

**INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY**

ANNUAL REPORT 2002-2003

© Commonwealth of Australia 2003

ISBN 0-646-42867-5

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without permission from AusInfo. Requests and inquiries concerning reproduction and rights should be addressed to the Manager, Legislative Services, AusInfo, GPO Box 1920, Canberra ACT 2601.

Printed by Pirion Printers Pty Ltd, Fyshwick, ACT.

GLOSSARY OF ACRONYMS USED IN THIS REPORT

AIC	Australian Intelligence Community
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ATI	Authority to Investigate
AUSTRAC	Australian Transaction Reports and Analysis Centre
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DSD	Defence Signals Directorate
IGIS	Inspector-General of Intelligence and Security
ISA	Intelligence Services Act
MOU	Memorandum of Understanding
ONA	Office of National Assessments
PM&C	Department of the Prime Minister and Cabinet

TABLE OF CONTENTS

	PAGE
LETTER OF TRANSMITTAL	iii
GLOSSARY OF ACRONYMS USED IN THIS REPORT	iv
TABLE OF CONTENTS	v
ROLE OF THE INSPECTOR-GENERAL	7
THE YEAR IN REVIEW	8
OVERVIEW	8
LEGISLATION	8
INSPECTIONS, COMPLAINTS AND INQUIRIES	10
EXTERNAL PROFILE	11
PERFORMANCE	13
PERFORMANCE INDICATORS	13
TIMELINESS	13
ACCEPTANCE OF RECOMMENDATIONS	14
RESPONSIVENESS TO ISSUES RAISED IN INSPECTIONS	14
LEVEL OF ASSURANCE	14
AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION	16
WHAT ASIO DOES	16
AWARD TO DIRECTOR-GENERAL	16
INSPECTION ACTIVITIES	16
COMPLAINTS AND INQUIRIES	24
AUSTRALIAN SECRET INTELLIGENCE SERVICE	27
WHAT ASIS DOES	27
SENIOR APPOINTMENTS	27
INSPECTION ACTIVITIES	28
COMPLAINTS AND INQUIRIES	30
DEFENCE SIGNALS DIRECTORATE	33
WHAT DSD DOES	33
SENIOR APPOINTMENTS	33
INSPECTION ACTIVITIES	33
TRAINING ACTIVITIES	37
COMPLAINTS AND INQUIRIES	37

DEFENCE IMAGERY AND GEOSPATIAL ORGANISATION	39
WHAT DIGO DOES	39
SENIOR APPOINTMENTS	39
ACCOUNTABILITY ARRANGEMENTS	39
INSPECTION ACTIVITIES	40
COMPLAINTS AND INQUIRIES	40
DEFENCE INTELLIGENCE ORGANISATION	41
WHAT DIO DOES	41
ACCOUNTABILITY ARRANGEMENTS	41
COMPLAINTS AND INQUIRIES	41
OFFICE OF NATIONAL ASSESSMENTS	43
WHAT ONA DOES	43
ACCOUNTABILITY ARRANGEMENTS	43
COMPLAINTS AND INQUIRIES	43
THE YEAR 2003-2004 IN PROSPECT	44
INSPECTION ACTIVITY	44
INQUIRIES	46
INTERNATIONAL	46
MANAGEMENT OF THE OFFICE	47
FINANCIAL STATEMENTS	50
IGIS CONTACT INFORMATION	65
ANNEX 1 - COMPLAINT AND INQUIRY STATISTICS	66
ANNEX 2 - BALI INQUIRY REPORT	69
ANNEX 3- REPORT INTO ALLEGATIONS THAT DSD INTERCEPTED COMMUNICATIONS OF THE HON LAURIE BRERETON MP	74
ANNEX 4 - FUNCTIONS, POWERS AND FREEDOMS OF INTERNATIONAL OVERSIGHT MECHANISMS	84

ROLE OF THE INSPECTOR-GENERAL

1. The Inspector-General of Intelligence and Security (IGIS) helps the ministers responsible for the following agencies to oversee and review their activities:

- Australian Security Intelligence Organisation (ASIO);
- Australian Secret Intelligence Service (ASIS);
- Defence Signals Directorate (DSD);
- Defence Imagery and Geospatial Organisation (DIGO);
- Defence Intelligence Organisation (DIO); and
- Office of National Assessments (ONA).

2. The purpose of this oversight and review is to ensure that the agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights.

3. The office was established by the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) on 1 February 1987.

4. The Inspector-General can undertake an inquiry into the activities of an agency in response to a complaint or a reference from a minister. The Inspector-General can also act independently to initiate inquiries and conducts regular inspections and monitoring of agency activities.

5. In conducting an inquiry, the Inspector-General has significant powers which include requiring the attendance of witnesses, taking sworn evidence, copying and retention of documents and entry into an agency's premises. The Inspector-General can also conduct preliminary inquiries into matters in order to decide whether to initiate a full inquiry.

6. Further information about the role and functions of the Inspector-General can be found at <http://www.igis.gov.au>.

THE YEAR IN REVIEW

OVERVIEW

7. During 2002-03 Australia's intelligence and security agencies continued to increase their efforts against global terrorism and other intelligence-related targets.

8. This heightened effort demanded, particularly in the wake of the terrorist attack in Bali in October 2002, continued attention to the possible involvement of Australian persons in terrorist activity, either from within Australia or overseas.

9. In the course of my inspection and inquiry work, however, I observed no diminution in the agencies' adherence to appropriate standards of legality, propriety and respect for human rights.

LEGISLATION

ASIO Act

10. The Parliament passed amendments to the ASIO Act to empower ASIO to obtain warrants for the detention and questioning of people reasonably believed to be able to provide important information relating to terrorism.

11. The amendments include several relating to the role of the Inspector-General:

- the Director-General of Security must make a statement of procedures to be followed in the exercise of warrants and before doing so must consult the Inspector-General;
- the legislation does not affect the exercise of any powers or functions of the Inspector-General under the IGIS Act;
- a detainee must be able to contact the Inspector-General, a warrant must specify the Inspector-General as someone whom the detainee is permitted to contact and the prescribed authority (the person who oversees the questioning) must inform the detainee of his or her right to complain to the Inspector-General, either orally or in writing, about ASIO;
- a detainee must be provided with facilities to complain to the Inspector-General;
- the Inspector-General may be present when a person is taken into custody or questioned;
- if the Inspector-General is concerned about impropriety or illegality in connection with the exercise of powers in relation to a person specified in a warrant, the Inspector-General may inform the prescribed authority, who must consider the

Inspector-General's concern and may give directions, such as requiring suspension of questioning, until the Inspector-General's concern has been satisfactorily addressed. If the concern cannot be satisfactorily addressed within the remaining period of detention, the prescribed authority may direct the release of the detainee;

- the Inspector-General must inspect material relating to multiple warrants and must report the results in the IGIS annual report; and
- the Director-General must as soon as practicable give the Inspector-General:
 - a copy of any draft request to the Attorney-General seeking consent to request a warrant;
 - a copy of the warrant;
 - a copy of video recordings of questioning, etc required under the legislation; and
 - statements detailing any seizure, taking into custody or detention and any action taken in response to concerns expressed by the Inspector-General.

12. The Director-General has informed me that, in addition to the statutory procedures, ASIO will put in place measures to ensure that the Inspector-General has adequate advance notice of any proposals to exercise the powers provided under the legislation.

Intelligence Services Act

13. The first full year of operation of the Intelligence Services Act saw ASIS and DSD further develop the internal checks and balances designed to improve compliance with the requirements of the Act designed to safeguard the privacy of Australian persons.

14. We continued working with both agencies, both by assisting with development of guidelines and other compliance-related processes, and by participating in training activities conducted within the agencies.

15. The Act provides (at section 14) that a staff member of an agency is not subject to civil or criminal liability for certain acts that might otherwise attract liability, provided the act is done in the proper performance of a function of the agency.

16. A further provision empowers the Inspector-General to certify in writing facts relevant to whether an act was done in the proper performance of the agency's functions. Such certificates are prima facie evidence for the purposes of proceedings.

17. It was necessary, following passage of the Act, to develop protocols to ensure that, in the event of any claim for immunity under the legislation, there would be an appropriate mechanism, involving consultation with the

Inspector-General, to enable law enforcement agencies to consider the legitimacy of the claim.

18. Considerable progress was made with the protocols during the reporting period and it should be possible to finalise them in the first half of 2003-04.

19. As mentioned in last year's report, experience with the Act and the privacy rules has revealed some deficiencies and unintended consequences that should be rectified by legislative amendment in due course. As the second anniversary of the Act's passage approaches it would be timely to review its operation to develop a package of such amendments.

Inspector-General of Intelligence and Security Act

20. There were no amendments to the IGIS Act during the reporting period. I have, however, suggested some minor amendments for inclusion in a bill when convenient.

INSPECTIONS, COMPLAINTS AND INQUIRIES

Inspections

21. As in previous years, inspection of the activities of the collection agencies (ASIO, ASIS, DSD and DIGO) has occupied the bulk of the effort of the office.

22. We visit each of these agencies regularly to inspect operational records, to check that their activities are conducted with propriety and comply with the law.

23. In the case of ASIS and DSD we also access their classified reporting and some other records electronically from computer terminals in our office.

24. Details of inspection activities are in the chapters of this report that deal with the individual agencies.

Complaints

25. The number of new complaints continued the upward trend noted in recent years. There were 29 new complaints leading to preliminary or full inquiries (26 in 2001-02) and 32 new complaints nominating a specific agency that were dealt with without the need for inquiry action (27 in 2001-02).

Bali inquiry

26. I provided the Prime Minister with a report on whether there was any intelligence that warned of the terrorist bombing in Bali. A copy of the introduction and summary of the report is at Annex 2 to this annual report.

