

---

The Parliament of the Commonwealth of Australia

# Review of Administration and Expenditure: No.9 – Australian Intelligence Agencies

Parliamentary Joint Committee on Intelligence and Security

March 2012  
Canberra

---

© Commonwealth of Australia 2012

ISBN 978-0-642-79550-2 (Printed version)

ISBN 978-0-642-79551-9 (HTML version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website:

<http://creativecommons.org/licenses/by-nc-nd/3.0/au/>



# Contents


- Membership of the Committee .....vi
- Terms of reference .....viii
- List of abbreviations .....ix
  
- 1 Introduction .....1**
  
- 2 Administration.....3**
  - Organisation of agency structure.....3
  - Impact on agencies of recent legislative changes .....4
  - Litigation.....5
  - Human resource management within the agencies.....6
  - Management of growth .....6
  - Recruitment.....7
  - Workplace diversity .....8
  - Training and development.....9
  - Linguistic skills .....9
  - Separation rates and retention strategies.....10**
    - Separation rates.....10
    - Retention strategies .....11
  - Security issues.....11**
    - Cyber security .....12

---

Security clearances .....	12
Visa Security Assessments .....	13
ASIO personnel Security Assessments.....	21
Counter-terrorism security assessments.....	21
Breaches of security.....	21
<b>Staff surveys.....</b>	<b>22</b>
<b>Accommodation .....</b>	<b>23</b>
ASIO's new central office .....	23
Other agencies.....	24
<b>Performance management and evaluation .....</b>	<b>24</b>
Organisational performance management .....	24
Individual performance management .....	25
<b>Issues raised by the IGIS.....</b>	<b>26</b>
Archives-related complaints .....	26
<b>Conclusions.....</b>	<b>26</b>
<b>3 Expenditure.....</b>	<b>29</b>
The efficiency dividend .....	29
Submission from the ANAO .....	30
<b>Budget Growth .....</b>	<b>31</b>
Agencies other than ASIO.....	31
ASIO .....	31
Recruitment costs .....	32
Training costs.....	33
<b>Financial governance systems .....</b>	<b>33</b>
<b>Fraud control and risk management .....</b>	<b>33</b>
<b>Conclusions.....</b>	<b>34</b>

---

<b>4</b>	<b>Interoperability .....</b>	<b>35</b>
	The National Intelligence Coordination Committee .....	36
	The National Intelligence Collection Management Committee .....	37
	The National Intelligence Open Source Committee .....	37
	The National Threat Assessment Centre .....	37
	National Interception Technical Assistance Centre .....	38
	The Cyber Security Operations Centre .....	38
	Conclusions.....	38
	<b>Appendix A – List of Submissions .....</b>	<b>39</b>
	<b>Appendix B – Witnesses appearing at hearings .....</b>	<b>41</b>
	Private hearing.....	41
	Public hearing .....	42



## Membership of the Committee

**Chair**            The Hon Anthony Byrne MP

**Deputy Chair**   The Hon Philip Ruddock MP

**Members**        Mr Michael Danby MP  
                      Mr John Forrest MP (from 06/07/11)  
                      Mr Daryl Melham MP (to 14/03/12)  
                      The Hon Kevin Rudd MP  
                      (from 14/03/12)  
                      Mr Andrew Wilkie MP

Senator Mark Bishop (from 01/07/11)  
Senator the Hon George Brandis SC  
(from 06/07/11)  
Senator the Hon John Faulkner  
Senator Michael Forshaw (to 30/06/11)  
Senator the Hon David Johnston  
(from 06/07/11)  
Senator Julian McGauran (to 30/06/11)  
Senator the Hon Ursula Stephens  
(from 06/07/11)  
Senator Russell Trood (to 30/06/11)

## Committee Secretariat

Secretary	Dr Margot Kerley (to 08/06/11)
A/g Secretary	Dr John Carter (from 09/06/11 to 25/07/11)
Secretary	Mr Jerome Brown (from 26/07/11)
Inquiry Secretary	Mr Robert Little
Research Officer	Dr Cathryn Ollif
Administrative Officers	Ms Jessica Butler
	Ms Gillian Drew



## Terms of reference

This review is conducted under paragraph 29(1)(a) of the *Intelligence Services Act 2001*:

- to review the administration and expenditure of ASIO, ASIS, DIGO, DIO, DSD and ONA, including the annual financial statements (of) ASIO, ASIS, DIGO, DIO, DSD and ONA.





## List of abbreviations

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
AIC	Australian Intelligence Community
ANAO	Australian National Audit Office
APS	Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASIO Act	<i>Australian Security Intelligence Organisation Act 1979</i>
ASIS	Australian Secret Intelligence Service
ASRC	Asylum Seeker Resource Centre
CSOC	Cyber Security Operations Centre
DFAT	Department of Foreign Affairs and Trade
DIAC	Department of Immigration and Citizenship
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DSA	Defence Security Authority
DSD	Defence Signals Directorate
Finance	Department of Finance and Deregulation

FMA Act	Financial Management and Accountability Act 1997
IGIS	Inspector-General of Intelligence and Security
IMA	Irregular Maritime Arrivals
ISA	Intelligence Services Act 2001
ISPT	Industry Superannuation Property Trust
MAL	Movement Alert List
NIC	National Intelligence Community
NICC	National Intelligence Coordination Committee
NICMC	National Intelligence Collection Management Committee
NIOSC	National Intelligence Open Source Committee
NiTAC	National Interception Technical Assistance Centre
NTAC	National Threat Assessment Centre
ONA	Office of National Assessments
PDF	ONA's Performance Development Framework
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PM&C	Prime Minister and Cabinet
RCOA	Refugee Council of Australia
R.I.S.E.	Refugees Survivors & Ex-Detainees
SES	Senior Executive Service
TIA Act	Telecommunications (Interception and Access) Act 1979
TSPV	Top Secret Positive Vetting
UNHCR	United Nations High Commissioner for Refugees

## Introduction

- 1.1 Under Section 29 of the *Intelligence Services Act 2001* (the Act), the Parliamentary Joint Committee on Intelligence and Security has an obligation to review the administration and expenditure of ASIO, ASIS, DSD, DIGO, ONA and DIO, including their annual financial statements.
- 1.2 This is the report of the Committee of the 43<sup>rd</sup> Parliament's Review of Administration and Expenditure No. 9 – Australian Intelligence Agencies.
- 1.3 Submissions were sought from each of the six intelligence and security agencies, from the Australian National Audit Office (ANAO) and from the Inspector General of Intelligence and Security (IGIS) (see Appendix A).
- 1.4 The submissions from ANAO and the six intelligence agencies were all classified Confidential, Restricted or Secret and are therefore not available to the public. As has been its practice for previous reviews, ASIO provided the Committee with both a classified and an unclassified submission. The unclassified version is available on the Committee's website.
- 1.5 The Committee also received a submission from the ANAO and from the IGIS. The IGIS' submission was made available on the Committee's website. More comment in relation to the ANAO is contained in Chapter 3 on Expenditure.
- 1.6 Each of the Defence intelligence agencies provided the Committee with a classified submission. The agencies marked each paragraph with its relevant national security classification. This has enabled the Committee for its 2009-10 review to directly refer to unclassified information provided in the Defence agencies submissions.
- 1.7 The Committee also received five submission from members of the public or public organisations which included:

- Asylum Seeker Resource Centre
- Brigidine Asylum Seekers Project
- R.I.S.E.
- Refugee Council of Australia

- 1.8 These submissions all dealt with ASIO security assessments of refugees.
- 1.9 The Committee is grateful to ASIO for providing an unclassified submission and the Defence intelligence agencies for providing unclassified paragraphs within their classified submissions. This has been very helpful in the writing of this report. It means, however, that ASIO and the Defence intelligence agencies are mentioned quite often in the subsequent chapters of this report while the other agencies are generally not referred to by name. This should not be taken to imply that the inquiry focused primarily on ASIO or the Defence intelligence agencies or that they were scrutinised more than other agencies. It merely reflects the amount of unclassified information on which the Committee was able to draw and incorporate directly into its report to support its findings.
- 1.10 In November 2010, the Committee wrote to the agencies seeking submissions and outlining the issues it would like to see addressed.
- 1.11 On 25 March 2011 the Committee held a private hearing at which ASIO, ASIS, DSD, DIGO, ONA and DIO appeared before the Committee. The Committee appreciates the commitment of time each agency made to this process (see Appendix B).
- 1.12 On 16 June 2011 the Committee held a public hearing – its first since July 2006<sup>1</sup> – and heard from representatives of the Refugee Council of Australia, RISE (Refugees, Survivors and Ex-Detainees), the Asylum Seeker Resource Centre and ASIO in relation to visa security assessments. The Committee thanks all attendees, particularly those from organisations providing support to refugees, for the time and effort they took to put their views to the Committee.

