 33.

130 ASIO (Review No. 11), *Submission 7*, p. 37.

131 ASIO (Review No. 12), *Submission 7*, p. 33.

132 ASIO (Review No. 12), *Submission 7*, p. 33.

### ASIO

2.141 ASIO advised that all ASIO staff were required to participate in security awareness education at the outset of employment, and at regular intervals thereafter, to ensure they are aware of their obligations.[133]

2.142 ASIO also conducts a comprehensive program of revalidation and re-evaluation of staff members' clearances to ensure that staff remained suitable to access highly classified information. This process includes a review of a person's circumstances, including financial, personal and psychological factors.[134]

2.143 In 2012-13, ASIO reported on the pressures involved in vetting processes:

> Pressures on ASIO's initial vetting and revalidation continued over the reporting period. It is a time consuming process and ASIO is constantly seeking ways to become more efficient in security vetting, without compromising the high standards the government rightly places on ASIO security practices.[135]

### ONA

2.144 ONA confirmed that its security team worked closely with other vetting agencies to develop best practice for the ongoing management of clearance holders against a robust framework.[136]

2.145 ONA advised that it continually reviewed its personnel security vetting procedures to ensure a rigorous process was maintained, enhancing internal systems where necessary to increase the efficiency of the process and to improve security analysis tools and capability.[137]

## Security breaches

2.146 Agencies have in place a number of internal security policies to ensure best practice in relation to security matters, including procedures for the reporting of security breaches within the organisation.

2.147 The reporting of security breaches relates to unintentional or accidental failure to observe the protective security mandatory requirements.[138]

---

133 ASIO (Review No. 11), *Submission 1*, p. 38.

134 ASIO (Review No. 11), *Submission 1*, p. 38.

135 ASIO (Review No. 12), *Submission 7*, p. 33.

136 ONA (Review No. 11), *Submission 6*, p. 38.

137 ONA (Review No. 11), *Submission 6*, p. 38; ONA (Review No. 12), *Submission 2*, p. 37.

138 ASIO (Review No. 11), *Submission 7*, p. 38.

2.148 Each agency reported information to the Committee on any physical or electronic security incidents identified over the reporting periods. Agencies also reported on any actions or risk mitigation measures (both internal and external) put in place to mitigate or prevent future compromises to security within the organisation, regardless of whether a breach or incident was accidental or unintentional.

2.149 The Committee discussed with the relevant intelligence agency a significant security incident that occurred during the reporting period. The Committee was satisfied that the recommendations arising from reviews in response to the incident were being implemented.

2.150 The Committee also discussed with agencies the response of the AIC to disclosures by former National Security Agency contractor Edward Snowden.

## ONA

2.151 ONA reported an increase in security breaches over the reporting period and enhanced efforts to foster a stronger security culture in the areas of personnel, physical and information technology security.[139]

2.152 ONA considered that its relocation to the new building during 2011-12 provided a practical and efficient balance between security controls and day-to-day operational requirements:

> This facility has enabled ONA to work effectively and securely with minimal overhead in the provision of high assurance security services to facilitate the classified work of ONA as well as a comfortable, secure venue for engagement with high level Australian and international visitors.[140]

## ASIO

2.153 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.[141]

2.154 ASIO reported that its senior executive was briefed on security breaches occurring within their divisions and branches in a timely fashion, to enable proactive management of each occurrence.[142]

---

139 ONA (Review No. 11), *Submission 6*, p. 39; ONA (Review No. 12), *Submission 2,* p. 37; ONA (Review No. 12), *Submission 2.1,* p. 2.