DSD inquiry - alleged bugging of politician

27. Following media allegations I conducted an inquiry into whether DSD intercepted the communications of The Hon Laurie Brereton MP. The inquiry report is reproduced at Annex 3 to this annual report.

ASIO searches

28. There were a number of complaints on behalf of people whose premises were searched under warrants issued by the Attorney-General. Details of the inquiries relating to these are in the chapter on ASIO.

Defence Force complainant

29. An inquiry into the concerns of a serving member of the Defence Force about matters related to DIO, referred by a former Minister for Defence, was completed during the year and I provided a report to the minister.

Asylum seeker compensation

30. The 1999-2000 report provided details of an inquiry into a complaint from an asylum seeker where I expected to recommend compensation. The complainant's lawyer finally submitted a detailed claim in June 2003 and as a result I expected to complete the matter early in the new reporting year.

EXTERNAL PROFILE

Commonwealth Parliament

31. I attended hearings of, and gave evidence to the Senate Finance and Public Administration Legislation Committee examining the budget estimates and the Parliamentary Joint Committee on ASIO, ASIS and DSD.

Media

32. There was media interest in several matters involving the Inspector-General, such as the Bali inquiry, the inquiry into alleged bugging of Mr Brereton's office and the execution of ASIO search warrants.

33. Our practice in such cases is not to confirm or deny the existence of a complaint, or to discuss the particulars of inquiries beyond process issues such as expected time frames for completion and the formal requirements of the IGIS Act.

Internet presence

34. The IGIS website (<http://www.igis.gov.au>) provides information about the office, including copies of previous annual reports and occasional statements about current activities.

35. We receive numerous inquiries about the work of the office via the electronic mail facility (info@igis.gov.au).

36. There is also a continuing upward trend in its use by complainants, both for initial contact and correspondence about the progress of complaints. We will correspond with complainants via e-mail, but will not include classified information in e-mails.

International

37. There was no meeting of international intelligence and security oversight bodies this year as the next is scheduled for 2004.

38. The United Kingdom's Intelligence Services Committee however, visited Australia in October 2002. In the course of the visit we consulted about our respective inquiries into the Bali bombing.

39. I also corresponded with some overseas counterparts about possible cooperation in relation to matters affecting each others' citizens.

40. Other countries have oversight bodies with different powers and responsibilities from the Australian Inspector-General. With the permission of the United Kingdom committee, Annex 4 to this report is an adaptation of a chart prepared for the committee, which provides a comparative analysis of the functions, powers and freedoms of oversight mechanisms in the United States, Canada, Australia, New Zealand, South Africa and the United Kingdom.

PERFORMANCE

PERFORMANCE INDICATORS

41. The effectiveness of the office may be assessed against a range of quantitative and qualitative performance indicators, including:

- the time taken to deal with complaints and conclude inquiries;
- acceptance by ministers and agency heads of recommendations arising from inquiries;
- positive responses from agencies to issues we raise arising from inspection activities; and
- the level of assurance I can give that the agencies are conducting their activities legally, with propriety, and with regard to human rights.

TIMELINESS

Statistics

42. At the start of the reporting period 6 inquiries or preliminary inquiries remained open. These comprised a ministerial referral regarding the activities of DIO, a complaint about ASIS and 4 complaints about ASIO. All were concluded during the reporting period.

43. In addition, there were 70 approaches from people with new or continuing complaints against a nominated agency (60 in 2001-02).

44. These comprised:

- 29 new complaints leading to preliminary or full inquiries (26 in 2001-02). They are listed at Annex 1, table 1. Ten remained open at the end of the reporting period;
- 9 approaches seeking review of previous complaints (7 in 2001-02); and
- 32 new complaints nominating an agency that were dealt with without the need for inquiry action (27 in 2001-02). They are listed at Annex 1, table 2.

45. We try to respond to the latter immediately or within a few days at most. One such contact remained to be dealt with at the end of the reporting period, but was finalised early in the next reporting period.

46. In addition, 78 people contacted the office with concerns of a generic or non-specific nature, also not requiring inquiry action.

47. We do not have specific target times for completing preliminary or formal inquiries because we often need input from people whom we cannot require to provide responses within our preferred time limits.

48. In the five years between 1 July 1998 and 30 June 2003, the average time taken on each such inquiry was 103.45 days, while the average times taken in 2001-2002 and 2002-2003 were 72.9 days and 123.5 days respectively.

49. This does not necessarily, however, say anything about effort on the part of this office compared to previous years. Resolution of inquiries is also influenced by factors such as:

- the complexity and range of issues raised;
- the immediacy of the matters to be inquired into;
- the accessibility of necessary information;
- locating persons with knowledge of the matters being inquired into; and
- the need to observe the formal processes set out in the IGIS Act.

50. The office's capacity to further reduce the time it takes to conclude its investigations will continue to depend on the complexity of the cases that come to our attention and the responsiveness of others, as well as our own efficiency.

ACCEPTANCE OF RECOMMENDATIONS

51. It is very rare for an agency to reject recommendations of the Inspector-General. All recommendations made by the Inspector-General in this reporting year were accepted.

RESPONSIVENESS TO ISSUES RAISED IN INSPECTIONS

52. During and following inspection visits to each of the collection agencies, I made a number of suggestions on how procedures could be streamlined or improved. These suggestions were generally accepted and acted upon. In cases where they were not, I accepted that there were good reasons for not doing so.

53. The intelligence and security agencies continued to seek my views on draft policies and procedures where issues of propriety and/or legality arose, or were likely to arise.

54. The willingness of the agencies to seek and accept input from my office demonstrates a genuine commitment on their part to conduct their activities legally and with propriety.

LEVEL OF ASSURANCE

Increasing number of complaints

55. The number of new complaints to the office has increased over the last few reporting periods. Several external factors are likely to have played a part in this.

56. Terrorist attacks such as occurred in the United States on 11 September 2001 and in Bali in October 2002, require greatly increased investigative effort by the intelligence community, with consequent impacts on the wider community.

57. In the immediate aftermath of the Bali bombings, for example, ASIO sought and obtained a number of entry and search warrants. The execution of these warrants led to a number of complaints that have required individual investigation.

58. Secondly, there have been some inquiries by the Inspector-General that have received considerable media attention. The level of community consciousness of the office's existence and role is, therefore, higher than in previous times.

Summary

59. During the reporting period I found some instances where the agencies acted beyond their authority. These are described in the chapters of this report that deal with each agency individually.

60. In summary, however, I have come across no evidence that the intelligence and security agencies, or individual members of the agencies, have knowingly acted, or wish to act, beyond their authority.

61. I am also satisfied that there is no evidence of enduring systemic deficiencies that would lead to breaches of propriety, the law, or the human rights of Australians.

62. I consider that the Australian public can be confident that the intelligence and security agencies continue to be:

- focussed on achieving the objectives set for them by the Parliament and government;
- responsive to ministerial direction;
- aware of the limits of their authority;
- concerned to conduct their business in a professional manner; and
- fully accountable for their actions via the various oversight mechanisms that apply to them.

AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION

WHAT ASIO DOES

63. The Australian Security Intelligence Organisation is Australia's security service. Its functions are set out in the *Australian Security Intelligence Organisation Act 1979*. It is also subject to guidelines issued by the Attorney-General.

64. ASIO's main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's security. It is not a law enforcement agency.

65. The focus of ASIO's work is on terrorism, people who may act violently for political reasons, and people who may clandestinely obtain sensitive government information or otherwise harm Australia's interests in order to further their own causes or the interests of foreign governments.

66. ASIO does not investigate lawful protest activity or engage in surveillance of ordinary members of the community going about their normal business. It has to obtain specific ministerial authority for use of its most intrusive powers, such as telecommunications interception and listening devices.

67. Other ASIO functions include collecting foreign intelligence in Australia, and providing security assessments and protective security advice.

68. Further information about ASIO, the Attorney-General's guidelines and the *Australian Security Intelligence Organisation Act 1979*, can be found on ASIO's Internet homepage located at <http://www.asio.gov.au>.

AWARD TO DIRECTOR-GENERAL

69. The Director-General of Security, Mr Dennis Richardson, was awarded an AO in the 2003 Queen's Birthday Honours list in recognition of his outstanding public service in a variety of portfolios over many years. I congratulate Mr Richardson on this award.

INSPECTION ACTIVITIES

Context of ASIO activities

70. The terrorist attacks of 11 September 2001 vividly demonstrated to the wider community the lethal threat posed by individuals and groups who are committed to using violent means to achieve their objectives.

71. The need for more active intelligence collection was reinforced, if this was necessary, by the terrorist outrage that occurred in Bali on 12 October 2002.

72. Australian involvement in armed conflict in the Persian Gulf and various military deployments elsewhere has also contributed to the increasingly complex security environment in which Australia now finds itself.

73. ASIO's response to these developments has of necessity led to a significant increase in its operational activities.

74. While the majority of ASIO's activities are hidden from view and are therefore unlikely to attract public attention, some, such as the overt execution of entry and search warrants, will inevitably bring attention to the Organisation.

75. It is perhaps not surprising that the public profile of ASIO has been greater in the past 12 months than at almost any time in its existence.

Scope and reporting arrangements

76. As ASIO is principally a national security agency, it is the agency most likely to come into contact with members of the Australian public. There are therefore more, and a wider range of, activities that require ongoing review by the Inspector-General than there are with other agencies.

77. During the reporting period, we inspected the following categories of ASIO activity:

- warrant operations;
- records of operations carried out under authorities to investigate;
- access to, and use of, information obtained from the Australian Transaction Reports and Analysis Centre and the Australian Taxation Office;
- provision of information to, and liaison with, law enforcement agencies;
- the official use of alternative documentation to support assumed identities; and
- compliance with the Archives Act.

