# 2

# Administration

2.1     This is the second full review of administration and expenditure of the six intelligence agencies carried out by the Committee of the 43rd Parliament. The Committee looked at all aspects of the administration of the agencies including human resource management, organisational structure, security clearances and breaches, accommodation issues, workforce diversity and growth management.

2.2     This chapter reports broadly on the areas discussed during hearings and/or in submissions relating to the administration of the six agencies within the Australian Intelligence Community (AIC). During private hearings and from the submissions, the Committee took a substantial amount of classified information which cannot be included in this report. However, the following discussion outlines the evidence without including any classified information.

## Organisation of agency structure

2.3     Three of the agencies reported changes to their organisational structures during 2010-11. The Committee notes that a majority of the six intelligence agencies restructured in 2007-08.

2.4     ASIO explains changes to its reporting structure as follows:

> During the reporting period, ASIO's new ten division structure was implemented. This was designed to better allocate resources, aligning skills and work group functions to enhance organisational performance and interconnectivity across divisions. The ASIO Senior Management group continues to review ASIO's structure to ensure the most appropriate allocation of resources

and matching of skills to duties, with a focus on ensuring ASIO's structure maintains sufficient fluidity to respond rapidly to any emerging thematic issues of security concern.[1]

2.5     At the public hearing the Director-General of ASIO, Mr David Irvine, told the Committee about ASIO's internal reform program:

> The point of this reform program is not simply to meet the demand for efficiency dividends and so on; it is to address what I think is a key responsibility of anyone in a position of leadership within the intelligence community today, and that is to make sure that the intelligence community is prepared for tomorrow. We regard our organisation as a national capability which we have to keep developing in terms of the skill sets but also in terms of the technology and the tradecraft that are required of a modern security intelligence organisation.[2]

2.6     One agency introduced a new and expanded organisational structure to ensure appropriate focus and risk management across all aspects of that agency's expansion in operational activities.

2.7     One agency combined two areas of its responsibilities into one so as to better focus on challenges in the current geo-political environment.

2.8     The Defence Imagery and Geospatial Organisation (DIGO)  also submitted to the Committee that it conducted a review of its Corporate Services Directorate which:

>  . . .led to a change in role and is now called the DIGO Business Sustainment Directorate. The Directorate now oversees business continuity planning, information technology and sustainment planning, manages DIGO's emergency control organisation and controls DIGO's registry, records management and safehand functions.[3]

2.9     DIGO also established the Strategic Capability Directorate to examine the need for, and user requirements of, an Australian Defence remote sensing satellite; and management of organisational strategic planning, including the DIGO Strategic Plan and the DIGO Business Plan.

---

1    *ASIO Unclassified Submission*, No. 2, p. 31.

2    *Classified Transcript*, 23 March 2012, p. 1.

3    *DIGO Classified Submission*, No. 5, p. 7.

# Impact on agencies of recent legislative changes

2.10    Out of the six agencies, four reported having to accommodate legislative changes in 2010-11. In general, all agencies again stated their commitment to ensuring that their staff are informed of legislative requirements as they relate to agency functions and operations, and that where applicable they received targeted training to ensure understanding and compliance.

## Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011

2.11    The *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011* received Royal Assent on 22 March 2011.

2.12    The Act Amended the *Telecommunications (Interception and Access) Act 1979* to:

- enable ASIO to provide technical assistance to law enforcement agencies in relation to telecommunications interception warrants;

- require carriers and certain carriage service providers to inform the Communications Access Co-ordinator of proposed changes to telecommunications services, networks, systems or devices that could adversely affect the ability to conduct interception;

- enable authorised police officers to disclose telecommunications data when trying to locate missing persons;

- enable enforcement agencies to apply for a stored communications warrant to access stored communications of a victim of a serious contravention, without the person's consent; and,

- permit notification of an interception warrant to be made to a representative of a carrier.

2.13    The Act also made minor and technical amendments to the *Australian Security Intelligence Organisation Act 1979*, *Intelligence Services Act 2001* and *Telecommunications (Interception and Access) Act 1979* to enable ASIO, the Australian Secret Intelligence Service, the Defence Signals Directorate and the Defence Imagery and Geospatial Organisation to work cooperatively.

## Intelligence Services Legislation Amendment Act 2011

2.14     The *Intelligence Services Legislation Act* received Royal Assent on 25 July 2011. Although slightly outside of the reporting period it was mentioned by agencies as having an impact on them.