140 ONA (Review No. 11), *Submission 6*, p. 38.

141 ASIO (Review No. 12), *Submission 7*, p. 33.

142 ASIO (Review No. 11), *Submission 7*, p. 38.

2.155 ASIO noted that multiple breaches by the same individual within a 12 month period attracted more significant consequences, from formal counselling to misconduct sanctions. Security breach history could also be taken into account when an officer was being considered for a promotion or posting.[143]

## E-security arrangements and enhancements

2.156 During both reporting periods, cyber-espionage remained a key concern within the intelligence community.[144]

2.157 ASIO submitted that it had implemented significant e-security arrangements to ensure its high value targets were protected, and that all ICT systems were designed, installed, maintained and operated within acceptable security risk boundaries.[145] In 2012-13, ASIO submitted:

> 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 information communication technology (ICT) systems to ensure vulnerabilities are avoided where possible and remedied when needed.[146]

2.158 In addition to enhancing its own systems, ASIO provided advice to government and entities in the private sector to assist them mitigate threats posed by cyber intrusions. [147]

2.159 ONA reported that it continually reviewed its systems, both internally and externally, to ensure e-security remained appropriate. These reviews led to improved functionality in the detection of phishing e-mails with malicious payload, and an increase in staff awareness of the risks associated with internet-based phishing e-mails.[148]

2.160 ONA advised that all its IT-related projects were reviewed to ensure the project would not compromise ONA's security arrangements or effect accreditation of ONA systems.[149]

2.161 Agencies also referred to the personal use of technology, the internet and social media by officers. Agencies reported on the outcome of staff surveys in this regard, and training opportunities offered to staff to raise

143 ASIO (Review No. 12), *Submission 7*, p. 33.
144 ASIO (Review No. 11), *Submission 7*, p. 13.
145 ASIO (Review No. 11), *Submission 7*, p. 38.
146 ASIO (Review No. 12), *Submission 7*, p. 33.
147 ASIO (Review No. 11), *Submission 7*, p. 38.
148 ONA (Review No. 11), *Submission 6*, p. 40.
149 ONA (Review No. 11), *Submission 6*, p. 40; ONA (Review No. 12), *Submission 2*, p. 38.

awareness of potential security issues arising from the personal use of social media and other technology.

## Public accountability and performance management

2.162 There are numerous internal and external accountability mechanisms in place for each of the intelligence agencies to provide assurance to the Australian public of the legality and propriety of agency activities. These mechanisms include:

- internal reviews,
- Ministerial and Parliamentary accountability, and
- the Inspector-General of Intelligence and Security.[150]

2.163 The Committee sought submissions from the Inspector-General of Intelligence and Security (IGIS)[151] on any issues of administration and expenditure arising during IGIS's inspection and inquiry activities in the reporting period. The IGIS also appeared before the Committee.

2.164 For 2011-12 and 2012-13, the IGIS raised two common issues relating to the administration of the intelligence agencies:

- recordkeeping, and
- personnel, recruitment and vetting in the AIC.[152]

2.165 The IGIS also raised the following specific issues:

- in 2011-12, communication between ASIO and DIAC,[153] and
- in 2012-13, delays and administrative deficiencies.[154]

### Recordkeeping

2.166 The IGIS stressed the importance of making and keeping appropriate records of intelligence and security related decisions, even where those decisions are not reviewable by the courts:

---

150 See, for example, ASIO (Review No. 12), *Submission 7*, p. 34.

151 The IGIS is an independent statutory office holder who reviews the activities of the AIC, to ensure that agencies act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights. The functions of the Inspector-General are prescribed under sections 8, 9 and 9A of the *Inspector-General of Intelligence and Security Act 1986*. IGIS, *Roles and Functions of the Inspector-General,* <http://www.igis.gov.au/about/index.cfm>, viewed 22 May 2014. See also, IGIS (Review No. 11), *Submission 9*, p. 5; IGIS (Review No. 12), *Submission 8*, p. 4.