---

1 Public hearings were held on 31 July 2006 and 1 August 2006 for the Committee's *Review of Security and Counter Terrorism Legislation*.

## Administration

- 2.1 This is the first full review of administration and expenditure of the six intelligence agencies carried out by the Committee of the 43<sup>rd</sup> 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 As reported in previous Administration and Expenditure reports, most of the intelligence agencies went through some organisational restructuring in 2007-08, then focussed on consolidating and monitoring those changes in 2008-09.
- 2.4 In 2009-10, most of the agencies did not make extensive organisational changes but continued to review and refine organisational structures following the significant growth which they experienced to varying

degrees over previous years. Only DSD reported substantial growth during the reporting period.

- 2.5 ASIO reported that in 2009-10, its Senior Management group reviewed the organisation's structure so that by improving efficiency and functional alignment it would be well-positioned to meet future challenges. The new structure was implemented just outside the reporting year, that is on 1 July 2010.<sup>1</sup>

## **Impact on agencies of recent legislative changes**

- 2.6 During 2009-10 several legislative changes were relevant to the work of the intelligence agencies.
- 2.7 Significant legislative amendments were made during 2009-10 to the *Telecommunications (Interception and Access) Act 1979*. Agencies told the Committee that these amendments will benefit agency operations.
- 2.8 The *Freedom of Information Act 1982* and the *Archives Act 1983* were both amended during the period under review and both amendments will impact intelligence agencies. The Archives Act contains an open access regime for records 30 years old or more. Intelligence agencies are not exempt from this Act. Over the next five years, the open access period will reduce from 30 to 20 years. This means that intelligence agency documents will be subject to a disclosure regime sooner and therefore the number of new records available for public access over the next 10 years will significantly increase.<sup>2</sup>
- 2.9 DIO told the Committee that during 2009-10 it received 175 Public Access Requests and responded to 104 with work continuing on the remaining case load. Consequently, at the close of 2009-10, it had enlarged its Public Access Requests area to three staff which is a significant increase from one part-time staff member during previous reporting periods. DIO is also reallocating staff resources to meet increasing demand for access to records.<sup>3</sup>
- 2.10 In 2009-10, DSD received 40 requests for public access to material under the *Archives Act 1983*. In 12 cases the material was no longer regarded as sensitive and was released by DSD. A further 25 requests contained

---

1 *ASIO Unclassified Submission*, No. 4, pp. 10 & 22.

2 *DIGO Classified Submission*, No. 10, p. 8.

3 *DIO Classified Submission*, No. 8, p. 5.

sensitive information, and these requests were agreed to with partial exemptions. The remaining three requests had not been finalised at the time of the Committee's inquiry.<sup>4</sup>

- 2.11 On 3 February 2010, Cabinet requested that the Attorney-General's Department lead a review of the *Intelligence Services Act 2001* (ISA) and the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) to address the issues of interoperability and intelligence sharing amongst Australian intelligence agencies. ASIS, DSD, DIGO and ASIO worked with the Attorney-General's Department and Prime Minister and Cabinet (PM&C) on these reviews. A number of recommendations were made which aim to improve interoperability and intelligence sharing between intelligence agencies. Agencies told the Committee that they believe these amendments will benefit agency operations. (The implications of these recommendations for the interoperability of intelligence agencies are discussed further in Chapter 4.) The Parliament passed the *Intelligence Services Legislation Amendment Act 2011* in respect of these changes on 4 July 2011.
- 2.12 The *Taxation Legislation Amendment (2010 Measures No.3) 2010 Act* made changes to tax legislation to allow the Directors-General of ASIS and ASIO to declare certain payments made in the performance of functions exempt from taxation.
- 2.13 Other legislative changes which affected ASIO included the *Anti-People Smuggling and other Measures Act 2010* and the *Crime Legislation Amendment (Serious and Organised Crime) Act 2010*.<sup>5</sup>

## Litigation

- 2.14 Only two agencies reported involvement in litigation or legal proceedings to the Committee.
- 2.15 ASIO was involved in over 40 litigation matters during the reporting period, including criminal (in particular terrorism) prosecutions, judicial and administrative review of Security Assessments, and a range of civil actions among which:

Particularly complex litigation proceedings to which ASIO contributed include the Sydney and Melbourne Pendennis and

---

4 DSD Classified Submission, No. 9, p. 25.

5 ASIO Unclassified Submission, No. 4, p. 12.

Operation NEATH terrorism prosecutions.

ASIO was also involved directly in two legal matters initiated by Mr Mamdouh Habib, a number of challenges to its Security Assessments, and former ASIO officer James Seivers's appeal against his conviction for the unauthorised communication of intelligence.<sup>6</sup>

- 2.16 The other agency reported to the Committee that during the reporting period it worked with the National Archives of Australia in relation to claims for access to its classified material under the Archives legislation and with the Department of Foreign Affairs and Trade (DFAT) to assist with the release, or partial release, of material in the course of litigation involving DFAT.
- 2.17 The Committee is satisfied that those agencies which were involved in litigation during 2009-10 dealt with these matters in an appropriate manner.

## **Human resource management within the agencies**

### **Management of growth**

- 2.18 Across most AIC agencies in 2009-10 staffing levels were stable.
- 2.19 DSD was the exception. It reported that it experienced significant organisational growth which was associated with additional funding. The growth posed some challenges for the agency, and in particular workforce management issues, including training and recruitment.<sup>7</sup>
- 2.20 ASIO aimed for significant growth during 2009-10 but it did not reach its 'ambitious recruitment targets' for the year due to employment market conditions combined with the necessarily stringent and lengthy security vetting of potential new staff.<sup>8</sup>
- 2.21 Another AIC agency reported to the Committee that it became apparent during 2009-10 that due to the growth of the agency over the past several years, the organisation did not have sufficient senior executive service

---

6 *ASIO Unclassified Submission*, No. 4, p. 12.

7 *DSD Classified Submission*, No. 9, p. 7.

8 *ASIO Unclassified Submission*, No. 4, p. 13.



personnel and, consequently, has made it a priority to expand that area of the agency.<sup>9</sup>

## Recruitment

- 2.22 As in previous years, recruitment remained a high priority for the agencies, in order to continue to attract high calibre staff with the necessary skill sets. Agencies provided information to the Committee on how they recruit staff.
- 2.23 The Committee also heard that some of the AIC agencies are now taking a more collaborative approach to both recruitment and security vetting. Discussions are taking place between some agencies to determine if there are opportunities to collaborate during recruitment processes for mutual benefit. It was said that AIC agencies are 'all fishing from the same pond'.<sup>10</sup>
- 2.24 As mentioned above, ASIO did not reach its recruitment targets in 2009-10 and recruitment will be a priority for the agency in 2010-11. ASIO told the Committee that it has developed new people management strategies to assist in meeting 'the higher net recruitment targets necessary to build and sustain a more effective national security intelligence capability'.<sup>11</sup>
- 2.25 ONA's new recruits during 2009-10 included the appointment in July 2009 of Mr Allan Gyngell as Director-General. Also during the reporting period, ONA developed a memorandum of understanding with PM&C to facilitate the short-term secondment of employees between the agencies. ONA sees this arrangement as valuable in exposing its staff to the policy environment and provides a gateway for exchange of ideas and the building of productive networks.<sup>12</sup>
- 2.26 DSD told the Committee that it continues to attract and retain talented staff by focusing on the provision of a work environment that offers continuous professional development, opportunities for career diversity or specialisation, and a clear link between work outputs and mission success.<sup>13</sup>
- 2.27 The Committee heard from at least one agency that while its recruitment goals were very successful in the early years of its growth because it

---

9 *Classified Transcript*, 25 March 2011, p. 22.

10 *Classified Transcript*, 25 March 2011, p. 28.

11 *ASIO Unclassified Submission*, No. 4, p. 13.

12 *ONA Classified Submission*, No. 7, p. 9.

13 *DSD Classified Submission*, No. 9, p. 12.

sought a broad set of job skills, in 2009-10 recruitment success has become more difficult because the skill sets the agency now seeks are much narrower and therefore, in a tight and competitive labour market, people with those skill sets are highly sought after.<sup>14</sup>

- 2.28 Competition in a tight labour market notwithstanding, the Committee is satisfied that each of the agencies continues to devote the necessary resources to ensure that their future recruitment needs have the best chance of being met.

### Workplace diversity

- 2.29 As for the previous year, all three Defence agencies demonstrated to the Committee that they are committed to the principles of equity and diversity. DSD, for example, had eight equity advisers within the organisation during 2009-10 and no complaints were made during this period.<sup>15</sup>

- 2.30 The three non-Defence agencies also demonstrated their commitment to equity and diversity in the workplace. ASIS told the Committee it maintains a Workplace Diversity Policy which adopts the spirit of Section 18 of the *Public Service Act 1999*. The policy encourages employees to reach their full potential in a workplace that welcomes a diversity of personal styles, ideas, solutions and innovation.<sup>16</sup> ONA told the Committee that it continues to support and recognise the diversity of people within the agency through the implementation of its disability action plan, workplace diversity program and development of its reconciliation action plan.<sup>17</sup> Similarly, ASIO has implemented recruitment and people management strategies intended to create an inclusive working environment that recognises and utilises the diversity of the workforce, while seeking to recruit a range of people that reflect the Australian community as much as is practical. ASIO noted that its staffing profile compares favourably with that of the broader Australian Public Service.<sup>18</sup>

---

14 *Classified Transcript*, 25 March 2011, p. 14.