2.15     The Act amended the *Australian Security Intelligence Organisation Act 1979*:

- to provide a consistent meaning of foreign intelligence and consistent approach to foreign intelligence with the *Intelligence Services Act 2001.*

2.16     The Act amended the *Criminal Code Act 1995* to:

- clarify that the immunity for liability for certain employees for computer-related activities cannot be overridden by other Commonwealth, state or territory laws.

2.17     The Act amended the *Intelligence Services Act 2001* to:

- provide a specific function for the Defence Imagery and Geospatial Organisation to assist the defence force;

- provide a new ground for granting a ministerial authorisation for producing intelligence on a person;

- clarify that the immunity for liability for certain employees for computer-related activities cannot be overridden by other Commonwealth, state or territory laws; and,

- move existing exemptions from the Legislative Instruments Regulations 2004 into the Act.

2.18     Commenting on these changes DIGO stated:

> This is not an extension of the functions of DIGO, but a clarification, and is consistent with a similar function for DSD. As DIGO and DSD are part of Defence, it is an inherent role of each to support the ADF. DSD has a specific function to provide assistance to the ADF in support of military operations and to cooperate with the ADF on intelligence matters (see paragraph 7(d) of the ISA[4]). However DIGO had no such provision included when it was added to the ISA in 2005. DIGO does have the ability to provide assistance and cooperate with the ADF under a number of its current functions. However, the new function ensures any gaps in DIGO's ability to assist the ADF are avoided and will make reporting, compliance and administrative processes more efficient,

---

4    *Intelligence Services Act 2001.*

particularly in areas of support of the ADF's own intelligence collection activities.[5]

# Litigation

2.19 ASIO reported to the Committee that it:

> . . . continued to contribute actively to prosecutions in national security cases, with ASIO officers and information often required in evidence or in responding to requests or subpoenas from the prosecution or defence. The diverse nature of the legal proceedings ASIO is involved in – including criminal (particularly terrorism) prosecutions, judicial and administrative reviews of security assessments and a range of civil actions – continues to produce a significant and increasing workload within ASIO.[6]

2.20 Another agency reported to the Committee that it worked with the National Archives of Australia in relation to claims for access to its classified material under the Archives legislation.

2.21 One agency reported being involved in the Coronial Inquiry into SIEV 221 in Western Australia.

# Human resource management within the agencies

## Management of growth

2.22 Apart from ASIO, those agencies experiencing growth in their workforce characterised it as marginal and some agencies actually decreased their Full Time Equivalent staffing levels.

2.23 The significant organisational growth experienced by some agencies has now abated and all agencies have succeeded in integrating large increases in staffing over recent years. ASIO, as recommended by the Review of ASIO Resourcing, conducted by the late Mr Allan Taylor AM in 2005 (the Taylor Review), did increase its staffing levels.

---

5 *DIGO Classified Submission*, No. 5, pp. 6-7.
6 *ASIO Unclassified Submission*, No. 2, p. 18.

2.24    In addition to the Taylor Review ASIO has also recently experienced significant growth due to the inclusion of border and territory sovereignty under the definition of security in the ASIO Act. ASIO told the Committee that:

> These factors, coupled with the fast-pace investigative work required in the areas of counter-terrorism and counter-espionage, have placed a considerable demand on ASIO to effectively manage the growth of the Organisation and its duties.

> ASIO's senior leadership has sought to manage this growth by focusing on developing the capabilities of ASIO staff, shaping an appropriate culture while actively managing change and engaging proactively with risks. The development of a modern, sophisticated senior committee structure, targeting recruitment to find the people with the right skills, characteristics and capabilities, and providing ongoing training and professional development for staff across all areas of ASIO will continue to assist the Organisation to manage growth experienced to date.[7]

## Recruitment

2.25    Recruitment remained a high priority for the agencies, in order to continue to attract staff with the necessary skill sets. Agencies described to the Committee the many methods which they employ to recruit staff.

2.26    ASIO reported to the Committee that its:

> . . . recruitment activity in 2010-11 was focused on positioning the Organisation to fulfil the target of 1,860 full-time staff by the 2012-13 budget cycle, to meet the recommendation in the Review of ASIO Resourcing conducted by Mr Allan Taylor AM in 2005.[8]

2.27    ASIO also told the Committee that:

> We have fallen back in the last two years in terms of the recruitment, although we are picking up again now for intelligence officers and also for technical people.[9]

2.28    In 2010–11, 196 new staff were recruited to the ASIO workforce, resulting in net growth of 78 and total staff of 1769. ASIO continues to use the

---

7    *ASIO Unclassified Submission*, No. 2, p. 33.

8    *ASIO Unclassified Submission*, No. 2, p. 17.