152 IGIS (Review No. 11), *Submission 9*; IGIS (Review No. 12), *Submission 8*.

153 IGIS (Review No. 11), *Submission 9*, pp. 2-3.

154 IGIS (Review No. 12), *Submission 8*, p. 2.

> I am well aware that some decisions need to be made quickly and that the tempo of intelligence and security work is often rapid. However, this does not make recordkeeping discretionary. Records of important meetings and decisions, even brief records, still need to be made and retained.[155]

2.167 In 2011-12, the IGIS found some deficiencies in ASIO's decision-making processes (which were subsequently addressed by ASIO), including:

- the decision-making pathway for some community detention determinations was unclear,
- there were a number of cases where the Attorney-General was not notified 'forthwith' that the grounds for a warrant had ceased as required by the legislation (although ASIO was found to have promptly ceased intelligence collection in these cases), and
- some records relating to internal approvals for the initiation of investigations and requests for access to telecommunications and financial data were found to be lacking in detail and poorly expressed.[156]

2.168 The Committee was informed that more recent inspections conducted by the office of the IGIS have noted marked improvements in ASIO's record keeping.[157]

2.169 In 2012-13, the IGIS conducted an inquiry into the analytic independence of ASIO, DIO and ONA. Despite overall positive findings, inconsistent recordkeeping and source referencing practices within ASIO and DIO were identified. The IGIS considered this made it difficult for the agencies to demonstrate a lack of bias and interference in the assessments.[158] ONA confirmed that the IGIS had found that the analytical independence of ONA (and the two other agencies) had been preserved.[159]

2.170 The IGIS advised that DIO was due to implement a new electronic intelligence production system in July 2013 which would offer a significant improvement in recordkeeping. The IGIS has undertaken subsequently follow up reviews with DIO.[160] ASIO had developed a new policy for referencing and improved electronic records systems in response to the inquiry.[161]

---

155 IGIS (Review No. 11), *Submission 9*, p. 1.
156 IGIS (Review No. 11), *Submission 9*, pp. 1-2.
157 *Classified transcript,* 15 May 2014, p. 4.
158 IGIS (Review No. 12), *Submission 8*, p. 1
159 ONA (Review No. 12), *Submission 2*, p. 13.
160 *Classified transcript,* 15 May 2014, p. 6.
161 IGIS (Review No. 12), *Submission 8*, p. 1

2.171 ASIO reported that it had accepted all recommendations made in regard to ASIO's recordkeeping, source referencing, key judgements review and dissent management.[162]

## Personnel, recruitment and vetting in the AIC

2.172 In 2011-12, the IGIS conducted an inquiry into a complaint about a particular recruitment action in ASIS. The IGIS found that the normal business practices relating to recruitment were sound. However, these practices had not been followed in this case. ASIS accepted all recommendations made about policies, procedures and training for staff involved in recruitment.[163]

2.173 IGIS also conducted a preliminary inquiry into a decision made by ASIO to terminate a person's employment. In this case, IGIS found that the processes and decisions made were not inappropriate. However, IGIS had concerns about the timeliness of ASIO's internal investigation. ASIO advised the IGIS of changes to internal policies and practices made in response to this inquiry.[164]

2.174 At the request of the Minister for Defence, the IGIS conducted an inquiry into the mechanisms and processes for managing risk in DIAs in circumstances where a staff member is identified as being an actual or potential security concern. The IGIS was also asked to compare the activities of DIAs with the mechanisms and processes being used by the other agencies of the AIC.[165]

2.175 The IGIS found areas where agencies could better manage security risks and information sharing and identified better practice principles to strengthen existing arrangements within and across the AIC agencies.[166]

2.176 Although not within the scope of the inquiry, the IGIS also provided suggestions to ASIO, ASIS and ONA on the better practice principles articulated in her report, which resulted in some processes being amended.[167]

2.177 In 2012-13, the IGIS investigated ASIO's handling of a withdrawal of an officer's security clearance. Here the IGIS found that the withdrawal was

162 ASIO (Review No. 12), *Submission 7*, p. 36.

163 IGIS (Review No. 11), *Submission 9*, p. 3.

164 IGIS (Review No. 11), *Submission 9*, p. 3.

165 IGIS (Review No. 11), *Submission 9*, p. 3.

166 IGIS (Review No. 11), *Submission 9*, pp. 3-4; *Classified transcript,* 15 May 2014, p. 5.

167 IGIS (Review No. 11), *Submission 9*, p. 4.

not inappropriate, but made three recommendations about ASIO's staff management processes.[168]