15 *DSD Classified Submission*, No. 9, p. 11.

16 *ASIS Classified Submission*, No. 6, p. 19.

17 *ONA Classified Submission*, No. 7, p. 22.

18 *ASIO Unclassified Submission*, No. 4, p. 50.

## Training and development

- 2.31 All the AIC agencies demonstrated to the Committee that they continue to invest heavily in training and development of staff.
- 2.32 Commencing in January 2010, ASIO implemented an enhanced approach to training and developing intelligence professionals. The new approach supports greater engagement with partner agencies, academia, and the private sector. It also increases the level of skill and competence upon graduation and provides access to modules for non-intelligence officer staff working in related areas.<sup>19</sup>
- 2.33 Since 1 July 2009, the responsibility for general professional development training for staff from all three Defence intelligence agencies rests with the consolidated Defence I&S Group agency.<sup>20</sup>
- 2.34 DSD told the Committee that it actively participates in National Intelligence Community (NIC) Training programs to increase awareness of NIC capabilities. Within DSD, 275 staff attended the NIC Orientation Program during 2009-10. Additionally, 22 DSD executive level staff attended the NIC Senior Officers' Course in 2009-10. This program gives participants an understanding of whole-of-government approaches to intelligence needs and provides a more advanced discussion on requirements and liaison opportunities.<sup>21</sup>

## Linguistic skills

- 2.35 For most AIC agencies linguistic capability is critical and finding and retaining staff with appropriate language skills is a vital aspect of workforce planning. Agencies draw from a variety of sources to recruit and train staff. Various language training facilities were discussed with the Committee as were strategies used by the agencies to ensure they maintain suitable linguistic capability.
- 2.36 The Committee received detailed classified evidence on the importance that appropriate linguistic skills play in operational capabilities within the AIC.

---

19 *ASIO Unclassified Submission*, No. 4, p. 30.

20 *DSD Classified Submission*, No. 9, p. 15.

21 *DSD Classified Submission*, No. 9, p. 16.

## Separation rates and retention strategies

### Separation rates

- 2.37 The average separation rate across the Australian Public Service (APS) for 2009-10 was 6.5 per cent.<sup>22</sup> However, the Committee heard that this relatively low separation rate is not necessarily desirable for all organisations within the AIC. While some organisations within the AIC are actively working to lower their separation rates, one of the smaller agencies considers a separation rate well in double figures to be right for it in order to keep 'people moving through [the agency]'. The agency told the Committee that 'otherwise you can become calcified very easily [and thus the organisation aims] to get the right mix between continuity and change.'<sup>23</sup> Another intelligence agency told the Committee that it aims to achieve a retention rate of around 10 per cent in order 'to keep the organisation vibrant and healthy and growing.'<sup>24</sup>
- 2.38 The average separation rate during this period for the three Defence intelligence agencies was 7.0 per cent.<sup>25</sup>
- 2.39 DSD has actively worked to lower its separation rate and informed the Committee that in 2009-10, the most cited reasons for individuals leaving DSD included following a spouse in a new job, increased family responsibilities, and undertaking study or seeking a change in career/lifestyle. Separations cited as 'other' showed a downward trend from 17.3 per cent in 2007-08 to 9.6 per cent in 2009-10. DSD found that the increase in staff leaving for the private sector may be attributable in part to external factors such as changes in the job market. Specifically, it seems likely that the continued strength of the Australian economy and employment market provides more competition for DSD.<sup>26</sup>
- 2.40 ASIO's separation rate for 2009-10 increased to five per cent compared with 4.5 per cent in the previous year. ASIO offers separating staff the opportunity to participate in a voluntary exit interview to help ASIO

---

22 Australian Public Service Commission, *State of the Service Report, State of the Service Series 2009-10*, Australian Public Service Commission, Canberra, 2010, viewed 28 May 2011, <<http://www.apsc.gov.au/stateoftheservice/0910/index.html>>.

23 *Classified Transcript*, 25 March 2011, p. 34.

24 *Classified Transcript*, 25 March 2011, p. 41.

25 *Classified Transcript*, 25 March 2011, p. 40.

26 *DSD Classified Submission*, No. 9, p. 15.

identify reasons for departure and to address concerns requiring a management response.<sup>27</sup>

- 2.41 Within intelligence agencies, it is believed that there is a higher separation rate among intelligence officers than among technical officers and, therefore, assessment agencies will demonstrate a higher separation rate than agencies which have a high technical personnel component.<sup>28</sup>

## Retention strategies

- 2.42 The Committee took evidence from all agencies regarding their retention strategies and the resources they commit to these strategies.
- 2.43 DSD told the Committee that it has directed considerable resources to recruit and retain the right people. One of the initiatives that DSD has implemented is to broadband advancement through a Unified Structure to retain staff with critical technical and specialist skills. This provides employees with the opportunity of advancing from one level to the next within a broadband if they can successfully demonstrate that they meet certain advancement requirements.<sup>29</sup>
- 2.44 ASIO is developing Human Capital Framework programs and initiatives such as career management, leadership development and a contemporary employment framework to facilitate the retention of its staff.<sup>30</sup>

## Security issues

- 2.45 All intelligence agencies provide their staff with initial and on-going security training. For example, all new DSD staff attend an *Introduction to Security* seminar within the first three months of their commencement and, following initial training, DSD provides ongoing security training for all staff with its *Security Refresher* seminar. It is mandatory for all staff to attend the refresher at least once every two years.<sup>31</sup> All other agencies have similar security training programmes.
- 2.46 The Committee discussed with the relevant intelligence agency an internal breach of procedures by an individual which had occurred during the

---

27 ASIO Unclassified Submission, No. 4, p. 58.

28 Classified Transcript, 25 March 2011, p. 41.

29 DSD Classified Submission, No. 9, p. 13.

30 ASIO Unclassified Submission, No. 4, p. 58.

31 DSD Classified Submission, No. 9, p. 17.

reporting period. After some discussion about the ensuing investigation and remedial action the Committee was satisfied that the investigation into the breach was handled in a timely and appropriate manner. This was the only internal security breach within the AIC during the reporting period.<sup>32</sup>

## Cyber security

- 2.47 Electronic interference is a growing security concern for all AIC agencies. The agencies described to the Committee a range of risk mitigation strategies which are being used to protect their systems from cyber attacks.
- 2.48 Following a recommendation in the 2009 *Defence White Paper*, the Cyber Security Operations Centre (CSOC) was established within DSD in late 2009. This is a multi-agency initiative to coordinate work against growing e-security threats. Personnel from ASIO, the Attorney-General's Department and the Australian Federal Police work in the Centre with DSD to identify developing cyber threats to critical infrastructure and determine appropriate responses.
- 2.49 ASIO told the Committee that maintaining information technology systems that have the necessary controls and security to communicate at the TOP SECRET level is expensive, both in the cost of security and the associated resource costs in people:
- Considerable personnel, security infrastructure and policy is required, which can present a significant barrier to new members of the national security community in building and maintaining these capabilities.<sup>33</sup>
- 2.50 The Committee is satisfied that all AIC agencies are taking the necessary steps to address cyber security concerns within each organisation. Cyber security is further addressed in Chapter 4.

## Security clearances

- 2.51 The process of completing security clearances for newly recruited personnel continues to consume large amounts of time and resources for AIC agencies. Average vetting times lead to significant delays between candidates being interviewed and commencing work. This delay impacts

---

32 *Classified Transcript*, 25 March 2011, p. 42.

33 *ASIO Unclassified Submission*, No. 4, p. 39.

the agencies' ability to accurately predict start dates for candidates and good candidates are frequently lost to other employment as a result.