9    *Classified Transcript*, 23 March 2012, p. 3.

internet as well as print media to engage with prospective employees, with advertisements appearing across a range of online media.[10]

2.29    The internet remains one of ASIO's key mediums through which it engages:

> . . . with prospective employees, placing recruitment advertisements across a range of online media, including social networking sites as well as traditional media. Prospective applicants were also attracted through the ASIO website, which was updated throughout the year with vacancies and information about positions available within the Organisation.[11]

2.30    DIGO informed the Committee that it tries to attract and retain talented staff by providing a work environment that offers continuous professional development, opportunities for career diversity or specialisation, and a clear link between work outputs and mission success.

2.31    DIO reported to the Committee that it used 'a number of methods' to attract staff in 2010-11 including conducting generic and specialist recruitment rounds and the Defence Graduate Development Program (GDP).[12]

2.32    DSD provided the Committee with detailed unclassified information on its recruitment processes:

> DSD used a number of strategies to recruit talented staff in 2010-11. This included generic and specialised recruitment rounds, transfers at level and the *Altitude@DSD* graduate program. In total, DSD conducted 167 recruitment actions in 2010-11 to fill current and future growth targets. These actions will continue to see applicants being engaged during 2011-12 and 2012-13. Increased recruitment activity in 2009-10 produced 221 external recruits in 2010-11 (compared to 171 in 2009-10) which contributed to required growth targets.

2.33    The Committee is satisfied that each of the agencies under review approach recruitment in a way that is sensitive to the national security issues that they deal with whilst being open to attracting the best candidates from the diversity of the Australian community.

---

10    *ASIO Unclassified Submission*, No. 2, p. 17.
11    *ASIO Unclassified Submission*, No. 2, p. 39.
12    *DIO Classified Submission*, No. 6, p. 9.

## Workplace Diversity

2.34    The Committee was informed that ONA:

> . . . continues to support the needs of people with disabilities, through the implementation of its Disability Action Plan and Workplace Diversity Program. Key strategies are contained in staff selection procedures and reflect merit, fairness and freedom from discrimination.[13]

2.35    The Committee was told that:

> During 2010–11, ASIO implemented recruitment and people management strategies designed to create an inclusive working environment that recognises and utilises the diversity in the workforce, seeking to recruit a range of people that reflect the Australian community.[14]

## Gender

2.36    Five of the six agencies submitted data on the workforce demographics within their agencies for 2010-11. Overall the proportion of women employed by the agencies, as against men, was lower in comparison with the APS average of 57.6 per cent of total employment.[15]

2.37    The Defence agencies were particularly low, with percentages for the three agencies ranging from a low of 27[16] per cent to a high of 39[17] per cent. In noting this the Committee acknowledges that some of the roles within the Defence agencies reflect the unique nature of some former ADF units that have been civilianised.

2.38    ASIO reported to the Committee that women now make up 44 percent of ASIO's workforce.[18] The Committee notes that this is the highest percentage amongst those agencies that reported its demographic data to the Committee for its 2010-11 review.

---

13    *ONA Classified Submission*, No. 8, p. 15.

14    *ASIO Unclassified Submission*, No. 2, p. 44.

15    Australian Public Service Commission, *State of the Service Report 2010-11*, p. 90. <http://www.apsc.gov.au/__data/assets/pdf_file/0015/3336/completereport.pdf> viewed on 30 May 2012.

16    *DIGO Classified Submission*, No. 5, p. 8.

17    *DIO Classified Submission*, No. 6, p. 6.

18    *ASIO Unclassified Submission*, No. 2, p. 44. 783 female employees out of a total of 1,769 employees.

## Training and Development

2.39    All agencies reported on the importance of training and development in providing the Australian Government with a professional, ethical and technologically competent intelligence gathering and analysis capability.

2.40    Tradecraft training is an integral part of the training for intelligence officers. Agencies explained the importance of tradecraft training to the Committee and, in some cases, described the kinds of courses officers might undertake.

2.41    DIO informed the Committee that they had:

> . . . launched a redeveloped analytic tradecraft training continuum to better match our analysts' unique tradecraft requirements. In addition to existing tradecraft courses, DIO designed and delivered a comprehensive suite of training targeted at building analysts' principle tradecraft skills.[19]

2.42    All agencies reported on training designed to develop staff in middle management, in executive leadership and to provide support through mentoring programs.

2.43    Agencies also reported on taking part in National Intelligence Community (NIC) training programs.

## Linguistic Skills

2.44    Linguistic skill is important to all members of the Australian Intelligence Community and forms a vital part of workforce planning for agencies. Significant classified evidence from ASIO and the Defence agencies was taken by the Committee.