78. The Director-General and I have agreed that if any concerns or matters worthy of comment arise during inspection activities, my staff or I will normally discuss them with an appropriate senior manager or liaison officer in the first instance.

79. Following each inspection I write to the Director-General outlining the pertinent issues. In each case ASIO has provided a considered response.

80. The Director-General and I have also agreed procedures to apply if I form the view that any matters arising from an inspection need to be brought to the attention of the Attorney-General or the Prime Minister. As in previous years no such matters arose during the 2002-2003 reporting period.

Warrant operations – procedures

81. The Attorney-General issues warrants to ASIO authorising the use of special powers such as intercepting telecommunications, using listening devices, entering and searching premises, intercepting mail, using tracking devices and remotely accessing computers.

82. We visit ASIO's central office approximately every eight weeks, and state offices as the opportunity arises, to inspect documentation associated with current or recently concluded warrant operations.

83. To ensure that ASIO does not seek warrants without proper justification, thorough planning and appropriate consideration at various levels of approval, we check ASIO's files for documents showing:

- the intelligence or security case that ASIO has made in support of the application;
- that the people named in warrants are in fact those of interest to ASIO;
- that appropriate internal approvals for the request have been obtained;
- the persons to whom the Director-General has given authority to execute the warrant or to communicate information obtained from a warrant;
- the Attorney-General's approval, when obtained;
- reports to the Attorney-General of the outcome of executed warrants; and
- that the activity concerned did not begin before, or continue after, the period approved by the Attorney-General.

84. In the course of our rolling visits programme we aim to inspect documentation for all warrants issued.

85. During the reporting period we reviewed a large number of warrant operation files several times, in order to be satisfied that ASIO prepared reports of the outcomes and provided them to the Attorney-General within the requisite time.

86. In each case we were satisfied that ASIO had:

- reasonable grounds for seeking a warrant - our experience is that the Director-General only seeks warrants when there are sound operational requirements for their use and the information cannot be obtained by less intrusive means;
- provided sufficient information for the Attorney-General to make an informed decision - the Director-General personally signs each request to the Attorney-General for issue of a warrant and the Attorney-General's Department provides separate legal advice to the Attorney in relation to each request;
- appropriate procedures in place to check that the conditions of the warrant were being fulfilled;

- reported the results of warrant operations to the Attorney-General in a balanced and timely manner; and
- maintained the key accountability documents on the relevant files.

Unauthorised telephone interception

87. We noted three instances of inadvertent unauthorised telephone interception caused by human error. This compares with five during the 2001-2002 reporting period. Details are as follows:

- Since warrants expire after six months, in some cases it is necessary to seek renewal of a warrant, with the new warrant timed to begin on expiry of the old. For various reasons, however, there may sometimes be a gap between the two, in which case ASIO ceases collection until the new warrant comes into operation. In the case in question, despite ASIO taking all reasonable precautions to remove all target numbers from coverage during this gap period, one number escaped being disconnected. No intercept obtained from this number in the gap period was processed and ASIO took appropriate steps to minimise the risk of any repetition.
- Shortly after renewal of a warrant a subscriber had a target service disconnected, following which the carrier reallocated the number. ASIO did not become aware of this for several weeks, during which time a significant number of dialling events were collected but not processed due to their short duration. Upon realising that the target service had been reallocated ASIO immediately ceased its coverage, destroyed all intercepted material, informed the Attorney-General, and had the relevant warrant revoked; and
- In another case the subscriber had a service disconnected before the relevant warrant lapsed. ASIO inadvertently reconnected this service to its collection system when the warrants for some related services were renewed shortly afterwards. ASIO, however, picked up the error before the service provider could reallocate the service, so no unauthorised intercept was received. The officers involved were counselled to be more vigilant in the future. I accepted that the error was inadvertent and endorsed the remedial action taken as appropriate.

Search warrants

88. ASIO conducted a number of overt searches of premises under warrant authority during the reporting period.

89. Several of these searches led to complaints to this office. A description of these matters is provided under the inquiries and complaints section elsewhere in this chapter.

Foreign translators

90. During the reporting period I asked ASIO to explain the rationale for using foreign assistance in two operations, and to sight the undertakings these

officers were required to complete in respect of the handling of processed material relating to Australian persons.

91. In each instance the Director-General of Security provided detailed responses and copies of the signed undertakings. I found these responses to be satisfactory.

Transcription errors

92. During the reporting period we noted two instances of errors on the face of warrants.

93. In the first instance, shortly after intercept began being processed it became apparent that the name on the warrant was a mixture of the name of the target identity and that of a relative living at the same residence.

94. ASIO immediately ceased collection and conducted urgent research to separately identify the two people.

95. Following this the faulty warrant was revoked, and ASIO sought new warrants to separately target both identities. I endorsed the corrective action taken by ASIO in this case.

96. In the other instance we noticed that the number of a warrant submitted to the Attorney-General for signature did not correlate to the associated warrant request number.

97. Although this clerical error is minor, I have asked ASIO to examine the effect of this error on the validity of the warrant.

Minor procedural matters

98. Several minor procedural issues also came to notice during inspections, mainly relating to the absence of some accountability documents. In each case the missing documents were quickly located and presented for review.

99. Given the increasing number of warrants that have been sought in recent years, the incidence of error is low.

Authorities to investigate - procedures

100. The authority to investigate (ATI) process involves applications by ASIO staff to more senior officers for authority to conduct investigations in relation to people or organisations.

101. We regularly inspect the records of the ATI consideration process and the files recording the resulting investigative activity.

102. During the reporting period we examined files relating to every ATI issued in ASIO's central office and a selection of those issued in ASIO's other offices.

Authorities to investigate – results of inspections

103. As with warrant operations, detailed public discussion of specific cases is not possible but comment follows in general terms upon several cases reviewed during the reporting period.

104. In one case we queried a particular ATI, which we considered was expressed in too general terms. As there was no question about the appropriateness of the proposed investigation, we suggested that it should be authorised at a higher level within the Organisation, via a different approvals mechanism.

105. In another case the purpose of an ATI was not clear from the description provided in the 'Objectives of Investigation' field on the relevant form. We sought and obtained a full briefing on the investigation, receiving satisfactory responses to all our queries.

106. We also raised a number of more minor procedural issues associated with the raising and approval of ATIs.

107. Last year's annual report commented that the quality of ATIs had improved during that reporting period. This trend continued during the 2002-2003 reporting period.

108. On the basis of our inspections, ASIO's responses to the various questions we posed and the responses of senior management to our comments, I consider that the ATI regime is operating to ensure that ASIO only conducts investigations that are properly justifiable by reference to its statutory functions.

109. I am confident that the arrangements strike an appropriate balance between the operational needs of ASIO and the need to protect people's privacy.

ASIO and law enforcement agencies

110. The increased focus on terrorism during the reporting period necessarily involved close cooperation between ASIO and law enforcement agencies.

111. As has been described elsewhere in this report, ASIO required the assistance of various federal and state law enforcement bodies in the course of executing a number of entry and search warrants. We received a number of complaints flowing from these joint operations.

112. The resultant inquiries revealed some systemic issues, one of which was the need for clearer definition of the respective roles and responsibilities of ASIO and the police forces when acting under the authority of search warrants issued to ASIO. I intend pursuing this matter further in the 2003-2004 reporting year.

113. More generally, during our periodic visits to ASIO regional offices we examine ASIO's records of exchanges of information with local law enforcement agencies.

114. We found these records to be properly maintained and sufficiently detailed for us to conclude that the exchange of information that occurs does not exceed what is necessary for the performance of the functions of the organisations concerned.

AUSTRAC and the Australian Taxation Office

115. The *Financial Transactions Reports Act 1988* and the *Taxation Administration Act 1953* provide for ASIO to obtain information from the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Taxation Office, in strictly prescribed circumstances.

116. The procedures involved in ASIO accessing financial transaction reports and taxation information are set out in memoranda of understanding (MOUs) between the respective parties.

117. The Inspector-General of Intelligence and Security and the Director of AUSTRAC have also entered into a MOU covering oversight issues and the Inspector-General provides an annual report to the Attorney-General on ASIO's compliance with its obligations.

118. We regularly review ASIO's access to financial transaction reports and it is apparent from this that ASIO is complying with the requirements of the MOU between itself and AUSTRAC.

119. ASIO has formal internal procedures for approving access to AUSTRAC information similar to those applying to ATIs. They require ASIO investigators who need information about financial transactions to obtain approval from senior officers. Interrogation of the databases is not undertaken by the investigator who requires the information but by an officer specially authorised and trained for the task. Under the memorandum of understanding between ASIO and AUSTRAC the maximum number of authorised officers at any one time is twelve.

120. The procedures require that, before access is approved, the entity under investigation also be the subject of an ATI.

121. We also review instances of ASIO obtaining access to taxation records and its compliance. It is apparent that, as with access to AUSTRAC records, ASIO is complying with the requirements of the MOU between itself and the Australian Taxation Office and is careful not to abuse the access to which it is entitled.

Use of assumed identities

122. Amendments to the Crimes Act during 2001-2002 require Commonwealth agencies that issue or use alternate identity documentation, to maintain appropriate records.

123. The amendments require ASIO, as soon as practicable after 30 June each year, to give the Inspector-General a report for the year.

124. The report for 2002-2003 showed that ASIO issued a small number of authorisations under the legislation for use of assumed identities by intelligence officers.

Archives issues

125. The Director-General of Security provides our office with quarterly progress reports on ASIO's performance in meeting its obligations under the Archives Act 1983. I also meet periodically with relevant ASIO staff to discuss their handling of significant archive issues.