- 2.52 In 2009-10, the Defence intelligence agencies worked towards the implementation of recommendations made by the IGIS following the *Inquiry into the Organisational Suitability Assessment* policy and procedures. Implementing the recommendations had implications for how the agencies carry out their security clearances and during 2009-10 agencies were adjusting their procedures in order to implement the recommendations. In some cases adjusting to the new procedures meant a slight increase in processing time.
- 2.53 The Committee explored the reasons why some of the intelligence agencies continue to do their own security vetting rather than join the new joint vetting agency. The Committee heard that the agencies which continue to do their own vetting also assess the candidate's suitability to hold the particular role when the security assessment is made:
- It is very difficult to separate those judgments and assessments throughout that process. For that reason, it was not appropriate to outsource the security vetting role for the intelligence service.<sup>34</sup>
- 2.54 The Committee heard that although the vetting process is lengthy by nature, agencies are looking at ways that vetting could be done better and they hope to see some improvements in the process during the next year.<sup>35</sup> Changes may include, as mentioned above, taking a more collaborative approach to security vetting by some of the AIC agencies. Benefits envisaged of a collaborative approach may include shortening the time vetting takes without diminishing the quality of vetting.<sup>36</sup>

## Visa Security Assessments

- 2.55 Any person applying for a visa to travel to, or remain in Australia may have the application referred by the Department of Immigration and Citizenship (DIAC) to ASIO for a Security Assessment.
- 2.56 In 2009-10, ASIO completed 38,438 visa Security Assessments including 989 assessments for protection visa applicants.<sup>37</sup> During this period, ASIO issued adverse Security Assessments for nineteen individuals seeking entry to Australia. Fourteen of these adverse assessments were issued on

---

34 *Classified Transcript*, 25 March 2011, p. 18.

35 *Classified Transcript*, 25 March 2011, p. 28.

36 *Classified Transcript*, 25 March 2011, p. 29.

37 *ASIO Unclassified Submission*, No. 4, p. 16.

counter-terrorism grounds and five were issued on espionage or foreign interference grounds.<sup>38</sup>

2.57 In most visa categories, a visa may not be issued (or must be cancelled) where ASIO determines the applicant to be directly or indirectly a risk to 'security' (as defined in the ASIO Act).<sup>39</sup>

2.58 The Committee received submissions from several refugee and asylum seeker advocacy groups. Representatives of some advocacy groups gave evidence to the Committee at the public hearing. All advocacy groups acknowledged the importance of the visa security assessment process<sup>40 41</sup> but they also raised their concerns about the process, including:

- the length of time being taken by ASIO to conduct visa security assessments for refugees and asylum seekers;
- that there is no obvious reason why the process being applied to visitors who seek refugee status could not be applied to asylum seekers who are currently subject to indefinite mandatory detention;<sup>42</sup>
- concern that because ASIO is prioritising assessments of people in detention, this results in further delays for asylum seekers who are living in the community;<sup>43</sup>
- that people who have had an 'incredibly prolonged and very negative detention experience' and are eventually found to be owed protection will take into the community mental health issues which 'are going to undermine their capacity to be a productive people within Australia.'<sup>44</sup>
- that there are inappropriately long periods between DIAC granting refugee status and ASIO completing the Visa Security assessment;<sup>45</sup>
- that there should be a means of risk assessing those who are least likely to prove problematic, with a view to getting them out of detention much faster;<sup>46</sup>

---

38 ASIO *Unclassified Submission*, No. 4, p. 16.

39 ASIO *Unclassified Submission*, No. 4, p. 40.

40 *Refugee Council of Australia Submission*, No. 14, p. 1.

41 Ms P Curr, Asylum Seeker Resource Centre, *Transcript*, 16 June 2011, p. 10.

42 *Refugee Council of Australia Submission*, No. 14, p. 2.

43 *Refugee Council of Australia Submission*, No. 14, p. 2.

44 Ms S Caton, Refugee Council of Australia, *Transcript*, 16 June 2011, p. 4.

45 *R.I.S.E. Submission*, No. 13, p. 3.

46 *The Asylum Seeker Resource Centre Submission*, No. 11, pp. 1-2.



- that ASIO's assessment processes are not transparent and asylum seekers who receive adverse security assessments often do not know why an adverse decision was made;<sup>47</sup>
- that full disclosure by ASIO of the non-statutory criteria it uses in undertaking visa security assessments would be in the interest of 'consistency, transparency and to ensure that findings are free from bias and error';<sup>48</sup>
- that there is no right of appeal to the Administrative Appeals Tribunal for non-citizens who receive adverse visa security assessments;<sup>49 50</sup>
- that ASIO does not always return important documents belonging to the asylum seekers<sup>51</sup>, and
- that the allocation of resourcing of visa security assessments may not be sufficient to ensure that assessments are done in a timely way.<sup>52</sup>

2.59 ASIO told the Committee that during 2009-10, managing visa security assessments for the increased number of people coming to Australia via Christmas Island has been a 'particular challenge' for the organisation. In 2008-09 ASIO carried-out two hundred security assessments on people arriving in Australia seeking protected visas but in 2009-10 the figure jumped to nearly 3,000. This sharp increase has placed ASIO under considerable 'resource pressure' and ASIO outlined to the Committee a number of steps it has taken to address the situation, including improved processes.<sup>53</sup>

2.60 ASIO told the Committee that it works closely with DIAC:

... to prioritise caseloads, with an emphasis on detention cases (including Irregular Maritime Arrivals (IMAs)) and compassionate or compelling cases, including identified by DIAC as vulnerable.<sup>54</sup>

2.61 In 2009-10, ASIO diverted significant resources to undertake security assessments of IMAs for DIAC. Consequently, the resources available to assess protection visa and other refugee referrals were limited and this caseload experienced delays. ASIO said that it continues to work very

47 Ms B Arthur, *Brigidine Asylum Seekers Project Submission*, No. 12, p. 1.

48 *R.I.S.E. Submission*, No. 13, p. 10.

49 *The Asylum Seeker Resource Centre Submission*, No. 11, p. 3.

50 Ms S Caton, *Refugee Council of Australia, Transcript*, 16 June 2011, p. 2.

51 Dr D Vigneswaran, *Affiliate R.I.S.E., Transcript*, 16 June 2011, p. 6.

52 Ms P Curr, *Asylum Seeker Resource Centre, Transcript*, 16 June 2011, p. 13.

53 *Classified Transcript*, 25 March 2011, pp. 1-3.

54 *ASIO Unclassified Submission*, No. 4, p. 42.

closely with DIAC to ensure visibility of the overall visa security assessment caseload and agreed priorities.<sup>55</sup>

- 2.62 ASIO told the Committee that any person applying for a visa to travel to, or remain in, Australia may have the application referred by DIAC to ASIO for a Security Assessment:

Given the large volume of visa applications, it is not practical for each one to be assessed by ASIO. A risk managed referral framework has, therefore, been developed so that applications more likely to be of concern are drawn to ASIO's attention. Still, ASIO assesses many thousands of visa applications annually.

In most visa categories, a visa may not be issued (or must be cancelled) where ASIO determines the applicant to be directly or indirectly a risk to 'security' (as defined in the ASIO Act). The enabling legislation in this instance is the Migration Act 1958, specifically the Migration Regulations 1994 and public interest criterion 4002.

Separately to visa application referrals from DIAC, ASIO's security intelligence investigations will from time to time determine that the holder of a valid visa to Australia (who is sometimes already in Australia, and other times overseas) presents a risk to Australia's security. In such circumstances ASIO may provide to the Minister for Immigration and Citizenship an adverse Security Assessment, which would lead the Minister to cancel the visa.<sup>56</sup>

- 2.63 At the private hearing ASIO told the Committee that to 'do assessments properly, they require considerable time and effort.'<sup>57</sup> ASIO explained to the Committee that security assessments take as long as they will take and cannot be speeded up or have a statutory timeframe put on them. If an IMA comes onshore in Australia without identifying documentation and gives one story to a DIAC officer and another story to ASIO these stories must, in ASIO's words, be 'de-conflicted'.
- 2.64 The Committee is advised that IMAs regularly throw identity documents overboard making the job of ASIO more difficult.
- 2.65 The process of de-conflicting stories without the ability to refer to documents such as identity card or passports can make the security assessment process a lengthy one.
- 

55 *ASIO Unclassified Submission*, No. 4, p. 42.

56 *ASIO Unclassified Submission*, No. 4, p. 40.

57 *Classified Transcript*, 25 March 2011, p. 2.

2.66 Regarding the number of people currently waiting for a visa security assessment, the Director-General told the Committee that:

... at the present time there are about 6,000 irregular maritime arrivals in some form of detention, be it detention within the community or otherwise. Of that number, currently ... there are 522 people awaiting a security assessment ... [including] some people who have been awaiting an assessment for a very long time. The reason for that is partly that over the previous 18 months – certainly prior to the beginning of March this year – ASIO was doing its security assessments according to priorities set for it by DIAC. Those priorities were being set ... with the objective of trying to move as many people out of detention as possible.<sup>58</sup>

2.67 The Committee asked ASIO for their response to concerns about withheld original documentation. ASIO told the Committee that it 'does not request or take possession of documents belonging to Irregular Maritime Arrivals. On occasion, Irregular Maritime Arrivals have offered ASIO photocopies of documentation.'<sup>59</sup>

2.68 Although outside the 2009-10 scope of the inquiry, the Committee notes that with effect from 1 March 2011 ASIO introduced a risk-managed intelligence-led framework for security assessments. Application of the framework has caused significant changes to the process. Now ASIO does not begin to assess people until DIAC advises that they have reached a category called '1a met', meaning that they are in the process to qualify for refugee status. This will avoid spending time assessing people who were not going to be granted refugee status. Also, with the risk-managed approach, ASIO is able to focus on the more complex cases which require full investigation. Many of the 522 cases mentioned above are complex cases from the previous year and, ASIO told the Committee, it now has the ability to focus a very substantial part of its resources on those complex cases.<sup>60</sup>

2.69 Since introducing the new risk management referral framework, all arrivals are still subject to some form of assessment but most occur very quickly.<sup>61</sup>

---

58 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 14.