2.45    ONA reported to the Committee that they have:

> . . . 47 staff members who are proficient in one or more foreign languages. In 2010-11 twenty-four staff received a language proficiency allowance to develop and maintain their skills; these are important to their analytical role and for members of the intelligence community. Some staff participate in lunchtime language discussion classes, either in ONA or at DFAT. Some also received on-on-one tutoring for an hour or so per week.[20]

2.46    ASIO has:

---

19    *DIO Classified Submission*, No. 6, p. 11.

20    *ONA Classified Submission*, No. 8, p. 17.

> . . . increased its foreign language capabilities and capacity to
> support the Organisation's counter-terrorism, counter-espionage
> and foreign interference investigations. Along with working with
> key domestic and international partners to strengthen resource
> sharing and benchmarking, ASIO streamlined procedures to
> process and disseminate foreign language product more
> efficiently.[21]

2.47    In addition to the above:

> ASIO also facilitated several short-term foreign language support
> activities with key domestic and foreign partners, including
> several secondments between ASIO and partner agencies. These
> short-term support activities filled critical language capability
> gaps and ensured agencies, including ASIO, were better placed to
> meet their foreign language requirements.[22]

2.48    It was very clear to all members of the Committee that linguistic skills are
        one of the key areas that intelligence agencies must develop and maintain.
        The Committee raised some concerns with agencies in relation to
        particular language groups. The Committee was assured that their
        concerns were already being acted upon by the agencies in question.

## Separation rates and retention strategies

### Separation rates

2.49    The average separation rate across the APS for 2010-11 was 6.8 per cent.[23]
        The Defence Intelligence agencies all reported separation rates higher than
        the APS average. Reasons given for this were, in part, improved
        employment conditions following the Global Financial Crisis, and the
        desirability and transferability of many of the skills that staff of DIGO,
        DIO and DSD possess.

2.50    The majority of staff separating from the Defence agencies remained
        within the wider Department of Defence or moved into another APS
        agency.

---

21   *ASIO Unclassified Submission*, No. 2, p. 41.
22   *ASIO Unclassified Submission*, No. 2, p. 41.
23   Australian Public Service Commission, *State of the Service Report 2010-11*, p. 107.
     <http://www.apsc.gov.au/__data/assets/pdf_file/0015/3336/completereport.pdf> viewed
     on 30 May 2012.

2.51    ASIO's separation rate increased to 5.8 percent compared with 5.0 percent in 2010-11.[24]

2.52    An ongoing theme when discussing separation rates with the agencies was the challenge in achieving a balance between retaining staff and encouraging mobility.

## Retention strategies

2.53    In classified evidence all of the Defence agencies reported on various management processes that encourage and increase staff retention. Some of these were:

- Mentoring

- Creating career pathways/mobility

- A healthy work-life balance

- Skilled, capable and accountable people managers. [25]

2.54    Other agencies did not specifically report on retention strategies although all agencies pointed to the importance of creating a work environment in which staff felt that their input was valued and recognised.

# Security issues

## Security clearances

### Australian Government Security Vetting Agency

2.55    On 1 October 2010, the Australian Government Security Vetting Agency (AGSVA) was established. AGSVA is located within the Department of Defence and is the central agency for the processing, evaluating and granting of security clearances for the Commonwealth. The AGSVA conducts clearances for the majority of Government agencies under a fee-for-service model.[26]

---

24    *ASIO Unclassified Submission*, No. 2, p. 40.

25    *DIGO Classified Submission*, No. 5, p. 16. *DIO Classified Submission*, No. 6, p. 10. *DSD Classified Submission*, No. 7, p. 14.

26    See < http://www.defence.gov.au/agsva/> viewed on 30 May 2012.

2.56    Across the Defence Intelligence agencies AGSVA provided most security clearances, including initials, upgrades and re-evaluations.

2.57    ASIO again provided the Committee with a detailed overview of its part in the security assessment process for the APS. Under Part IV of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act), ASIO is responsible for providing security assessments to Commonwealth agencies.

2.58    In making their assessment, ASIO officers are required to limit the factors underpinning security assessments to grounds related to 'security' as is defined in the ASIO Act.[27] Within the act, 'security' is defined as the protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence system and acts of foreign inference.[28] Once ASIO has provided advice to the requesting agency in relation to whether the assessment should be granted, the requesting agency then makes the determination as to whether to grant the clearance.