## Inquiries into processes for visa security assessments

2.178 The IGIS advised that in 2011-12 the IGIS received 430 complaints about visa security assessments, most of which concerned delays. This number had decreased from 1 111 received in 2010-11.[169]

2.179 In her submission to the Committee for 2010-11, the IGIS outlined the reasons why she thought the office had continued to received large numbers of complaints about the timeliness of security assessments for visa applicants:

> As the number of visa applicants referred to ASIO for a security assessment has trended upwards in recent years backlogs develop. This is particularly so for complex cases.
>
> Another reason is that the role and functions of the IGIS have become better known amongst particular groups who have resettled in Australia, and amongst migration agents and refugee advocates.[170]

2.180 The IGIS attributed a stabilisation and then relative decline in the number of complaints made in the last quarter of 2010-11 to the implementation of a triaging approach by the then Department of Immigration and Citizenship (DIAC) (in collaboration with ASIO) to security assessments for visa applicants who meet the criteria for refugee status.[171]

2.181 The IGIS had also determined that an inquiry would not be conducted where the application had been made less than 12 months previously.[172]

2.182 For 2011-12, the IGIS outlined several matters, noting also her concerns about coordination and communication between ASIO and DIAC:

- A visa security assessment had been cancelled due to a handling error, however, upon being discovered, the assessment was finalised and a formal apology issued to the complainant.
- DIAC had sent 43 referrals to ASIO to the wrong electronic mailbox and five of these were more than 12 months old. ASIO took action by prioritising these cases and making changes to minimise the risk of recurrence.

168 IGIS (Review No. 12), *Submission 8*, p. 2.
169 IGIS (Review No. 11), *Submission 9*, p. 2.
170 IGIS (Review No. 10), *Submission 1*, p. 2.
171 IGIS (Review No. 10), *Submission 1*, p. 2.
172 *Classified transcript*, 15 May 2014, p. 1.

- A number of incomplete assessments were identified which pre-dated the DIAC-ASIO electronic referral system. ASIO took steps to finalise these.[173]

2.183 The IGIS recommended that ASIO engage in dialogue with DIAC so that in cases where ASIO has issued an adverse assessment but DIAC has identified significant health, welfare and other exceptional issues, the Minister for Immigration and Citizenship could be advised on possible risk mitigation strategies and conditions with which a person might be placed in community detention.[174]

2.184 The Inspector-General noted that this proposal had not been pursued by ASIO. The IGIS stated:

> I am also aware that other recent events, such as the appointment of an Independent Reviewer to review the appropriateness of adverse security assessments may have overtaken my earlier recommendation.[175]

2.185 ASIO outlined its response to the IGIS recommendations in its submission for 2011-12:

> ASIO agreed to two recommendations, pertaining to recording decision-making processes and the maintenance of ASIO's policy and training documentation for interviews, particularly with regard to mental health considerations. The remaining recommendation, of ASIO providing risk mitigation advice to DIAC should DIAC allow a person subject to an ASA into community detention, was considered by ASIO. However, ASIO considers this to be outside its current remit and might have unintended consequences.[176]

2.186 On 27 March 2013, the IGIS initiated an inquiry into the attendance of legal representatives at ASIO security assessment interviews. This report was published outside the reporting period in January 2014. ASIO commented however that it had accepted four of the IGIS' five recommendations and partially accepted one recommendation.[177]

2.187 On 5 June 2013, the then Prime Minister requested the IGIS to conduct an inquiry into the management by Australian agencies of people seeking