59 Private correspondence from ASIO to the Committee.

60 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 14.

61 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 15.

2.70 When asked by the Committee why ASIO cannot meet the Government's objective of completing all security assessments within three months, Mr Irvine told the Committee that:

The first reason throughout most of last year was the sheer number and the requirement to conduct a full investigation into every individual who was not a minor during that process. Once that issue was resolved with a much more risk management based process, we are still confronted with the same sorts of issues that we had to address last year. The first has been the identity issue. The fact is that people do need some form of identity document to have got to Malaysia or Indonesia in most cases, before they come to Australia, but they do not arrive with them. This creates a whole series of issues for us. Secondly, ... information provided is not always accurate or truthful on some occasions and that sort of thing needs to be checked.<sup>62</sup>

2.71 Regarding suggestions taken in evidence that ASIO 'conducts its security checks and makes its assessments based on information provided by the government of the country from which that immigrant has come,'<sup>63</sup> Mr Irvine said that he can give a categorical assurance that:

... ASIO's policy, in accordance with government policy and with Australia's international obligations, does not refer the names of individuals who have sought asylum in Australia to the host government. We just do not do it. So our decisions are not, therefore, made on the basis of information provided about an individual from the host government.<sup>64</sup>

2.72 The Director-General of ASIO responded to a question about the adequacy of the resources it directs to the visa security assessment process, saying:

There is a real tension between the resources I would love to have to put on to this process and the number of qualified people that I have to do it. Some people will say "just get the government to give you more money and you can go out and recruit more people and they can rush off and do it". The security assessment discipline requires very extensive training, and I am very confident and personally convinced that, whatever their age – and the demographic of ASIO is that, because we have grown so quickly, we have a lot of young people in ASIO – the degree of

---

62 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 15.

63 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 15.

64 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 16.

training that we put people through to qualify them to conduct this sort of security interview process will contribute significantly to the integrity of that process. Yes, sure, they work under pressure, they have to get through a lot of cases and so on, but I am confident that what we are doing we are doing well and under appropriate conditions.<sup>65</sup>

2.73 The Inspector-General of Intelligence and Security (IGIS) told the Committee that, during 2009-10, she saw a significant increase in the number of complaints from members of the public who were concerned about 'the timeliness with which ASIO processes security assessments in relation to visa applications.' The IGIS received '... a total of 1015 new complaints about security assessments in 2009-10, compared to 153 in 2008-09.'<sup>66</sup>

2.74 The IGIS is not able to direct ASIO to change the priority of a case, or make the process quicker for a particular applicant but the IGIS can look at individual complaints to see whether they indicate systemic problems. The IGIS told the Committee that:

We continue to have discussions with senior ASIO staff about its approach to security assessments for persons in this situation and have looked at ASIO's handling of a large number of these security assessments. In considering these assessments we have found no evidence that ASIO had acted in anything other than a proper and legal manner.<sup>67</sup>

2.75 Several advocacy groups noted that non-citizens who receive adverse visa security assessments do not have a right of appeal to the Administrative Appeals Tribunal (AAT). The Committee is aware that in 1998-1999, the IGIS recommended to the Attorney-General:

... that the government introduce legislation to provide a determinative review process for refugee applicants where appropriate Australian authorities find that the applicants have a well-founded fear of persecution if returned to their country of origin.<sup>68</sup>

---

65 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 19.

66 *Inspector General of Intelligence and Security Submission*, No. 1, p. 2.

67 *Inspector General of Intelligence and Security Submission*, No. 1, p. 3.

68 Inspector-General of Intelligence and Security, *Annual Report 1998-99*, <[http://www.igis.gov.au/annual\\_report/98-99/asio.cfm](http://www.igis.gov.au/annual_report/98-99/asio.cfm)>.

- 2.76 In the 2006-07 Annual Report of the IGIS, Mr Ian Carnell reiterated the recommendation made by his predecessor in 1999.<sup>69</sup>
- 2.77 Whilst not expressing a view on the IGIS' recommendation, the Committee is of the opinion that it is timely for the Independent National Security Legislation Monitor to examine the recommendation made by the IGIS in 1999 and again in 2007, subject to having adequate resources.
- 2.78 At the public hearing, the Director-General of ASIO was asked about resource implications should non-citizens be granted right of appeal to the AAT if they receive an adverse security assessment. The Director-General said he thought that 'there would be significant resource implications'.<sup>70</sup>
- 2.79 The Committee notes the request by some advocacy groups for ASIO to declare its non-statutory criteria for making visa security assessments. The Committee believes that making non-statutory criteria publicly available could have an adverse effect on national security and therefore does not support this suggestion.
- 2.80 The Committee notes that since the previous Administration and Expenditure inquiry, ASIO's visa security assessment workload has increased significantly. Processes for doing visa security assessments have been placed under considerable strain and, in some cases, assessments have taken longer to do than is desirable.
- 2.81 The Committee also notes that advocacy groups which are dissatisfied with ASIO's processes can contact the Independent National Security Legislation Monitor.
- 2.82 The Committee notes that the IGIS has stated that ASIO is doing its job in a "proper and legal manner".<sup>71</sup>
- 2.83 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.

---

69 Inspector-General of Intelligence and Security, *Annual Report 2006-07*, p.12.

70 Mr D Irvine, Director-General of ASIO, *Transcript*, 16 June 2011, p. 17.

71 *Inspector General of Intelligence and Security Submission*, No. 1, p. 3.

## ASIO personnel Security Assessments

- 2.84 ASIO undertakes personnel security assessments at the request of other Australian Public Service agencies to determine if an individual can have access to national security classified material.
- 2.85 ASIO completed 22,343 personnel Security Assessments in 2009-10. Among these, ASIO issued one adverse and one qualified personnel Security Assessment.<sup>72</sup>
- 2.86 The majority of ASIO's Security Assessments are resolved based on material provided by the requesting agency. If there are issues of potential security concern, ASIO undertakes further investigative actions.<sup>73</sup>

## Counter-terrorism security assessments

- 2.87 ASIO conducts counter-terrorism checks at the request of AusCheck and the Australian Federal Police. In 2009-10, ASIO completed 98,086 counter-terrorism Security Assessments. Ninety-nine per cent of these were completed in five days.<sup>74</sup>

## Breaches of security

- 2.88 All agencies assured the Committee that they continue to foster and maintain very strong security cultures within their organisations. Organisational security plans provide strategies to mitigate security risks and provide frameworks for staff to practice sound security in daily business. ONA, for example, reported to the Committee that it participates in inter-agency security-related forums, and implements changes based on revised security guides and bulletins issued by the forums. Additionally, in order to further reduce the number of security breaches, it has introduced a new security breach policy.<sup>75</sup>
- 2.89 DSD told the Committee that it continually monitors internal infringement trends to assess and target security training needs and maintain an appropriate security culture.<sup>76</sup>
- 2.90 ASIO noted that its security policies meet or exceed the standards laid down in the Australian Government Protective Security Policy

---

72 ASIO *Unclassified Submission*, No. 4, p. 43.

73 ASIO *Unclassified Submission*, No. 4, p. 43.

74 ASIO *Unclassified Submission*, No. 4, p. 44.

75 ONA *Classified Submission*, No. 7, p. 35-36.

76 DSD *Classified Submission*, No. 9, p. 22.

Framework. Its *Security Plan 2009-12* and *Security Breach Policy* provide strategies to mitigate security risks and provide a framework for staff to ensure that sound security is practiced in daily business. ASIO's senior executive is briefed on security breaches every quarter, and senior managers are notified of breaches occurring within their divisions and branches.<sup>77</sup>

- 2.91 All other agencies reported that their policies also meet or exceed the standards laid down in the Australian Government Protective Security Policy Framework.
- 2.92 Agencies discussed with the Committee where security breaches had occurred and what remedial action was taken. The Committee is satisfied that breaches of security, where they occurred during 2009-10, were properly investigated and appropriate remedial action was taken.