## Visa security assessments

2.59    ASIO stated in their submission that any person applying for a visa to travel to, or remain in, Australia may have their application referred by the Department of Immigration and Citizenship (DIAC) to ASIO for a security assessment. ASIO makes an assessment of the risk that the person's presence in Australia would pose to security (as defined above).

2.60    ASIO stated that it:

> . . . completed 34,396 visa security assessments in 2010–11. 45 adverse assessments were made in relation to visas, with 40 of these adverse assessments issued on counter-terrorism grounds, two on the grounds of involvement in people smuggling and three on the basis of counter-espionage or foreign interference.
>
> In December 2010, the government directed that only irregular maritime arrivals (IMAs) found to be owed protection obligations, such as refugee status, would be referred to ASIO for a security assessment to determine any threat to security from the granting of permanent residence in Australia. As a result, in January 2011, ASIO developed a referral framework which commenced operation in April 2011. This new framework has enabled ASIO to

---

27    *ASIO Unclassified Submission*, No. 2, p. 55.

28    Part I 4(a) of the *Australian Security Intelligence Organisation Act 1979*.

focus on complex IMA cases requiring intelligence investigation and to streamline the security process for non-complex cases in accordance with the risk to security they present.[29]

2.61    The ASIO Director-General told the Committee at its public hearing that:

> . . . given the number of boat people arriving, the requirement for us to conduct, a security assessments process, which we have been refining down and refining down, nevertheless still represents a very, very considerable allocation of the organisation's resources. It is not a misallocation, in the sense that those assessments have turned up 58 cases in the last year and a half or two years where we have said, 'No, we don't believe that that person should be coming to Australia, because there is a potential security risk there.'[30]

2.62    The Committee also heard that, whilst the attention in relation to visa security assessments is focussed on boat arrivals it is plane arrivals that create a lot of work for ASIO, but that:

> . . . at least they arrive with a passport and at least they do not have four different dates of birth or three different names, so you actually have something you can check.[31]

2.63    For its report *Review of Administration and Expenditure No. 9* the Committee took a large amount of detailed evidence from ASIO – including some evidence given during a public hearing – and from several refugee and asylum seeker advocacy groups in relation to the visa security assessment process. After considering this evidence the Committee commented that:

> The Committee takes very seriously the concerns put before it by various refugee and asylum seeker advocacy groups but it also recognises that the job ASIO has is a very difficult one. Therefore, the Committee welcomes the efforts, introduced by ASIO on 1 March 2011, to streamline the process of security assessments in an attempt to clear the backlog and to process future assessments in less time.  The Committee is satisfied that the current regime for visa security assessments is the correct one.[32]

---

29  *ASIO Unclassified Submission*, No. 2, pp. 56-57.
30  *Classified Transcript*, 23 March 2012, p. 2.
31  *Classified Transcript*, 23 March 2012, p. 6.
32  Parliamentary Joint Committee on Intelligence and Security, *Review of Administration and Expenditure No. 9 – Australian Intelligence Agencies* Parliamentary Paper No.:156/2012; Tabled 18 June 2012, p. 20.

2.64    The Committee has received no evidence to cause it to adjust this
        assessment of the current regime for visa security assessments.

## ASIO Personnel security assessments

2.65    ASIO also undertakes personnel security assessments at the request of
        other APS agencies to determine if an individual can have access to
        security classified material.

2.66    ASIO explained that, under changes to Australian Government policy in
        2010-11 :

> . . . the new national security clearance levels are Baseline,
> Negative Vetting Level 1 (encompassing the previous levels of
> Confidential and Secret), Negative Vetting Level 2 (Top Secret
> Negative Vetting) and Top Secret Positive Vetting. The non-
> national security clearance levels of Protected and Highly
> Protected were abolished. ASIO personnel security assessments
> are mandatory for all persons requiring security clearances, except
> Baseline clearances. Agencies should refer Baseline clearances to
> ASIO where they identify a genuine link to security.[33]

2.67    ASIO states:

> Since January 2011, all security access assessment referrals have
> come to ASIO electronically from AGSVA, except for a small
> percentage received by ASIO from AGSVA-exempt agencies. In
> 2010–11, ASIO completed 31,099 security access assessment
> referrals, which represents a 39 per cent increase in the number of
> security access assessment referrals completed by ASIO in 2009–
> 10.[34]

## Counter-terrorism security assessments

2.68    ASIO undertakes counter-terrorism security assessments to assist in
        granting:

- maritime security identification cards (MSIC);

-  aviation security identification cards (ASIC);

- access to the Australian Nuclear Science and Technology Organisation
  (ANSTO) facility at Lucas Heights, Sydney;

---

33   *ASIO Unclassified Submission*, No. 2, p. 58.
34   *ASIO Unclassified Submission*, No. 2, p. 58.