126. We sometimes receive complaints about the handling of archives access requests but the incidence of such complaints has declined in recent times. People who are dissatisfied with decisions on archives applications have the right to have them reviewed by the Administrative Appeals Tribunal.

127. There have been resource pressures in recent times arising from the increased focus on terrorism. Performance, however, has been satisfactory considering the competing priorities, with large numbers of documents cleared for access. Based on our occasional inspection activities, our interaction with archives staff and the progress reports we receive, I am satisfied that ASIO is committed to processing access requests as quickly and efficiently as it can, and to otherwise meeting its obligations under the Archives Act.

Contact with staff

128. I regularly participate in training sessions for ASIO officers and inductees, addressing them on accountability issues and the work of this office.

129. ASIO officers also brief me from time to time on matters that touch upon the work of the office, or to seek an independent opinion.

130. The Director-General places no barriers to contact between ASIO staff and members of this office. Indeed he encourages such contact and does not seek to monitor or control it in any way. For our part, we seek to use this freedom of access positively and responsibly so as to minimise any adverse impact on the work of the agency.

COMPLAINTS AND INQUIRIES

131. During the reporting period 32 complaints about ASIO were concluded without proceeding to a preliminary inquiry¹ (compared with 23 such cases in 2001-2002).

132. Four outstanding matters were carried over from the previous reporting period. The office conducted preliminary inquiries into 19 new complaints about ASIO, an inquiry into whether Australia's intelligence agencies had any warning of the Bali bombings (which naturally included ASIO), and one preliminary inquiry which also involved approaching each agency (see Annex 1).

133. In conducting inquiries I sought briefings on a range of subjects, as well as access to files and to individuals. The Director-General of Security met all such requests.

134. I conducted no 'own-motion' inquiries into ASIO's activities during the reporting period

135. Some of the complaints dealt with during the reporting period are summarised below.

Search warrants

136. The 2001-2002 annual report described a complaint alleging, among other things, that a computer, seized in an ASIO search, was damaged when returned to its owner. ASIO, however, had claimed that it was functioning correctly.

137. At my request the complainant's lawyer obtained a report from a computer technician. The report described a number of defects in the computer, which the complainant said did not exist before the search, but the report did not indicate when they might have been caused.

138. Since the report was prepared many months after ASIO returned the computer, I took possession of the computer and had a technician examine the hard disk, to try and establish whether the computer had been used after ASIO returned it to its owner.

139. The results of this report suggested that, although the computer may indeed have been used, it was not in the same condition when returned as when ASIO seized it.

140. ASIO subsequently agreed to my suggestion that it offer the complainant compensation and the complainant accepted the offer.

¹ See Annex 1 for description of the various types of inquiry.

141. In another case the legal representative of a complainant, after examining the search warrant, alleged that the search took place at premises other than those specified in the warrant.

142. On inquiry it appeared that ASIO officers in fact presented the warrant at the right premises but the occupant, who was a relative of the person whose premises they were authorised to search, told them that they could find that person in nearby premises, to which he would lead them.

143. He took the ASIO officers and accompanying police to the other premises and they began the search in accordance with normal procedures, only to realise after a short time that they were not at the address specified in the warrant.

144. They immediately withdrew without removing any property and destroyed the recordings they had begun making.

145. I concluded that the error was unintentional. Nevertheless the search was unauthorised and I recommended that ASIO negotiate with the complainants to reach a mutually acceptable settlement. Those negotiations were still in progress at the close of the reporting year.

146. A number of other people whose residences ASIO searched complained about various aspects of the searches.

147. The principal allegation was that they were, in effect, detained and prevented from going about their normal business. Search warrants do not authorise the detention of people and if people whose premises are being searched wish to leave they are at liberty to do so.

148. When conducting an overt search under warrant ASIO obtains assistance from the Australian Federal Police and State police, principally at the start of the search, to gain entry to the premises and ensure that risks to persons involved in the search are minimised.

149. In doing this, although acting under the authority of the warrant issued to ASIO and with the benefit of ASIO intelligence about the risks, the police use their own judgment about the techniques to use.

150. A good number of the complaints about conduct related to incidents alleged to have occurred at the initial stages of searches and appeared to be about police behaviour.

151. I therefore encouraged complainants in such cases to exercise rights to have police behaviour reviewed. The Commonwealth Ombudsman became involved in investigations under the Complaints (Australian Federal Police) Act.

152. At the close of the reporting year the inquiries were in their final stages. I expect that they will result in some suggestions for procedural improvements

that could reduce the probability of complaints about ASIO when it conducts searches in the future.

Recruitment practices

153. There were several complaints from people who applied for positions in ASIO but were unsuccessful.

154. Such complaints tend to arise when ASIO has decided to reject applicants on organisational suitability grounds after initial psychological testing.

155. In these circumstances some applicants, normally those employed or expecting to be employed elsewhere in the public sector, are concerned less with the decision not to employ them than with the possibility that their future security status may be affected.

156. The conduct and assessment of psychological tests involves the exercise of professional judgment which it would be inappropriate for the Inspector-General to try and second-guess. In the absence, therefore, of procedural deficiencies the Inspector-General will not be able to recommend change to ASIO's decisions.

157. We can, however, reassure complainants that failure to meet ASIO's occupational suitability requirements does not necessarily have implications for their ability to obtain security clearances for other areas of Commonwealth employment.

Compensation for asylum seeker

158. Previous annual reports have described a complaint made on behalf of an asylum seeker who was detained for many months longer than he should have been due to a defective ASIO security assessment.

159. In 1999 I invited the asylum seeker's legal representative to submit a detailed claim for compensation. After many reminders the claim arrived shortly before the close of the reporting year.

160. The claim was in excess of what appeared justifiable and I referred it to the Australian Government Solicitor for advice. I expect to recommend that ASIO pay a lower, but still significant amount and to finalise this complaint during the first part of the new reporting year.

Bali terrorist attack

161. ASIO provided full and enthusiastic assistance with the conduct of this inquiry, devoting major resources to the task of identifying and bringing to attention possibly relevant material. The body of the final report is classified, but the unclassified introduction and summary is at Annex 2 to this annual report.

AUSTRALIAN SECRET INTELLIGENCE SERVICE

WHAT ASIS DOES

162. ASIS collects foreign intelligence, relying on human sources to obtain information. It produces and disseminates intelligence reports to key government decision-makers.

163. ASIS was established by executive order on 13 May 1952 and operated under government directive until the Intelligence Services Act (ISA) came into effect on 29 October 2001.

164. ASIS's intelligence collection and reporting activities are now regulated by ministerial directions, ministerial authorisations and privacy rules, which have been made pursuant to the ISA.

165. The ISA prohibits ASIS from engaging in activities involving violence or the use of weapons. There is also a prohibition on activity for the purpose of furthering the interests of political parties.

166. Targeting priorities for ASIS and other members of the AIC are established in a planning document that is endorsed and regularly reviewed by the National Security Committee of Cabinet.

167. Further information about ASIS is at <http://www.asis.gov.au>.

SENIOR APPOINTMENTS

168. Mr Allan Taylor AM completed his five-year term as Director-General of ASIS in February 2003.

169. During his period as Director-General, Mr Taylor oversaw the placement of ASIS on a statutory footing, an increasing openness of the Service to external scrutiny, and continuous attention to maintenance and improvement of professional standards.

170. Mr Taylor consistently promoted accountability through all levels within ASIS and strongly supported the work of this office in its inquiry and review activities. I wish Mr Taylor well in his retirement.

171. Mr Taylor was replaced as Director-General of ASIS by Mr David Irvine. Mr Irvine has had a long and distinguished career in the diplomatic service and was most recently Australian Ambassador to China.

INSPECTION ACTIVITIES

172. Inspection activities involving ASIS during the reporting period have included:

- monitoring compliance with the ASIS privacy rules;
- inspecting current operational files; and
- reviewing all submissions, including requests for ministerial authorisations, made by ASIS to the Minister for Foreign Affairs.

173. The Director-General and I have agreed that following each inspection activity, we would discuss any concerns with an appropriate senior manager or liaison officer. I have also made a practice of following up each inspection with a letter reporting the results and outlining any issues raised during the inspection.

174. We have also agreed procedures that would operate should I form the view that any matter arising from an inspection needed to be brought to the attention of the Minister for Foreign Affairs or the Prime Minister. No such matters arose during the reporting year.

Intelligence Services Act and privacy rules

175. Last year's annual report discussed the background to the ISA and its first few months of operation.

176. Since coming into effect, the ISA has brought about a number of changes in the way ASIS goes about its business, the foremost being that the Minister for Foreign Affairs, rather than the Director-General ASIS, is now the person responsible for approving activities carried out for the purpose of collecting intelligence on Australian persons. ASIS rarely carries out such activities.

177. At the conclusion of the reporting period the ISA and ASIS's privacy rules had been in operation for approximately 20 months. In that time we have raised several queries about the application of the rules.

178. ASIS is maintaining a list of these issues so that legislative amendments, where appropriate, can be proposed at an opportune time.

Review of operations

179. In previous years, a member of the office and I would review a selection of current ASIS operational case files at ASIS headquarters every eight weeks to ensure that the operations are carried out legally and with propriety.

180. In March 2003 I engaged a former Inspector-General and Commonwealth Ombudsman, Mr Ron McLeod AM, as a consultant, in order to increase the frequency of these reviews. They now take place every three to four weeks.

181. While this review activity necessarily has a retrospective focus we sometimes comment on very recent actions.

182. For the most part, the cases we reviewed were well planned, well run, tightly controlled, and delivered outcomes that were of significant benefit to the national interest.