## Staff surveys

- 2.93 All the AIC agencies conduct staff surveys annually or biennially. During the reporting period surveys were used to capture key drivers and overall levels of employee engagement in the agencies. Most agencies reported that they performed above the Australian benchmark average for overall staff/agency engagement. Some described changes to the Committee which had been or will be implemented in response to findings from staff surveys during 2009-10.
- 2.94 DSD told the Committee that its staff survey was administered online and, after presentation to the DSD Executive, results were presented to all staff. The DSD survey consisted of 57 core questions, split across 11 categories. There was an option for anonymity and free-text space for additional comments. DSD achieved a response rate of 69.4 per cent and an overall engagement rate of 47 per cent.<sup>78</sup> DSD reported to the Committee that when benchmarked against Australian Central Government Agencies it is performing above average across all survey categories. However, it noted opportunities to improve in the areas of change management, career development and learning and development.<sup>79</sup>
- 2.95 ONA engages external consultants at least every two years to conduct a staff attitudinal survey to measure corporate health and how staff
- 

<sup>77</sup> ASIO *Unclassified Submission*, No. 4, p. 38.

<sup>78</sup> The Australian benchmark average is 36 per cent.

<sup>79</sup> DSD *Classified Submission*, No. 9, p. 19.



members think ONA is performing across a range of areas. ONA's most recent survey was conducted in November 2010 which, although outside the reporting period of 2009-10, enabled ONA to report to the Committee that results indicated that 80 per cent of ONA employees are fully engaged and 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'.<sup>80</sup>

## Accommodation

### ASIO's new central office

- 2.96 As at 30 June 2010, the base building architectural design work had been completed for ASIO's new central office on Constitution Avenue in Parkes, Canberra. At this time, the fit-out design was 85 per cent complete and so was the excavation work.
- 2.97 Construction of the building commenced in September 2009 with construction of levels one, two and three well underway at the end of the reporting period.
- 2.98 During 2010-11, construction activity will include the completion of the erection of the facade and continuation of the interior fit-out. At the time of writing their submission, ASIO reported that construction was progressing on schedule for the building to be handed over to ASIO in mid-2012, with the main relocation of ASIO staff to commence from late 2012.
- 2.99 The building is being designed and constructed in partnership with the Department of Finance and Deregulation (Finance). ASIO told the Committee that close financial management against the project schedule by ASIO and Finance (through a jointly chaired Steering Committee), has ensured that the project is proceeding on time and within budget and scope. However, given the nature of the security environment and the pace of technological change, it is inevitable that additional capabilities will need to be added to the new building to maintain ASIO's capacity to provide sound advice to Government on issues of national security.<sup>81</sup>

---

80 *ONA Classified Submission*, No. 7, p. 25-26.

81 *ASIO Unclassified Submission*, No. 4, p. 59.

## Other agencies

- 2.100 Each agency updated the Committee on accommodation issues. In some cases accommodation is satisfactory, in other cases agencies are finding that they are reaching capacity in accommodation terms. Agencies described the strategies being adopted to solve accommodation pressures where they exist.
- 2.101 ONA reported that it was planning to move into new premises in June 2011. It entered into a lease based on a market commercial rent with the Industry Superannuation Property Trust (ISPT) for the former Patent Office at 2 National Circuit, Barton. ISPT was fully refurbishing the heritage building in accordance with a conservation management plan. Following some unexpected delays which were outside ONA's control or responsibility, at the time of speaking to the Committee, the estimated completion date was June 2011.<sup>82</sup>
- 2.102 ONA expects its new offices to 'provide significant environmental benefits for ONA'. Design efforts met the 4.5 star National Australian Built Energy Rating System mandated by the Energy Efficiency in Government Operations policy.<sup>83</sup>
- 2.103 DSD told the Committee that its workforce expansion has placed significant pressure on its accommodation. DSD informed the Committee about its management of these accommodation issues.<sup>84</sup>

## Performance management and evaluation

- 2.104 Each agency within the AIC demonstrated to the Committee that performance management and evaluation, both at the organisational level and at the level of individual employees is a key element of strategic planning and organisational growth.

## Organisational performance management

- 2.105 During 2009-10, ASIO made changes to its internal performance reporting mechanisms. According to ASIO these changes:

---

82 *ONA Classified Submission, No. 7, p. 33.*

83 *ONA Classified Submission, No. 7, p. 34.*

84 *DSD Classified Submission, No. 9, p. 7.*

... have provided the Organisation with an improved tool to measure its performance against pre-determined benchmarks. The new reporting format captures performance indicators, outcomes and risks centrally, which has resulted in more focused discussion and pro-active decision-making by ASIO's Corporate Executive.<sup>85</sup>

- 2.106 ONA reported to the Committee that its system for regularly reviewing organisational performance has been useful in identifying resource and skills gaps as well as assessing other performance-related factors.<sup>86</sup>

## Individual performance management

- 2.107 During 2009-10 ASIO formulated its Human Capital Framework which 'integrates all people functions into a single, strategic system directed specifically at building people capability rather than a discrete set of fragmented administrative processes'.<sup>87</sup>
- 2.108 DSD told the Committee that management and leadership capability development remains of high importance to DSD. In 2009-10, the organisation continued to invest in leadership and management development through the Executive Leadership Development Program and Middle Management Development Program. Both programmes are conducted for staff in the Defence I&S Group.<sup>88</sup>
- 2.109 All ONA staff members participated in ONA's Performance Development Framework (PDF) during 2009-10. The PDF focuses on each individual's role, specific priorities and broader behaviour and capability expectations consistent with the APS Integrated Leadership System. ONA told the Committee that each employee and their manager are required to meet and discuss priorities for the year ahead, and to document their agreement. The PDF requires participation in biannual performance reviews and a rating process which determines annual remuneration outcomes for individual employees.<sup>89</sup>

---

85 *ASIO Unclassified Submission*, No. 4, p. 29.

86 *ONA Classified Submission*, No. 7, p. 5.

87 *ASIO Unclassified Submission*, No. 4, p. 31.

88 *DSD Classified Submission*, No. 9, p. 16.

89 *ONA Classified Submission*, No. 7, p. 20-21.

## Issues raised by the IGIS

2.110 In her submission to the Committee, the IGIS raised two issues relating to ASIO: complaints about the timeliness of ASIO visa security assessments and archives-related complaints.<sup>90</sup> The timeliness of ASIO visa security assessments was discussed above under the sub-heading *Visa Security Assessments*. Archives-related complaints are discussed below.

### Archives-related complaints

- 2.111 The IGIS told the Committee that to assist with general monitoring of ASIO's overall archives performance, the Director-General of Security provides IGIS with quarterly progress reports.
- 2.112 The IGIS ran an inquiry into an archive related matter which concerned the adequacy or otherwise of the transfer of historical cinefilm records to VHS cassette format and the subsequent destruction of the original cinefilm in the early 1990s. The inquiry confirmed that the storage arrangements were inadequate and are contributing to the degradation and destruction of the cinefilm. To minimise further damage, ASIO undertook to relocate the film to an appropriate location, in negotiation with the National Archives of Australia. This relocation was delayed and at 30 June 2010 the cinefilm remained in inappropriate storage conditions. However, the IGIS was notified that the transfer of the film was completed in December 2010.<sup>91</sup> The issue concerning archive-related complaints has therefore been satisfactorily resolved.
- 2.113 The IGIS had no further issues to raise with the Committee relating to the Administration and Expenditure of the AIC agencies during the period 2009-10.

## Conclusions

- 2.114 Extensive organisational growth and change over the last few years has presented challenges to all AIC agencies but the Committee is satisfied that all agencies are overseeing their administrative functions satisfactorily and mostly to a high standard.

---

90 Inspector General of Intelligence and Security, *Submission* No. 1.

91 Inspector General of Intelligence and Security, *Submission* No. 1, p. 3.

- 
- 2.115 Recruitment continues to be a high priority and a resource intensive activity for the AIC. Attracting staff of high calibre with the necessary skill sets is difficult and resource intensive but the agencies demonstrated to the Committee that each continues to seek new and/or better ways of approaching this challenge.
- 2.116 AIC agencies continue to invest heavily in the training and development of their staff and the Committee believes that new approaches supporting improved engagement between AIC agencies, academia and the private sector are appropriate. The Committee will examine the results of this engagement in its next Administration and Expenditure Review.
- 2.117 The Committee notes that two issues were raised by the IGIS in relation to ASIO, and is satisfied that both are being or have been addressed.
- 2.118 The Committee is satisfied that overall the administration of the six intelligence and security agencies is currently sound.



## Expenditure

- 3.1 The Committee has a statutory obligation to review the financial statements of all six AIC agencies. All agencies, except ASIO provided the Committee with a copy of their financial statements. ASIO's financial statements are publicly available and the Committee sourced these from ASIO's *Report to Parliament 2009-2010*.
- 3.2 As most of the evidence taken from the intelligence agencies at the hearings was of a classified nature, the following is a broad overview of the Committee's findings relating to the expenditure of the agencies.