- access to dangerous goods; and

- accreditation for individuals to work at special events, such as CHOGM.[35]

2.69    ASIO reported to the Committee that it completed 109,166 counter-terrorism security checks in 2010-2011 which represents an 11 per cent increase from 2009-10. 97,922 of these were ASIC and MSIC assessments.

> During the reporting period, ASIO issued two adverse counter-terrorism security assessments – one was for access to dangerous goods and the other was for an ASIC. This was the first time ASIO has issued adverse security assessments for these purposes.

> In 2011, ASIO undertook counter-terrorism security assessments for MSIC renewals for the first time and also provided security assessments for access to restricted areas in relation to CHOGM 2011.[36]

## Breaches of security

2.70    Each of the Defence agencies provided the Committee with information on physical and electronic security breaches.[37] In all cases there was either a finding or consequence rating of 'no compromise of national security information' or incidents were assessed as a 'breach of the need-to-know principle as a result of these breaches'.

2.71    The Committee was informed that a consequence rating is an internal rating done by each of the agencies in relation to a security breach and that flowing from this:

> . . . it might not simply be a matter of disciplining some person; we might, through the investigation process, learn that we actually have a flaw in procedures, or procedures and policies are not being implemented, and we can take steps to address that. So it is an iterative learning process from each of these events.[38]

2.72    The Committee was briefed on a breach by an officer of one agency at a classified hearing.

---

35    *ASIO Unclassified Submission*, No. 2, p. 58.
36    *ASIO Unclassified Submission*, No. 2, pp. 58-59.
37    *DIGO Classified Submission*, No. 5, p. 24. *DIO Classified Submission*, No. 6, p. 18. *DSD Classified Submission*, No. 7, p. 24.
38    *Classified Transcript*, 23 March 2012, p. 46.

2.73    ASIO reported to the Committee that they have a host of internal security policies to help staff uphold high standards when it comes to security practice. ASIO have a Security Plan 2009-12 and a Security Breach policy which:

> . . . provide strategies to mitigate security risks and provides a framework for staff to ensure sound security is practised in daily business. [39]

2.74    ONA reported 21 technical security breaches in 2010-11 and that the IT security:

> . . . function has become embedded in routine management processes. All major systems are fully audited and daily analysis and investigation of anomalies is undertaken to identify any security breaches or system intrusions. New security controls are continuously evaluated to maintain effectiveness in addressing the evolving cyber threat landscape and to enable the use of cutting-edge information technology.[40]

## Staff surveys

2.75    All agencies conduct staff surveys annually or biennially. Two agencies did so in the review period 2010-11.

2.76    ASIS reported that it achieved a high participation rate of 86.8 per cent. The agency stated that overall the survey results revealed an encouraging picture, while identifying some areas for improvement.[41]

2.77    ONA's survey results indicated:

> . . . that 80% of ONA employees are very positive about the organisation. This figure is well above the Australian High Performing Organisations Benchmark average of 53%. External benchmarking indicates that ONA is performing well above the Australian government and Australian workforce averages on all survey items and categories and set new benchmark highs for most categories surveyed.[42]

---

39   *ASIO Unclassified Submission*, No. 2, p. 61.
40   *ONA Classified Submission*, No. 8, p. 27.
41   *ASIS Classified Submission*, No. 4, p. 21.
42   *ONA Classified Submission*, No. 8, p. 18.

2.78    The Committee believes that staff surveys are an important management
        tool and looks forward to taking evidence from other agencies on their
        results in the next report covering 2011-2012.

## Accommodation

### ASIO's new central office

2.79    The Committee is aware that the collapse of Heyday Group — a
        subsidiary of engineering company Hastie —has had an impact on ASIO's
        new building. However this occurred outside the time-frame of this
        review and will be dealt with by the Committee in the next review.

2.80    During 2010-11 those involved in constructing ASIO's new headquarters:

> . . . continued to increase, with over 800 contractors employed on
> site as at time of writing. At the close of the reporting period,
> construction 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.[43]

### Other agencies

2.81    DIGO's accommodation consists of offices at building R4 in the Russell
        Offices Complex and the Geospatial Analysis Centre (GAC) at Junortoun,
        near Bendigo, Victoria.