173 IGIS (Review No. 11), *Submission 9*, pp. 2-3.

174 IGIS (Review No. 11), *Submission 9*, p. 3.

175 IGIS (Review No. 11), *Submission 9*, p. 3.

176 ASIO (Review No. 11), *Submission 7*, p. 42.

177 ASIO (Review No. 12), *Submission 7*, p. 36. See also, IGIS, *Inquiry into the attendance of legal representatives at ASIO intervies, and related matters*, <http://www.igis.gov.au/inquiries/docs/legal_representatives_ASIO_Jan2014.pdf>, viewed 22 May 2014.

asylum who present complex security issues. Although the report had not been released at the time submissions were made to this Committee, ASIO reported that it had begun to implement reforms in this area in January 2013, in advance of the inquiry commencing.[178]

## Delay and administrative deficiencies

2.188 In 2012-13, the Inspector-General raised a number of issues in relation to the administration of ASIS, including:

- Concern about lapses of proper administration demonstrated by senior management in reviewing an anonymous complaint about a lack of action by ASIS management into a number of allegations of misconduct. The IGIS noted that under the new public interest disclosure scheme, ASIS would have had three months from the time the allegations were made to finalise its investigation.
- Delays in promptly informing the Minister for Foreign Affairs when the grounds for a ministerial authorisation had ceased to exist. The IGIS indicated she was satisfied that new processes implemented in 2012-13 had addressed this matter.
- Deficiencies in some of ASIS's obligations under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act), and its administrative processes in the management of AUSTRAC material. ASIS advised that it had updated its procedures to comply with the legislation.[179]

2.189 In relation to ASIO, IGIS raised the following:

- There were a relatively small number of errors relating to the execution of ASIO warrants, including typographical errors and identification of an incorrect service. In these cases, appropriate remedial action was taken.
- ASIO was generally compliant with AML/CTF Act obligations, but did not comply with AUSTRAC's guidelines on storage. In response, ASIO obtained a waiver from AUSTRAC for storage requirements.[180]

2.190 In January 2011, the IGIS announced an inquiry into the actions of Australian government agencies in relation to the arrest and detention overseas of Mr Mamdouh Habib from 2001 to 2005.[181] An unclassified version of this report was released in March 2012.[182]

178 ASIO (Review No. 12), *Submission 7*, p. 36.

179 IGIS (Review No. 12), *Submission 8*, p. 2.

180 IGIS (Review No. 12), *Submission 8*, p. 2.

181 ASIO (Review No. 11), *Submission 7*, p. 42.

182 See IGIS, *Public Reports*, <http://www.igis.gov.au/inquiries/index.cfm>.

2.191 ASIO accepted all of the IGIS's recommendations relevant to its policies and procedures, including engagement with and provision of information to foreign authorities.[183]

# Additional developments in reporting period

## Independent Reviewer of Adverse Security Assessments

2.192 On 3 December 2012, the Hon Margaret Stone commenced as the Independent Reviewer of Adverse Security Assessments (the Independent Reviewer). [184]

2.193 The Independent Reviewer was appointed to conduct an independent advisory review of ASIO adverse security assessments made in relation to individuals in immigration detention.[185]

2.194 In performing her role, the Independent Reviewer is required to examine all material relied on by ASIO in making the assessment. ASIO reported that it provided the Independent Reviewer with the information it had relied on in making the adverse security assessments for all eligible persons.[186]

2.195 During 2012-13, ASIO advised that the Independent Reviewer released findings on five assessments issued by ASIO, finding that three of these remained appropriate and two were not. ASIO undertook new assessments of these two cases, resulting in the Director-General issuing non-prejudicial security assessments in relation to both individuals.[187]

## Independent Review of the Intelligence Community

2.196 During 2011-2012, the Independent Review of the Intelligence Community was completed by Mr Robert Cornall AO and Dr Rufus Black. The findings of the Review were presented to the Australian Government in July 2011.[188] This was the first comprehensive review of the AIC since the 2004 inquiry conducted by Mr Phillip Flood AO.[189]

---

183 ASIO (Review No. 11), *Submission 7*, p. 42.

184 ASIO (Review No. 12), *Submission 7*, p. 36.

185 ASIO (Review No. 12), *Submission 7*, p. 36.

186 ASIO (Review No. 12), *Submission 7*, p. 37.

187 ASIO (Review No. 12), *Submission 7*, p. 37.

188 Commonwealth of Australia, 2011 Independent Review of the Intelligence Community Report, Robert Cornall AO, Dr Rufus Black, 2011.