### **The efficiency dividend**

- 3.3 During its report *Review of Administration and Expenditure: Australian Intelligence Organisations, Number 8* it became clear to the Committee that issues relating to the efficiency dividend and its impact on agencies outside of the AIC apply equally to smaller agencies within the AIC. The Committee recommended that the Australian Government review the potential adverse effects of the efficiency dividend on the AIC having particular regard to the Joint Committee of Public Accounts and Audit report *The efficiency dividend and small agencies: Size does matter*.
- 3.4 The concerns raised during the Committee's *Review of Administration and Expenditure: Australian Intelligence Organisations, Number 8* were specifically raised in the evidence the Committee took for the current review. This is extremely concerning to the Committee. The Committee will continue to monitor the impact of the Efficiency Dividend on the Australian Intelligence Community.

- 3.5 The Government responded to recommendation contained in its Administration and Expenditure No. 8 report, tabled on 21 June 2010, on 22 September 2011. Whilst the Committee understands that the 2010 Federal Election would have caused some delay in replying to its previous report, a delay of over 12 months is unacceptable.
- 3.6 The Committee reiterates its recommendation that the Australian Government review the potential adverse effects of the efficiency dividend on the Australian Intelligence Community, having particular regard to the Joint Committee of Public Accounts and Audit report *The efficiency dividend and small agencies: Size does matter*.<sup>1</sup> In addition the Committee notes that this Government response contained elements of concern that the Committee will be discussing.

## Submission from the ANAO

- 3.7 The Committee relies to a large extent on the advice it receives from the ANAO when it assesses the financial health of the AIC agencies. The Auditor-General responded to the Committee's request to make a submission to the inquiry, reporting on the results of the ANAO audits of the 2009-10 financial statements of the intelligence agencies.
- 3.8 The ANAO conducts an annual audit of the internal systems and key financial controls of each organisation. In the case of the Defence agencies, they are audited as part of the overall Defence financial statement audit.
- 3.9 In ANAO's submission, the results of the audits for the Defence agencies as a group and the three other individual agencies were discussed. ANAO raised issues for two of the individual agencies.

## Budget Growth

### Agencies other than ASIO

- 3.10 Of the agencies other than ASIO, two received a significant increase in their budget for 2009-10 with the other three receiving modest increases.

---

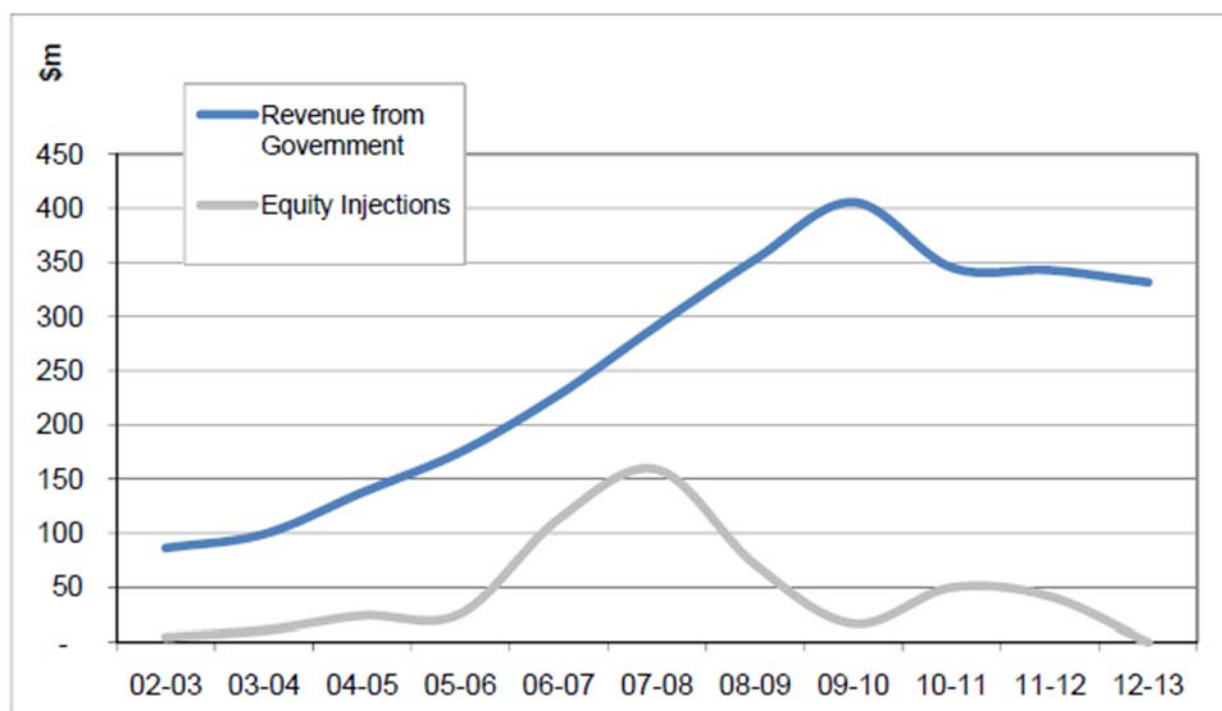
1 Parliamentary Joint Committee of Public Accounts and Audit, *The efficiency dividends and small agencies: Size does matter*, 4 December 2008.



## ASIO<sup>2</sup>

- 3.11 Funding to ASIO in terms of total price of program expenses was \$368m, an increase of five per cent from the total cost in 2008–09 of \$352m. The estimated total cost for program expenses for 2010–11 is \$413m, an increase of twelve per cent from 2009–10.
- 3.12 Revenue from Government in 2009–10 increased 15 per cent to \$406m, while revenue from independent sources (such as for services rendered) was similar to the 2008–09 figure of \$10m.
- 3.13 This reporting period saw the last year of growth arising from the *Review of ASIO Resourcing*.
- 3.14 Separately, ASIO received an equity injection of \$16m for 2009–10, to fund telecommunications interception capabilities (\$2m) and capability enhancements (\$14m).
- 3.15 A further equity injection will be received in 2010–11 of \$89m. This provides funding for asset replacement (\$28m) and for ASIO's new building project (\$61m).

Figure 3.1 ASIO Revenue from Government, 2002 – 2013



Source: ASIO Unclassified Submission, page 19.

## Recruitment costs

- 3.16 The costs to agencies for recruitment have been steadily increasing in line with increasing recruitment. Advertising and security clearance costs continue to account for a large portion of recruitment budgets.
- 3.17 During the reporting period, recruitment media planning, coupled with online media assisted ASIO to attract and source suitable applicants. ASIO's expenditure on recruitment advertising decreased from \$1.962m in 2008-09 to \$1.250m in 2009-10.<sup>3</sup>
- 3.18 As is expected security clearance costs continue to be a significant part of recruitment costs for agencies. The process takes agencies between three and nine months to complete and is resource intensive. The Committee accepts that this is necessary to ensure the suitability of applicants to work in a National Security environment.

3 ASIO Unclassified Submission, No. 4, p. 47.

## Training costs

- 3.19 Expenditure on training, both corporate and operational, comprises a significant portion of each agencies budget.
- 3.20 Each agency provided the Committee with its costs for training. In contrast to the period 2008-09, there have been very significant increases in training costs for 2009-10 in some cases.

## Financial governance systems

- 3.21 Each agency has its own internal audit committee. The functions of internal audit committees and the key issues that they addressed in the period under review were set out in the submissions. Typically, such committees comprise the Director or Director-General; one or two Assistant Directors or Assistant Directors-General; Chief Finance Officer and/or Director of Finance; and a representative from the ANAO with other staff members invited as required. Audit Committees generally meet quarterly, or more frequently if required.
- 3.22 In 2009/10 ASIO's Audit and Evaluation Committee was chaired by the Deputy Director-General and includes a representative from the ANAO.
- 3.23 Submissions also listed a range of other resource management committees in place within agencies to manage and monitor expenditure.
- 3.24 In 2009-10 ASIO completed fourteen internal audits which were the subject of classified reporting to ASIO's Audit and Evaluation Committee. No loss of public monies was reported in these audits and recommendations for improvements with the exception of one, which was rejected on a sound operational basis and agreed to by the Committee and Internal Audit, have been accepted through the Audit and Evaluation Committee and responsible work areas.<sup>4</sup>

## Fraud control and risk management

- 3.25 Section 45 of the *Financial Management and Accountability Act 1997* (FMA Act) requires the chief executive of an agency to implement a fraud control plan:

---

4 ASIO Unclassified Submission, No. 4, p 29.

A Chief Executive must implement a fraud control plan for the Agency. For this purpose, fraud includes fraud by persons outside the Agency in relation to activities of the Agency.<sup>5</sup>

- 3.26 Agencies noted their compliance with this requirement in their submissions.

## Conclusions

- 3.27 Together with assurances from the Australian National Audit Office, the Committee was satisfied, within the limits provided to it by the *Intelligence Services Act 2001*, that all the agencies are appropriately managing the expenditure of their organisations.

---

5 *Financial Management and Accountability Act 1997*, Part 7—Special responsibilities of Chief Executives, Section 45 Fraud control plan.