2.82    DIGO reported the following to the Committee:

- During 2010-11 work concluded on the installation of a redundant
  power supply for the site at Junortoun. This work enables the site to
  have independent power … in the event of an outage and helps protect
  critical equipment capability at the site; and

- To improve safety and amenity for DIGO workers and residents around
  the GAC, traffic lights were installed at a major intersection near the
  site. The Defence funded works address safety issues identified in a
  traffic study conducted where the GAC was built.[44]

43   *ASIO Unclassified Submission*, No. 2, p. 49.
44   *DIGO Classified Submission*, No. 5, p. 7.

2.83    During 2010-11 DSD continued to work on plans for further upgrades to
        the Cyber Security Operations Centre (CSOC). The number of staff is
        expected to grow over the next few years and the refurbishment will
        therefore optimise the current space for CSOC functionality and
        accommodate the maximum number of staff possible.[45]

2.84    ONA informed the Committee that they moved to their new office at 2
        National Circuit on 17 October 2011. The new building is a 1930's heritage
        brick building which required extensive refurbishment and the design of
        environmentally sustainable infrastructure that respected the heritage
        attributes of the building. ONA told the Committee that:

>       The 2 National Circuit project provides significant environmental
>       benefits for ONA. Design efforts have focused on meeting the 4 1/2
>       star National Australian Built Energy Rating Sytem (NABERS)
>       energy rating mandated by the Energy Efficiency in Government
>       Operations (EEGO) policy.[46]

## Performance management and evaluation

2.85    All agencies within the AIC engaged in performance management and
        evaluation in 2010-2011, both at the organisational level and at the
        individual employee level. All agencies submitted to the Committee that
        performance management, at both levels, remains a key element of
        strategic planning and focus.

### Organisational performance management

2.86    On organisational performance management ASIO submitted to the
        Committee that:

>       ASIO's senior leadership group rigorously assesses its
>       performance against specific benchmarks on a quarterly basis,
>       utilising a 'traffic light' evaluation system. Underperformance
>       against particular outputs or goals can impact on decisions and
>       resourcing; operational or corporate priorities may need to be
>       changed and specific strategies may need to be implemented to
>       address the situation. [47]

---

45   *DSD Classified Submission*, No. 7, p. 7.
46   *ONA Classified Submission*, No. 8, p. 24.
47   *ASIO Unclassified Submission*, No. 2, p. 36.

2.87    In 2010-11 ASIO carried out some specific activities in relation to organisational performance management as follows:

- mapped the relationship between strategic risks identified in the Strategic Risk Management Framework and performance reporting benchmarks to assess the extent to which performance reporting informs ASIO's management of strategic risks.

- created an Organisational statistics library to collate, in a single coordinated space, statistical data reflecting ASIO performance and output over the last ten years. This will serve as a valuable platform for past and future trend analysis and inform ASIO's strategic planning.[48]

2.88    ONA's main process for organisation performance management is their Review of Key Judgments which is conducted twice yearly:

> The focus of the review is primarily on key judgments. These are usually the judgments that appear on the cover page of an assessment, but important judgments in the text are also covered. ONA branch heads identify where key judgments, with the benfit of hindsight, proved not to be correct. The review also covers any 'judgment creep', that is, inadvertent or incremental change to previous judgments.[49]

## Individual performance management

2.89    Each agency submitted to the Committee the process or frame work under which they manage individual performance.

2.90    In relation to individual performance management ASIO told the Committee about its performance management framework, Enhancing Performance, which is:

> . . . a modern approach to managing, building and delivering capability within ASIO's workforce, while interconnecting with ASIO's mission and objectives to provide opportunities to improve employee engagement across the Organisation.

> The Enhancing Performance framework and associated activities are supported by a range of interactive processes and tools. These aim to cultivate leadership skills and practices, assist managers to focus on managing for performance, support effective performance conversations and plan for individual and

---

48  *ASIO Unclassified Submission*, No. 2, p. 36.
49  *ONA Classified Submission*, No. 8, p. 6.

professional growth. This newly designed framework was
implemented within ASIO in July 2011.[50]

2.91    In addition to the Enhancing Performance framework in October 2010:

> . . . ASIO launched the new People Capability Framework, which
> allows ASIO to more accurately describe the capabilities and
> behaviours required of its workforce to deliver broader and more
> complex outcomes to the Australian Government. The People
> Capability Framework is based on the Australian Public Service
> Integrated Leadership System. Future focused, the framework
> supports ASIO's strategic intent, reflects ASIO's unique role and
> frames the workforce required to achieve excellence.[51]

2.92    ONA told the Committee that:

> All ONA staff members participated in ONA's Performance
> Development Framework (PDF), which focuses on individual's
> role specific priorities and the broader behaviour and capability
> expectations consistent with the APS Integrated Leadership
> System. Employees and their managers are required to meet and
> discuss priorities for the year ahead and document their
> agreement. The framework requires biannual participation in
> performance reviews and a rating process that determines the
> annual bonus or pay grade for individual employees.[52]