189 Commonwealth of Australia, *Report of the inquiry into Australian intelligence agencies*, Phillip Flood AO, 2004.

2.197 The overall conclusions reached by the Review were:

- The intelligence community has grown substantially over the last ten years in response to increasing demand, mainly in relation to terrorism, fighting wars and countering espionage (including cyber attacks), proliferation of weapons of mass destruction and people smuggling,
- The investment made in building up the intelligence agencies has been justified and rewarded with more capability and increased performance,
- That capability and performance has enabled Australia's agencies to make an effective contribution as a member of the international intelligence partnerships,
- The investment made in the intelligence agencies has resulted in improved capability and performance in Australia, and has also gained Australia access to intelligence from international partners,
- The intelligence agencies are working well together,
- The intelligence agencies are also beginning to work more effectively with the other members of the recently expanded National Security Community, and
- The principal new challenges for the next five years or so will be to better align the AIC's priorities with the new geo-political and technological realities facing Australia as a middle power with global interests.[190]

## Public relations

2.198 Where possible, agencies have endeavoured to engage with the public through their unclassified public websites and/or public statements and speeches made via their Director or Director-General.

2.199 Significantly, on 19 July 2012, the Director-General of ASIS, Mr Nick Warner AO PSM, gave the first ever public speech about ASIS as part of the Lowy Institute's Distinguished Speakers series. This public address concerned the role and nature of the organisation. [191]

2.200 The significance of this public speech was explained by Mr Warner in the speech itself:

190 Commonwealth of Australia, 2011 Independent Review of the Intelligence Community Report, Robert Cornall AO, Dr Rufus Black, 2011.

191 ASIS, *ASIS at 60*, <http://www.asis.gov.au/about-us/speech.html>, viewed on 23 May 2014.

> Conceived in secrecy, the Australian Secret Intelligence Service has, unsurprisingly, spent the last 60 years operating in carefully cultivated shadows. Over that time no Director-General of ASIS has, until today, made a public address concerning the role of nature of the organisation.[192]

2.201 In 2011-12, AGO launched an updated and revised unclassified website. AGO explained:

> The new site layout clearly explains [AGO]'s role and functions, highlights career opportunities, and includes examples of releasable product types … The site was launched in time to support the 2013 I&S Group graduate recruitment campaign.[193]

2.202 Over the reporting period, ASD published a number of articles in the public domain relating to ICT security issues. This included the release of the revised *2012 Australian Government Information Security Manual* (ISM), which governs the security of government ICT systems. ASD commented on the substantial changes made to this manual:

> This change has made the ISM accessible to more users across government, helping to better promote information security awareness.[194]

2.203 In 2011-12, ASD expanded the scope of material published on its public website, to assist agencies in improving the security of government ICT systems.[195]

2.204 Additionally, ASD issued a media release about its world first certification of the Apple iOS5 operating system for use within government, in response to significant media interest.[196]

## Requests for access to public records

2.205 Agencies also 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.

2.206 In 2011-12, in response to a 2011 Administrative Appeals Tribunal decision, DIO processed two high-priority applications for access to information held in DIO archives. DIO also reviewed two draft volumes of the *Official History of Australian Peacekeeping, Humanitarian and Post Cold-War Operations,* for which the authors had been granted extraordinary

192 ASIS, *ASIS at 60*, <http://www.asis.gov.au/about-us/speech.html>, viewed on 23 May 2014.

193 DIGO (AGO) (Review No. 11), *Submission 3*, p. 32.

194 DSD (ASD) (Review No. 11), *Submission 5*, p. 30.

195 DSD (ASD) (Review No. 11), *Submission 5*, p. 30.

196 DSD (ASD) (Review No. 11), *Submission 5*, p. 31.

access to classified information.[197] In 2012-13, Volume 3 of this work was reviewed.[198]