## Interoperability

- 4.1 In his National Security Statement to the Parliament of Australia the then Prime Minister of Australia the Hon. Kevin Rudd MP stated that:

I believe that Australia's national security community is highly effective and has proven highly adaptable. But in an increasingly complex and interconnected security environment, we need a more integrated national security structure that enhances national security policy coordination.<sup>1</sup>

- 4.2 Following this statement the Counter-Terrorism White Paper stated that:

Australia's counter-terrorism efforts are intelligence-led and focused on prevention. This approach hinges on strong partnerships and cooperation at the national level, effective engagement at the international level, and effective information sharing. Over recent years, there has been significant growth in Australia's security, intelligence and law enforcement agencies and the Government has taken steps to improve their capabilities and enhance information sharing. The establishment of the National Intelligence Coordination Committee has ensured that Australia's intelligence effort, both domestically and internationally, is better integrated into the new national security arrangements. The creation of a new Counter-Terrorism Control Centre will also ensure that we better integrate our overall counter-terrorism intelligence capabilities.<sup>2</sup>

---

1 The Hon Kevin Rudd MP, *First National Security Statement to the Parliament*, Department of the Prime Minister and Cabinet, Canberra, 4 December 2008, viewed on 19 April 2011, <<http://prrudd.archive.dpmc.gov.au/node/5424>>.

2 *Counter-Terrorism White Paper, Securing Australia, Protecting Our Community*, Department of the Prime Minister and Cabinet, Canberra, February 2010, viewed on 19 April 2011, <[http://www.dpmc.gov.au/publications/counter\\_terrorism/exec\\_summary.cfm](http://www.dpmc.gov.au/publications/counter_terrorism/exec_summary.cfm)>.

- 4.3 Given these statements the Committee thought it timely to ask that the AIC report to it on issues of interoperability.
- 4.4 The Committee asked that a separate section of each of the AIC agencies submissions address some or all of the following:
- Areas of interoperability between the AIC and any other Department or Agency;
  - Any e-security arrangements underpinning this interoperability;
  - Memorandum of Understandings providing the basis for interoperability;
  - Accommodation requirements;
  - Public relations and/or public reporting requirements as result of interoperability arrangements;
  - Direction and strategic planning underpinning interoperability;
  - How interoperability is being managed administratively;
  - How interoperability is being managed financially;
  - The effects of interoperability on performance management and evaluation;
  - The effects of interoperability on recruitment and training; and
  - Costs and benefit analysis of interoperability.
- 4.5 All of the agencies included information on interoperability in their submissions to the Committee. Given that issues relating to interoperability go directly to the operational priorities and practices of the agencies evidence to the Committee on interoperability is overwhelmingly classified SECRET and cannot be referred to in this report.
- 4.6 The Committee therefore outlines some of the publicly reportable information on the interoperability of the AIC.

## **The National Intelligence Coordination Committee**

- 4.7 The National Intelligence Coordination Committee (NICC) is chaired by the National Security Adviser and comprises the heads of the Office of National Assessments, the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate, the AFP, the Australian Crime Commission, and Customs and Border Protection. The departments of Defence, Foreign Affairs and Trade, Immigration and Citizenship, and Attorney-General's are also represented at the Deputy Secretary level.

- 4.8 The NICC enhances the ability of Australia's security agencies to share information, coordinate effort and identify opportunities to improve the whole-of-government response to terrorism and other national security challenges.
- 4.9 The NICC oversees the operations of two sub-committees: the National Intelligence Collection Management Committee (NICMC) and the National Intelligence Open Source Committee (NIOSC). Both of these committees are chaired by ONA.

### **The National Intelligence Collection Management Committee**

- 4.10 The NICMC is responsible for setting specific requirements and evaluating collection effort against each of the National Intelligence Priorities set by the government.

### **The National Intelligence Open Source Committee**

- 4.11 The NIOSC is responsible for enhancing the coordination and capabilities of the National Intelligence Community's open source efforts. Open source collection is considered the first information source for meeting the government's intelligence and security requirements.

### **The National Threat Assessment Centre**

- 4.12 The multi-agency National Threat Assessment Centre (NTAC) is located within ASIO and assesses intelligence and information from a wide range of sources to prepare threat assessments in relation to specific people, places, and events. These assessments inform the risk management decisions made by operational agencies, the implementation of protective security measures and the travel advisories regarding potential threats when travelling overseas that are prepared by the Department of Foreign Affairs and Trade for the Australian public. ASIO also provides protective security advice to Australian Government agencies and, with the approval of the Attorney-General, to state and territory governments and private sector companies to protect vulnerable facilities.

## National Interception Technical Assistance Centre

- 4.13 ASIO gave evidence to the Committee that it is working in partnership with the AFP and other Commonwealth agencies to provide coordinated technical assistance to other Australian intercepting agencies.
- 4.14 In 2010-11 ASIO will conduct a pilot study for the establishment of a National Interception Technical Assistance Centre (NiTAC). The NiTAC is planned to provide a central point of reference from which agencies can receive technical assistance to help keep pace with the rate and scale of technical change.

## The Cyber Security Operations Centre

- 4.15 The Cyber Security Operations Centre (CSOC) is a Defence Signals Directorate capability that serves all government agencies.
- 4.16 The CSOC has two main roles:
- it provides government with a comprehensive understanding of cyber threats against Australian interests; and
  - it coordinates operational responses to cyber events of national importance across government and critical infrastructure.
- 4.17 The CSOC serves all government agencies and has embedded representation from a number of other agencies involved in assessing the threat to, and the protection of, Australian interests from sophisticated threat actors. The CSOC will also assist CERT Australia<sup>3</sup>, in the Attorney-General's Department, to support industry that owns or manages critical infrastructure.

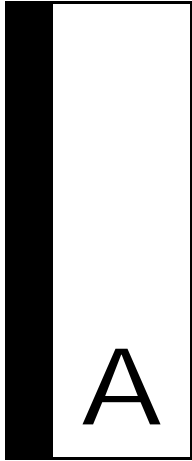
## Conclusions

- 4.18 The Committee was pleased with the level of information given to it in relation to interoperability and will continue to monitor this area to ensure that interoperability management and budgetary structures are in place across the AIC.

---

3 Australia's official national computer emergency response team.

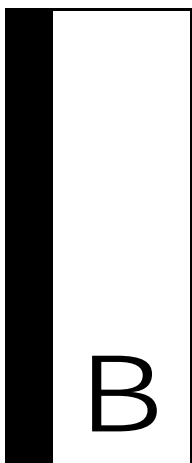




## Appendix A – List of Submissions

1. Inspector-General of Intelligence and Security (Unclassified)
2. Australian National Audit Office (Audit-in-Confidence)
3. Confidential submission
4. Australian Security Intelligence Organisation (Unclassified)
5. Australian Security Intelligence Organisation (Secret)
6. Australian Secret Intelligence Service (Secret)
7. Office of National Assessments (Restricted)
8. Defence Intelligence Organisation (Secret)
9. Defence Signals Directorate (Secret)
10. Defence Imagery and Geospatial Organisation (Secret)
11. Asylum Seeker Resource Centre
12. Brigidine Asylum Seekers Project
13. R.I.S.E. – Refugees Survivors & Ex-Detainees
14. Refugee Council of Australia
15. Australian Secret Intelligence Service – Answers to Questions on Notice (Secret)





## Appendix B – Witnesses appearing at hearings

### Private hearing

Canberra

Friday, 25 March 2011

#### **Australian Security Intelligence Organisation**

Mr David Irvine, Director-General of Security

Mr David Fricker, Deputy Director-General

First Assistant Director-General, Corporate Capability Services

First Assistant Director-General, Security, Strategy and Engagement

#### **Australian Secret Intelligence Service**

Mr Nick Warner PSM, Director-General

Deputy Director-General, Corporate

Deputy Director-General, Operations

#### **Office of National Assessments**

Mr Allan Gyngell, Director-General

Mr Derryl Triffett, Assistant Director-General, Corporate and IT Services

**Defence Signals Directorate, Defence Intelligence Organisation and Defence Imagery and Geospatial Organisation**

Mr Stephen Merchant, Deputy Secretary for Intelligence and Security, Department of Defence

Mr Ian McKenzie, Director, DSD

MAJGEN Richard Wilson, Director, DIO

Mr Steve Meekin, Director, DIGO

**Public hearing**

**Canberra**

Thursday, 16 June 2011

**Refugee Council of Australia**

Ms Sonia Caton, Member

**R.I.S.E (Refugees, Survivors and Ex-Detainees)**

Dr Bala Vigneswaran, Affiliate

Mr Arasa Ratnakanthan, Affiliate

**Asylum Seeker Resource Centre**

Ms Pamela Curr, Campaign Coordinator

**Australian Security Intelligence Organisation**

Mr David Irvine, Director-General of Security