2.93    The majority of ONA's SES received pay increases or a one-off bonus
payment based on a percentage of their annual remuneration. These
bonuses ranged from $1,000 — $4,000.[53]

2.94    Each of the Defence agencies reported on their individual performance
management frameworks.[54] DSD told the Committee that:

> The performance of DSD's APS staff is formally assessed through
> the Defence *Performance Feedback and Development Scheme* (PFADS).
> Individual performance is assessed twice a year, in August and
> February, with performance progression payment occurring in
> November. DSD also encourages supervisors to regularly provide
> timely and accurate feedback to their staff on an informal basis.[55]

---

50  *ASIO Unclassified Submission*, No. 2, p. 42.

51  *ASIO Unclassified Submission*, No. 9, p. 42.

52  *ONA Classified Submission*, No. 8, p. 14.

53  *ONA Classified Submission*, No. 8, p. 14.

54  *DIGO Classified Submission*, No. 5, p. 19. *DIO Classified Submission*, No. 6, p. 13. *DSD Classified Submission*, No. 7, p. 20.

55  *DSD Classified Submission*, No. 7, p. 20.

2.95    DIGO and DIO also use the Defence *Performance Feedback and Development Scheme* (PFADS).[56]

# Issues raised by the IGIS

2.96    The Committee received an unclassified submission from the Inspector General of Intelligence and Security (IGIS) in which she raised some specific concerns about the administrative functions of the AIC agencies. The Committee greatly values the input from the IGIS. Her contribution provides invaluable, well informed third-party commentary on the matters before the Committee.

## Visa security assessments

2.97    In commenting on visa security assessments the IGIS stated:

> In 2010/11 the OIGIS received 1111 complaints about ASIO's processing of security assessments for visa applicants. This figure is an increase of around 9% from the 1015 received in 2009/10.[57]

2.98    The IGIS listed several reasons as to why she thought there had been such an increase in complaints about visa security assessments. These were:

- as the numbers of visa applicants referred to ASIO for a security assessment has trended upwards in recent years backlogs develop; and,

- the role and functions of the IGIS have become better known.[58]

2.99    The IGIS also stated that:

> I noted a stabilisation and then a relative decline in the number of complaints made to my office in the last quarter of 2010/11. I attribute this to the implementation by the Department of Immigration and Citizenship (DIAC), in collaboration with ASIO, of a triaging approach to security assessments for visa applicants who meet the criteria for refugee status.[59]

---

56   *DIGO Classified Submission*, No. 5, p. 19. *DIO Classified Submission*, No. 6, p. 13.
57   *IGIS Unclassified Submission*, No. 1, p. 2.
58   *IGIS Unclassified Submission*, No. 1, p. 2.
59   *IGIS Unclassified Submission*, No. 1, p. 2.

2.100    The IGIS pointed to an incidence of administrative error that was very small and had implemented, in consultation with ASIO, a new inspection process in relation to visa security assessments.[60]

## DSD testing inquiry

2.101    The IGIS investigated and confirmed the use of 'study guides' or 'cheat sheets' in relation to compliance testing within DSD. She made recommendations concerning:

- the re-testing of staff;

- future coordination of compliance training and testing; and,

- professional development of first-level supervisors.[61]

2.102    DSD accepted all of the IGIS's recommendations.[62]

2.103    The IGIS reported to the Committee on certain other matters she was investigating:

- An inquiry into the arrest and detention overseas of Mr Mamdouh Habib.
  - ⇒ The inquiry was ongoing as at 30 June 2011, but was completed and the report provided to the Prime Minister and relevant Ministers in late December 2011.

- Two preliminary inquiries about the processing of visa security assessments.
  - ⇒ Both inquiries indentified some administrative errors.

- Two preliminary inquiries into ASIO concerning the alleged misconduct of ASIO officers in their dealings with members of the public.
  - ⇒ In both cases the IGIS found no evidence to support the allegation that ASIO officers acted in an illegal, in appropriate or unprofessional manner.

- A preliminary inquiry into the handling of personal information by DSD during a recruitment process and delays in that process.

---

60    *IGIS Unclassified Submission*, No. 1, p. 2.

61    *IGIS Unclassified Submission*, No. 1, p. 4.

62    See *DSD Classified Submission*, No. 7, p. 21.

# Conclusion

2.104   The Committee is satisfied that overall the administration of the six
        intelligence and security agencies is currently sound.