2.207 DIO stated that 74 new requests were received in 2011-12, with 30 outstanding as at June 2012.[199] In 2012-13, 100 new requests were received, with 121 processed, leaving nine to be finalised as at June 2013. DIO noted that improved administrative processes had resulted in reduced processing times and the elimination of backlogs.[200]

2.208 DSD received 12 requests in 2011-12 and 19 requests in 2012-13.[201] There were no requests for access to DIGO records in 2011-12 and one request in 2012-13.[202] Other AIC agencies also processed requests for access to records.[203]

2.209 ASD noted developments in a case involving an individual who had made a series of requests to the National Archives of Australia under the *Archives Act* 1983 for the release of documents containing substantial amounts of classified signals material. In 2011-12, ASD was consulted on the review of a decision to refuse access to nine records containing partial exemption claims. The decision to protect sensitive information was upheld in this case.[204]

2.210 The Committee was informed that the number of requests for public access to records is increasing:

> There is no question that we are seeing an increase in the number of requests, and the change from 30 years to 20 years brings a lot more material into the open period than was previously the case. So there is growing pressure in terms of access requests.[205]

2.211 Additionally, for a small number of senior officers, an increasing amount of time is being spent on these matters. The necessity for the IGIS or head of an agency to appear before the Administrative Appeals Tribunal (AAT) was described as particularly time consuming. Some agencies highlighted that, in addition to the time spent at the AAT, substantial preparation and assessment of archival materials was required prior to their appearance.

---

197 DIO (Review No. 11), *Submission 4*, p. 21.

198 DIO (Review No. 12), *Submission 4*, p. 21.

199 DIO (Review No. 11), *Submission 4*, p. 21.

200 DIO (Review No. 12), *Submission 4*, p. 21.

201 DSD (ASD) (Review No. 11), *Submission 5*, p. 29; ASD (Review No. 12), *Submission 5*, p. 30.

202 DIGO (AGO) (Review No. 11), *Submission 3*, p. 3; AGO (Review No. 12), *Submission 3*, p. 26.

203 ASIS (Review No. 11), *Submission 2*, p. 29; ASIS (Review No. 12), *Submission 6*, p. 30; ONA (Review No. 11), *Submission 6*, p. 23; ONA (Review No. 12), *Submission 2*, p. 23.

204 DSD (ASD) (Review No. 11), *Submission 5*, p. 29.

205 *Classified transcript,* 16 May 2014, p. 11.

Matters were also sometimes discontinued after all the preparatory work had been completed.[206]

2.212 Some agencies expressed concern about the resource implications associated with this matter. One agency head expressed the view that the level of resources required would increase over time, particularly where cases may be appealed to a higher court.[207]

### Committee comment

2.213 The Committee notes the concerns raised by agencies and will continue to monitor this issue.

## Concluding comments

2.214 The Committee has conducted a thorough review of the administration of the six intelligence agencies for the 2011-12 and 2012-13 financial years and is satisfied that agencies are overseeing their administrative functions effectively within the constraints posed by the current budgetary environment.

2.215 Agencies are managing reduced staffing numbers within this environment. Agencies also continue to address the challenges faced in recruiting the technical specialists needed in their organisations as well as developing effective strategies to retain and develop existing staff.

2.216 Despite budgetary constraints, 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.

2.217 As noted earlier, the Committee is concerned by aspects of the mandatory security training regime within the DIAs. The Committee considers that proper security training is a fundamental step toward limiting the number of security incidents.

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

206 *Classified transcript,* 15 May 2014, p. 10; *Classified transcript,* 16 May 2014, p. 24.

207 *Classified transcript,* 16 May 2014, p. 24. See also ASIS (Review No. 12), *Submission 6.1,* p. 2; ONA (Review No. 11), *Submission 6,* p. 23.

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