183. We did, however, raise a number of issues with the Director-General. While it is not possible to comment in detail on each of these matters in a public report, they included:

- issues arising from ASIS officers travelling with material that, while legal in Australia, might attract attention from overseas law enforcement agencies;
- the appropriate handling of a dissatisfied former human source ;
- clarifying the respective roles of Australian intelligence agencies in conducting a risk assessment of a human source; and
- concerns associated with the acquisition of specialist equipment.

184. The Director-General provided considered responses and I was satisfied with the outcome in each case.

185. In addition to raising issues of this kind, senior managers in ASIS frequently brief me on issues of common interest.

Ministerial submissions

186. We regularly review ASIS's written submissions to its minister relating to operations, including submissions seeking authorisations under the Intelligence Services Act.

187. I am satisfied that these submissions contain sufficient information for the minister to make well-informed decisions.

Use of assumed identities

188. Recent amendments to the *Crimes Act 1914* require Commonwealth agencies that issue or use alternate identity information to maintain appropriate records.

189. The amendments require ASIS, as soon as practicable after 30 June each year, to give the Inspector-General a report for the year.

190. The report for 2002-2003 showed that ASIS issued a number of authorisations under the legislation for use of assumed identities by its officers.

Contact with staff

191. Most ASIS officers meet with me prior to their overseas postings. The purpose of these meetings is to remind ASIS representatives of the role and functions of this office.

192. I also meet with heads of mission who are being sent to posts where ASIS staff are present, to discuss any issues or concerns they might have prior to their departure.

193. In addition to these pre-departure meetings I regularly attend training sessions for ASIS officers and inductees, addressing them on accountability issues and the work of the office.

194. As I did not travel overseas during the reporting period, I visited no ASIS stations in the past 12 months.

COMPLAINTS AND INQUIRIES

195. One complaint about ASIS was carried over into the 2002-03 reporting period. Four new complaints about ASIS led to preliminary or full inquiries. One complaint required checking with all AIC agencies, while the Bali inquiry (see Annex 2) also necessarily required involvement with all AIC agencies.

196. In addition to these matters we received six other complaints about ASIS which were handled without need for inquiry action.

197. A summary of some of the full or preliminary inquiries is provided below.

Termination of relationship

198. I received a complaint in January 2002 from a person who alleged that ASIS terminated its relationship with him in a premature and unsatisfactory manner, contrary to undertakings it had given him. As a consequence, the complainant claimed he had been left with obligations he could not meet.

199. Following an extensive inquiry I invited comment from the Director-General on a draft report in February 2003 and finalised the report in April 2003.

200. The draft report foreshadowed a recommendation for a payment to the complainant to enable him to meet some of the obligations he claimed to have assumed for ASIS's benefit. The complainant, however, informed me that he considered the proposed payment insufficient and he subsequently took other action to try and achieve a better result.

201. The final report, therefore, did not recommend a payment but it did recommend a number of improvements to procedures relating to such matters as agreements with sources, record keeping, and confirming customer requirements.

202. The Director-General informed me that ASIS had already, or would as soon as possible, implement all these suggested improvements.

Psychological assessments

203. An unsuccessful applicant for employment with ASIS contacted my office in August 2002, raising concerns about the selection process she had just undertaken.

204. The complainant had previously applied for employment with another intelligence agency and in the course of that process had been the subject of a psychological assessment.

205. The complainant questioned:

- the appropriateness of intelligence agencies sharing psychological profiles of job applicants;
- the timing of ASIS's request to access the results of this earlier psychological assessment - she believed this should happen at the start of the process, before applicants had gone to the trouble of attending for interview; and
- whether there had been discrimination against her on the grounds of her declared religious beliefs.

206. I have previously concluded that sharing information of this kind is appropriate, for good reasons related to security.

207. On the question of timing, I found that it was appropriate for intelligence agencies not to seek this information immediately upon receipt of an application but to first assess applicants against their own selection criteria, without being influenced by opinions expressed in another agency.

208. In this case, however, it became apparent on inquiry that ASIS had accessed the other agency's material after it decided not to employ the complainant. I could see no good reason for this and sought an explanation from the Director-General.

209. The explanation was that ASIS wished to confirm that the complainant had not been recommended for employment in the other agency following her psychological assessment interview; and to compare its assessment with that of the other agency as a quality control measure.

210. There did not seem to me to be any significant security benefit to offset the infringement of the applicant's privacy.

211. I therefore sought and obtained from the Director-General an assurance that ASIS would not in future seek to access psychological assessment material from other agencies simply for the purposes described above.

212. In view of the possibility that other agencies might be adopting similar practices I also sought and received similar assurances from the heads of the other agencies in the Australian intelligence community.

213. I found no evidence to support the complainant's concerns that she might have been discriminated against on religious grounds.

Recruitment processes

214. In March 2003, I received a complaint from an unsuccessful applicant for employment with ASIS.

215. The complainant wished to obtain reasons why his application was unsuccessful and to ascertain whether security concerns led to the decision.

216. After a short investigation I was able to provide the complainant with some additional detail about the selection exercise he was a part of.

Bali terrorist attack

217. ASIS provided full and enthusiastic assistance with the conduct of this inquiry, devoting major resources to the task of identifying and bringing to attention possibly relevant material. The body of the final report is classified, but the unclassified introduction and summary is at Annex 2 to this annual report.

DEFENCE SIGNALS DIRECTORATE

WHAT DSD DOES

218. DSD's primary function is to collect foreign signals intelligence. It produces and disseminates reports based on what it collects. These reports, which are concerned with significant political, military and economic developments in our region, are provided to key policy makers, the intelligence assessment agencies, and other selected government agencies.

219. DSD may not intercept communications within the domestic Australian telecommunications network.

220. Since 29 October 2001, DSD's intelligence collection and reporting activities have been regulated by ministerial directions, ministerial authorisations and privacy rules, made pursuant to the *Intelligence Services Act 2001* (ISA).

221. Targeting priorities for the Australian intelligence community are established in a planning document that is endorsed and regularly reviewed by the National Security Committee of Cabinet.

222. DSD also acts as the government's authority on all matters pertaining to communications security and information technology security.

223. Further information about DSD can be found at <http://www.dsd.gov.au>.

SENIOR APPOINTMENTS

224. Mr Stephen Merchant replaced Mr Ron Bonighton as Director DSD in December 2002.

225. In accordance with a recommendation of the *MV Tampa* inquiry report (see 2001-02 annual report) DSD obtained in-house legal expertise, a Special Counsel outposted from the Australian Government Solicitor.

INSPECTION ACTIVITIES

226. Inspection activities involving DSD during the reporting period have included:

- daily monitoring of DSD reporting for compliance with the ISA and the DSD privacy rules;
- monthly meetings with DSD staff to discuss compliance and policy issues;
- reviewing ministerial authorisations and other submissions made by DSD to the Minister for Defence; and

- visiting DSD collection sites outside of Canberra, as opportunity permits.

227. Following each of these activities we discuss any concerns with an appropriate senior manager or liaison officer.

228. I have also made a practice of following up our monthly meetings with a letter to the Director outlining any issues of on-going significance or concern.

229. The Director and I have also agreed procedures to operate should I form the view that any matter arising from an inspection needed to be brought to the attention of the Minister for Defence or the Prime Minister. No such matters arose during the reporting year.

Intelligence Services Act and privacy rules

230. Last year's annual report discussed the background to the ISA and its first few months of operation.

231. The Act has brought about significant changes, the foremost being that the Minister for Defence, rather than the Director DSD, is now responsible for approving collection activities involving Australians.

232. Several unintended effects and minor deficiencies in the Act and rules have become apparent. We have raised these either at our monthly meetings or directly with the Director, and administrative solutions have been possible in some cases.

233. At my suggestion, DSD has been keeping a list of these problems so that legislative amendments, where appropriate, can be proposed at an opportune time.

Collection and reporting of Australians' communications

234. The ISA provides a framework within which DSD can collect the foreign communications of Australians in certain restricted circumstances.

235. The Minister for Defence must authorise any activity undertaken for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person.

236. If DSD wishes to conduct such an activity, therefore, the Director needs to satisfy the minister that the criteria set out in the ISA for such intelligence collection will be met.

237. Sometimes in the course of collecting the communications of foreign targets, DSD unintentionally collects the communications of an Australian person engaged in activity (eg involvement in terrorism) that is of legitimate intelligence interest.

238. DSD can legitimately report the intelligence, but in order to deliberately target the Australian's communications to produce further such intelligence it must have a ministerial authorisation.

239. DSD provides a written submission to its minister in relation to each authorisation that it seeks. We regularly review this material as well as the signed authorisations.

240. I am satisfied that these submissions contain sufficient information for the minister to make well-informed decisions.

241. The privacy rules regulate the communication of intelligence information about Australian persons collected by DSD. They require that all such communication meet certain strict criteria.

242. We inspect reports containing intelligence information relating to Australians to check whether they comply with the privacy rules.

243. The proportion of such reports compared to the total output of reports disseminated by DSD is very small.

244. DSD maintains a register, for inspection by the Inspector-General, of every report containing intelligence information about Australian persons. The register, amongst other things, indicates whether the reference was the result of deliberate or incidental collection.

245. Separately, we cross check by interrogating the DSD reports database from a computer terminal in our office. We query DSD when we see reports that contain intelligence information about Australian persons, where it is not obvious that the privacy rules permit such reporting.

246. In the reporting year there were also occasions when, as required by the privacy rules, DSD consulted me about action that should be taken in relation to infringements it believed had occurred.

247. In several instances there was, in fact, a breach of the rules. This occurred for various reasons, the most common being that DSD became aware that a person they had believed to be a foreign national (in some cases on advice from another agency) in fact was an Australian citizen or permanent resident. In one case the person concerned changed their residency status and DSD did not discover it in time to avoid reporting.

248. There were also several instances of DSD consulting me about possible breaches when, after considering the circumstances, I concluded that no breach had occurred.

249. Remedial action taken by DSD normally involves cancellation of the report and notification to recipients to destroy copies. Sometimes, however, particularly if the breach occurred some time before its discovery, our advice to

DSD is to take no further action, because to do so would draw renewed attention to material that could be sensitive.

250. Although not required by the privacy rules, DSD does not name Australian persons in its reporting. It typically uses a generic description such as *a named Australian person, a possible Australian person, etc.*

251. A client agency needing a name must justify having access. DSD will not release the name unless:

- the intelligence information is directly pertinent to the functions of the requesting agency; and
- the agency identifies an appropriate provision of the privacy rules and provides sufficient supporting information.

252. DSD keeps records of the requests and decisions, which we regularly inspect. Also, DSD sometimes consults our office before making a decision in respect of these requests. On occasion we raise issues with DSD after a decision on the release of a name has been made.

253. In the reporting year there were no instances in which DSD's release of a name requested by another agency constituted a breach of the privacy rules.

Comsec monitoring

254. One section of DSD is devoted to Communications Security (Comsec) monitoring.

255. This involves targeting the communications of personnel taking part in selected Defence operations to assess how secure their communications are and, if deficiencies are identified, to instigate remedial action. Comsec monitoring is not directed against members of the public.

256. Comsec monitoring requires ministerial authorisation. Those whose communications are targeted must be warned in advance.

257. Given the potential of such monitoring to intrude upon the privacy of individuals, I regularly receive an update on Comsec activities and issues when I visit DSD headquarters.

258. I am satisfied that the responsible staff are fully aware of their responsibilities under the Intelligence Services Act and discharge their duties with care and within the limits of their authority.

New collection activities

259. DSD frequently develops new projects involving different approaches to collection of intelligence. DSD regularly informs me of the nature of such projects and we discuss any issues that might arise concerning legality or

propriety. My main concern in such cases is to ensure that adequate attention is given to such issues, including DSD obtaining legal advice where necessary.

260. In addition to receiving briefings at DSD headquarters, we also inspected some of DSD's other facilities.

261. I am confident, based on these inspections, other inspection activities and discussions with DSD staff at all levels, that its activities do not involve collecting the domestic communications of the Australian community.

TRAINING ACTIVITIES

262. In the year following the commencement of the ISA and the privacy rules, DSD devoted significant resources to the development of new guidelines and reporting systems to ensure compliance with their newly mandated obligations.

263. During the 2002-03 reporting period, DSD devoted significant resources to fine-tuning and delivering an in-house training module on the practical requirements of the ISA and the principles underpinning the application of the privacy rules.

264. DSD intends delivering this day-long training module to all reporting staff and line managers, and a shortened form to staff members who need less detail (eg. technical and administrative staff).

265. The Director DSD has shown his commitment to this training program by participating in the training module with a group of his most senior managers and personally speaking to as many training groups as he is able.

266. The Inspector-General's office is equally supportive of this training program. During the reporting period we:

- provided input on the course content;
- presented an overview of accountability arrangements and the work of the IGIS, at each training module;
- participated in questions and answer sessions/group discussions on various scenarios drawn from real-life situations; and
- attended training courses at various DSD facilities located outside Canberra.

COMPLAINTS AND INQUIRIES

267. The level of complaints about DSD is generally low due to the fact that DSD collects foreign signals intelligence by technical means. It is unlikely that members of the Australian public would have any direct dealings with DSD.

268. During the reporting period three new complaints about DSD led to either a preliminary or full inquiry. One complainant had concerns about employment within the Australian intelligence community, which required checking with each member of the AIC including DSD.

269. Four complaints about DSD were handled without need for inquiry action.

Bali terrorist attack

270. DSD provided full and enthusiastic assistance with the conduct of this inquiry, devoting major resources to the task of identifying and bringing to attention possibly relevant material. The body of the final report is classified, but the unclassified introduction and summary is at Annex 2 to this annual report.

Alleged bugging of a federal politician

271. On 30 April 2003 a number of news outlets reported on DSD cooperation with an investigation into leaks of material relating to East Timor in 1999-2000. There were allegations that DSD might have eavesdropped on the communications of Mr Laurie Brereton MP, then Opposition spokesman on foreign affairs.

272. There were also suggestions that DSD might have asked a cooperating overseas agency to monitor Mr Brereton's communications because it would have been illegal for DSD to do so itself.

273. Given the nature of the allegations I decided to conduct an inquiry.

274. The report of the inquiry is reproduced at Annex 3 to this annual report.

DEFENCE IMAGERY AND GEOSPATIAL ORGANISATION

WHAT DIGO DOES

275. The Defence Imagery and Geospatial Organisation (DIGO) has prime responsibility for the acquisition and analysis of satellite and other imagery and for the development, acquisition and exploitation of geospatial data.

276. This means that DIGO collects and analyses images of foreign and domestic subjects (eg. landforms, waterways, disputed territories etc.), and develops mapping and imagery intelligence products for a range of Commonwealth agencies and the Australian Defence Force.

277. Detailed technical analysis of imagery obtained by DIGO can reveal information that is of value to key decision makers in the development of policies that are in the national interest, and of possible benefit in national and international emergency management.

278. DIGO also has the capacity to combine imagery with other available sources of data to prepare highly accurate topographical maps and other aids that are of value in the preparation of plans relevant to national defence and security.

SENIOR APPOINTMENTS

279. Mr Chris Stephens AM was foundation Director of DIGO from 1999 until his retirement on 4 July 2003.

280. In establishing DIGO as a separate entity within the Australian intelligence community, Mr Stephens was concerned to ensure ethical conduct, transparency and accountability within the agency.

281. I would like to thank Mr Stephens for supporting the work of our office, and wish him well in his retirement.

ACCOUNTABILITY ARRANGEMENTS

282. During the reporting period DIGO continued to pursue initiatives to formally establish itself as a separate agency.

283. As was noted in last year's annual report, one piece of legislation that needs to be amended is the *Inspector-General of Intelligence and Security Act 1986*, which currently makes no reference to DIGO.

284. Meanwhile, the Director DIGO and I have agreed that I should oversee the activities of DIGO as if the IGIS Act had already been amended. The Minister for Defence has endorsed this approach.

INSPECTION ACTIVITIES

285. We visited DIGO headquarters approximately every three months during the reporting period to identify and review DIGO intelligence collection activities that may have had some impact upon Australians or Australian entities.

286. While DIGO's collection priorities are focussed outside Australia, there are occasions when it collects images of Australian territory, for example in support of defence operations.

287. The scope for collection of imagery which could intrude upon the privacy of Australians is limited and occurs subject to the *Rules Governing DIGO's Activities in Respect of Australia and Australians*.

288. These rules, which were endorsed by the Minister for Defence in November 2000, embody similar principles to the ASIS and DSD privacy rules.

289. My staff and I have received comprehensive briefings on DIGO's capabilities from the Director and his staff. These briefings have been helpful in better appreciating DIGO's capabilities and planning our inspection activities.

290. During the reporting period we raised several procedural issues with the Director DIGO. Each approach received a timely and appropriate response.

291. In overall terms, we were satisfied that all necessary approvals had been obtained in respect of all tasking involving Australian locations and that DIGO's records are being kept in good order.

292. At the invitation of the Director I visited DIGO's facility in Bendigo, Victoria in July 2002, to meet staff, to learn of the work they undertake, and to discuss the role and functions of the Inspector-General.

COMPLAINTS AND INQUIRIES

293. No complaints during the reporting period specifically referred to DIGO.

294. One complainant had concerns about employment within the Australian intelligence community, which required checking with each member of the AIC including DIGO.

Bali terrorist attack

295. As mentioned in the unclassified introduction and summary at Annex 2 to this annual report, we concluded at an early point in our investigations that it was most unlikely that DIGO could have obtained relevant intelligence.

DEFENCE INTELLIGENCE ORGANISATION

WHAT DIO DOES

296. The role of the Defence Intelligence Organisation is to provide intelligence to inform defence and government policy and planning, to support the planning and conduct of Defence Force operations.

297. DIO also aims to develop and maintain a defence intelligence capability for use in time of crisis and conflict. DIO does not concern itself with domestic developments or situations within Australia.

298. Further information about DIO is at <http://www.dod.gov.au/dio/>.

ACCOUNTABILITY ARRANGEMENTS

299. DIO is an intelligence assessment agency, not a collector of intelligence. This means that its day to day activities are unlikely to impinge upon the privacy of Australians.

300. This is recognised in the *Inspector-General of Intelligence and Security Act 1986*, which provides the Inspector-General with restricted functions in relation to DIO.

301. Although I have periodic consultations with and briefings from the Director, it is not necessary to inspect DIO's activities on a routine basis.

COMPLAINTS AND INQUIRIES

302. In December 2000 the then Minister for Defence asked me to inquire into a complaint by a member of the Australian Defence Force who was critical of certain intelligence reporting and related issues affecting the complainant personally.

303. The investigation concluded in February 2003 and I provided a final report to the minister in May.

304. Several factors influenced the duration of the inquiry, as follows:

- a lot of records required review;
- difficulty in contacting some of the people nominated by the complainant as supporting his position;
- the need to obtain information from a number of DIO officers; and
- the greater weight placed on higher priority investigations conducted by the office.

305. The inquiry report contained classified information but the minister was able to provide the complainant with an unclassified version.

306. The report concluded that while the complainant's concerns were genuinely and sincerely held, they did not stand up to objective scrutiny.

307. The report also suggested, though not as a formal recommendation, that it might be desirable, in special circumstances, to establish *ad hoc* external reviews of intelligence performance.

308. No new complaints during the reporting period specifically referred to DIO.

309. One complainant had concerns about employment within the Australian intelligence community, which required checking with each member of the AIC including DIO.

Bali terrorist attack

310. DIO provided full and enthusiastic assistance with the conduct of this inquiry, devoting major resources to the task of identifying and bringing to attention possibly relevant material. The body of the final report is classified, but the unclassified introduction and summary is at Annex 2 to this annual report.

OFFICE OF NATIONAL ASSESSMENTS

WHAT ONA DOES

311. The role of the Office of National Assessments is to produce analytical assessments of international developments. ONA produces reports on international developments and strategic and economic matters in order to assist the government and Commonwealth agencies in the formation of policy and plans.

312. ONA bases its assessments on information available both inside and outside government. It draws on secret intelligence collected by other agencies, as well as diplomatic reporting and open source material including news media and other publications.

313. Further information about ONA can be found at <http://www.ona.gov.au>.

ACCOUNTABILITY ARRANGEMENTS

314. As indicated above, ONA is an analytical agency rather than a collector of intelligence.

315. Recognition of this is reflected in the fact that the Inspector-General of Intelligence and Security Act provides the Inspector-General with limited powers and responsibilities in relation to ONA.

316. Although the Inspector-General has few formal responsibilities for ONA, I have consultations with and briefings from the Director-General when necessary.

COMPLAINTS AND INQUIRIES

317. No new complaints during the reporting period specifically referred to ONA.

318. One complainant had concerns about employment within the Australian intelligence community, which required checking with each member of the AIC including ONA.

Bali terrorist attack

319. ONA provided full and enthusiastic assistance with the conduct of this inquiry, devoting major resources to the task of identifying and bringing to attention possibly relevant material. The body of the final report is classified, but the unclassified introduction and summary is at Annex 2 to this annual report.

THE YEAR 2003-2004 IN PROSPECT

320. The following is a summary of the main activities planned during the remainder of my term, which ends early in 2004.

INSPECTION ACTIVITY

ASIO

321. We intend to inspect all requests for warrants and associated documentation. In selected cases we will follow up these inspections by seeking full details of investigations carried out under warrant, including examining the relevant files and, if necessary, discussing operations with the responsible ASIO officers.

322. We will attend, at our discretion, the questioning of persons detained under the authority of a warrant issued in accordance with section 34D of the ASIO Act.

323. We will continue monitoring ASIO's access to and use of AUSTRAC and taxation records, to ensure compliance with the legislation and the MOUs under which this access is provided.

324. We propose also to inspect all requests for authorities to investigate (ATIs) generated in the Canberra office and as many ATIs as possible on visits to ASIO's regional offices.

325. We will inspect the files on which actions resulting from the ATIs are recorded, examine records of authorities provided for less intrusive inquiries, and monitor the appropriateness of the existing policy.

326. Where ASIO obtains details about Australians from DSD or ASIS reporting we will, if necessary, examine the relevant records in ASIO.

327. We will review ASIO's procedures for controlling the use of alternative documentation associated with assumed identities.

328. We will continue to monitor ASIO's performance with regard to its obligations under the *Archives Act 1983*.

329. We have a standing invitation from ASIO to address training courses for its staff on ethics and accountability. We expect to visit several ASIO offices for this purpose and to conduct inspection work when doing so.

330. We will continue to monitor ASIO's internal audit program and obtain reports on reviews that are of interest to this office.

Inquiries

331. I expect to complete the inquiries that were still on foot at the end of the reporting year.

332. In relation to ASIO's execution of warrants to authorise overt searches, I expect to suggest a number of procedural improvements, including the establishment of agreed procedural guidelines with the Australian Federal Police and State police services.

333. As one of the outcomes of a complaint about ASIO's security assessments of an applicant for permanent residence, I expect to suggest a range of measures to reduce the likelihood of unfairness in the assessment process.

ASIS

334. We plan to inspect records relevant to ASIS's compliance with the ASIS privacy rules on a daily basis and meet with relevant ASIS staff approximately every two months.

335. I expect also to have further discussions with ASIS management about issues relating to interpretation of the rules and the guidance ASIS provides to its staff.

336. We will review all ASIS's submissions to the Minister for Foreign Affairs seeking ministerial authorisations under section 9 of the Intelligence Services Act.

337. We will continue to inspect operational files with regard to the legality and propriety of the conduct of ASIS officers in the field.

338. Where ASIS obtains details about Australians from DSD reporting we will, if necessary, examine the relevant records in ASIS.

339. I will continue to meet with ASIS officers before they proceed on postings to reinforce that they are subject to internal and external scrutiny and are accountable for their conduct.

340. We will review ASIS's procedures for controlling the use of alternative documentation associated with assumed identities.

341. I will continue to address ASIS training courses and other forums on ethics and accountability issues.

DSD

342. Our principal activity will be to monitor DSD's compliance with its obligations under the DSD privacy rules.

343. We will conduct spot audits of DSD records to monitor compliance with ministerial authorisations under the Intelligence Services Act.

344. We will meet key DSD staff on a monthly basis to discuss issues arising out of our monitoring activities, and policy issues affecting compliance, as they arise.

345. We expect DSD will continue to consult us on a range of operational matters. We will in turn continue to assist with prompt advice on issues related to legality and propriety.

346. We will continue to address DSD training courses and other forums on ethics and accountability issues.

347. We plan to visit and inspect the operations of at least one DSD facility outside Canberra each year.

DIGO

348. My staff and I plan to visit DIGO on a regular basis to review the Organisation's compliance with the *Rules Governing DIGO's Activities in Respect of Australia and Australians*.

349. We will pursue amendments to the IGIS Act to formalise this office's jurisdiction over the organisation.

INQUIRIES

350. Ten inquiries under the IGIS Act were in progress at the close of the reporting year. I expect to conclude investigations into each of these cases during the first half of the new reporting year.

351. It is not possible to predict future inquiry workload but there is no reason to expect any significant departure from previous years' patterns.

INTERNATIONAL

352. The fourth biennial conference of international intelligence oversight bodies is planned to take place in the USA in 2004. I expect that my successor will attend this valuable conference.

MANAGEMENT OF THE OFFICE

Support from PM&C and DSD

353. As a very small agency, the office relies on the assistance of the Department of the Prime Minister and Cabinet (PM&C) in handling staff and other administration issues and in providing general support. This support is provided on the basis that we are a portfolio agency and collocated with PM&C. The arrangement works well and I am grateful to PM&C for their continued support.

354. The other major provider of support is DSD which maintains the secure computer network systems within the office. I would like to record my thanks for DSD's continued assistance.

Outputs and outcomes

355. The office is committed to maintaining the outcome for the office which is providing assurance that Australia's intelligence agencies act legally, ethically and with propriety.

356. The agency outcome and outputs are an integral part of the accrual budgetary structure and are outlined in detail in the current portfolio budget statements.

Composition of the office

357. During the reporting year positions were filled as follows:

- Inspector-General of Intelligence and Security
Mr Bill Blick PSM
- Assistant Inspector-General
Vacant
- Principal Investigation Officer
Mr Neville Bryan
- Senior Investigation Officer
Ms Jane Trevor
- Personal Assistant to the Inspector-General
Ms Sandy Thomas
- Office Manager and Monitoring Officer
Ms Robyn Kelly.

Resources

358. The staffing budget has remained relatively static now for several years. The increased workload has resulted in a part time member of the office increasing the number of hours worked and the office temporarily engaging a former Inspector-General as a consultant to assist in monitoring. I believe, however, that resources at this level are adequate providing workload demands do not continue to increase.

Workplace agreements

359. All staff have entered into individual Australian Workplace Agreements as provided for by the Workplace Relations Act.

Performance pay

360. All staff have indicated that they do not wish to receive performance based pay. Accordingly, no staff members were allocated performance based pay during the reporting period.

Industrial democracy

361. The small size of the office lends itself to a collegiate approach to dealing with workplace issues. Whole of agency meetings are held frequently and all staff have direct access to me on a daily basis.

Social justice: access and equity

362. The Inspector-General oversees the activities of Australia's intelligence community to ensure that each agency acts legally, with propriety, and with appropriate regard to human rights. Respect for these fundamental principles fosters an awareness and appreciation of social justice issues.

Workplace diversity

363. All agencies are responsible for developing a workplace diversity plan and reporting progress on workplace diversity issues to the Public Service Commissioner.

364. Given the small size of the office, we have adopted PM&C's workplace diversity plan.

Occupational health and safety

365. The office is covered by the PM&C occupational health and safety plan. The office conducts an annual OH&S audit of the workplace and reports the findings to the office audit committee. There are no outstanding OH&S issues identified and no incidents occurred that needed to be reported.

Disaster recovery plan/business continuity plan

366. The office developed its own disaster recovery/business continuity plan in May 1997 to ensure the continued operation of the office in the event of a disaster. This plan is reviewed periodically to ensure its currency.

Communications strategy

367. The office has an Internet homepage, which is located at <http://www.igis.gov.au>.

368. The site features information about the role and functions of the office, an archive of our annual reports, statements of public interest, links to relevant legislation, and links to other government sites of interest. This site is updated when necessary.

369. People may also communicate with the office by electronic mail. The address is info@igis.gov.au.

Fraud control

370. The office has adopted the fraud control plan of PM&C.

Training and development

371. Staff attend relevant courses and information sessions as necessary.

Internal and external scrutiny

372. The office has again received an unqualified audit report from the ANAO in relation to its financial statements.

373. I appeared before the Senate Finance and Public Administration Legislation Committee, which considered the office's estimates, and the Parliamentary Joint Committee on ASIO, ASIS and DSD.

Consultancy services

374. Della Vedova and Associates provided assistance with the preparation of the financial statements in this annual report at the cost of \$11,000.

375. Mr Ron McLeod AM, a former Inspector-General, assisted with inspections of ASIS operational files at the cost of \$3 300.

Advertising and market research

376. The office incurred no expenditure on general advertising or advertising campaigns during the reporting period.

Freedom of information

377. The office is an exempt agency for the purposes of the *Freedom of Information Act 1982*.

FINANCIAL STATEMENTS

STATEMENT BY THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2003 give a true and fair view of the matters required by the Finance Minister's Orders made under the *Financial Management and Accountability Act 1997*.

W J Blick
Inspector-General of
Intelligence and Security

1 October 2003

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF FINANCIAL PERFORMANCE
for the year ended 30 June 2003

	Notes	2002-03 \$	2001-02 \$
Revenues from ordinary activities			
Revenues from Government	4	657 000	634 000
Reimbursement for Defence inquiry	1.4(b)	-	16 014
Resources received free of charge	1.4 (c)	68 875	79 130
Interest earned		1 628	5 143
Total revenues from ordinary activities		727 503	734 287
Expenses from ordinary activities			
Employees			
Remuneration		481 302	457 422
Superannuation	1.5 (b)	77 753	74 422
Comcare premium		899	866
Total employees		559 954	532 710
Suppliers			
Resources received free of charge	1.4 (c)	68 875	79 130
Other goods and services		111 575	96 368
Total suppliers		180 450	175 498
Equipment depreciation		2 379	4 125
Total expenses from ordinary activities		742 783	712 333
Net surplus /(deficit)		(15 280)	21 954
Total changes in equity other than those resulting from transactions with owners as owners		(15 280)	21 954

The above statement should be read in conjunction with the accompanying notes.

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF FINANCIAL POSITION
as at 30 June 2003

	Notes	2002-03 \$	2001-02 \$
ASSETS			
Financial Assets			
Cash (notes, coins and deposits at bank)	3	300 178	264 035
Receivables	1.4(e)		
Accrued interest income		-	1 386
GST receivable		371	330
Total receivables		371	1 716
Total financial assets		300 549	265 751
Non-financial assets			
Prepayments		1 027	1 622
Plant and equipment	1.8		
Equipment (at cost)		58 247	58 247
Less: accumulated depreciation		(54 900)	(52 521)
Total plant and equipment		3 347	5 726
Total non-financial assets		4 374	7 348
Total assets		304 923	273 099
LIABILITIES			
Provisions – employees			
Employee current liabilities			
Salaries and wages		13 411	10 607
Annual leave	1.5 (a)	36 731	30 160
Long Service Leave	1.5 (a)	143 420	-
Superannuation	1.5 (b)	13 371	18 455
Accrued FBT		11 591	4 049
Total employee current liabilities		218 524	63 271
Employee non current liabilities			
Annual leave	1.5 (a)	21 394	29 511
Long service leave	1.5 (a)	70 880	172 620
Total employee non current liabilities		92 274	202 131
Total provisions – employees		310 798	265 402
Payables - trade creditors (current)		2 735	1 027
Total liabilities		313 533	266 429
Net Assets		(8 610)	6 670
EQUITY			
Contributed equity	2	66 000	66 000
Accumulated results	2	(74 610)	(59 330)
Total equity		(8 610)	6 670

The above statement should be read in conjunction with the accompanying notes.

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY
STATEMENT OF CASH FLOWS
for the year ended 30 June 2003

	Notes	2002-03 \$	2001-02 \$
OPERATING ACTIVITIES			
Cash received			
Appropriations		657 000	634 000
Reimbursement for Defence inquiry		-	16 014
Interest		3 014	4 394
Expense refunds		-	1 509
Net GST refunds		5 557	3 588
Total cash received		665 571	659 505
Cash used			
Employees		(514 557)	(500 935)
Suppliers		(114 871)	(107 755)
Total cash used		(629 428)	(608 690)
Net cash from operating activities	3	36 143	50 815
Net increase/(decrease) in cash held		36 143	50 815
Cash at beginning of reporting period		264 035	213 220
Cash at the end of the reporting period	3	300 178	264 035

STATEMENT OF COMMITMENTS AND CONTINGENCIES
As at 30 June 2003

The office had no contingencies to report in either 2001-02 or in 2002-03.

The office had at the end of year an operating leasing commitment totalling \$5 497 (2001-02: \$5 497) for the provision of a motor vehicle to the Inspector-General. There are no renewal or purchase options available to the office and this lease matures within one year. No contingent rentals exist.

The above statements should be read in conjunction with the accompanying notes.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

for the period ended 30 June 2003

Note 1 - Summary of Significant Accounting Policies

1.1 - Objectives of the Office of the Inspector-General of Intelligence and Security

The objective of the office is to meet the following outcome:

Assurance that Australia's intelligence agencies act legally, ethically and with propriety.

The office is structured to meet two outputs:

Output 1: Inspect and report on the activities of the intelligence and security agencies (60% of resources)

Output 2: Conduct inquiries and provide a complaint resolution service (40% of resources)

1.2 Basis of Accounting

The financial statements are required by section 49 of the *Financial Management and Accountability Act 1997* and are a general purpose financial report.

The statements have been prepared in accordance with:

- Finance Minister Orders (or FMO's, being the *Financial Management and Accountability (Financial Statements for reporting periods ending on or after 30 June 2003) Orders*);
- Australian Accounting Standards and Accounting Interpretations issued by the Australian Accounting Standards Board; and
- Consensus views of the Urgent Issues Group.

The Statements of Financial Performance and Financial Position have been prepared on an accrual basis and are in accordance with the historical cost convention. No allowance is made for the effect of changing prices on the results or the financial position.

Assets and liabilities are recognised in the statement of Financial Position when and only when it is probable that future economic benefits will flow and the amounts of the assets or liabilities can be reliably measured.

Revenues and expenses are recognised in the statement of Financial Performance when and only when the flow or consumption or loss of economic benefits has occurred and can be reliably measured.

The continued existence of the office in its present form and with its present programs, is dependent on continuing appropriations by Parliament for the office's administration and programs.

1.3 Changes in Accounting Policy

The accounting policies used in the preparation of these financial statements are consistent with those used in 2001-02, except in respect of measurement of certain employee benefits at nominal amounts (refer to Note 1.5).

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 1 - Summary of Significant Accounting Policies (cont.)

1.4 Revenues

(a) Revenues from Government

The full amount of the appropriation for agency outputs for the year is recognised as revenue.

(b) Reimbursements for Defence inquiry

In 2001-02 the office received reimbursement of direct administration costs from the Department of Defence for the Balibo inquiry

(c) Resources Received Free of Charge

Services received free of charge are recognised as revenue when and only when a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense.

The main resources received free of charge are the internal secure computer network (from Defence Signals Directorate) and office space (from the Department of Prime Minister and Cabinet). Other resources received free of charge include auditor remuneration as disclosed in note 7.

(d) Interest

Interest is recognised on a proportional basis taking into account the interest rate applicable to the financial assets up to a threshold of \$3,000 in accordance with the Agency Banking Incentive Scheme.

(e) Receivables

All receivables are not overdue and are therefore classified as current assets.

1.5 Employee Benefits

Liabilities for services rendered by employees are recognised at the reporting date to the extent that they have not been settled.

Liabilities for wages and salaries (including non-monetary benefits), annual leave, sick leave and long service leave are measured at their nominal amounts. Other employee benefits expected to be settled within 12 months of the reporting date are also measured at their nominal amounts.

The nominal amount is calculated with regard to the rates expected to be paid on settlement of the liability. This is a change in accounting policy from last year required by an initial application of a new Accounting Standard AASB 1028 from 1 July 2002.

(a) Leave

The liability for employee entitlements includes provision for annual leave and long service leave. No provision has been made for sick leave as all sick leave is non-vesting and the average sick leave taken in future years by employees of the office is estimated to be less than the annual entitlement for sick leave.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 1 - Summary of Significant Accounting Policies (cont.)

The leave liabilities are calculated on the basis of employees' remuneration, including the office's employer superannuation contribution rates to the extent that the leave is likely to be taken during service rather than paid out on termination.

The liabilities for annual leave and long service leave reflect the value of the total leave entitlements of all employees at 30 June 2003 and is recognised at the nominal amount.

(b) Superannuation

Staff of the Office of the Inspector General of Intelligence and Security are members of the Commonwealth Superannuation Scheme and the Public Sector Superannuation Scheme. The liability for their superannuation benefits is recognised in the financial statements of the Commonwealth and is settled by the Commonwealth in due course.

The Office of the Inspector General of Intelligence and Security makes employer contributions to the Commonwealth at rates determined by an actuary to be sufficient to meet the cost to the Commonwealth of the superannuation entitlements of the office's employees.

The liability for superannuation recognised as at 30 June represents outstanding contributions for the final fortnight of the year.

1.6 Financial instruments

Accounting policies for financial instruments are stated at note 10.

1.7 Acquisition of Assets

Assets are recorded at cost on acquisition. No assets have been exchanged or liabilities undertaken.

1.8 Plant and Equipment

The office's fixed assets comprise office equipment only.

Asset recognition

Purchases of equipment are recognised at cost in the Statement of Financial Position, except for purchases costing less than \$2 000, which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

Depreciation and Amortisation

Depreciable equipment assets are written-off to their estimated residual values over their estimated useful lives to the office using the straight-line method of depreciation.

Depreciation rates (useful lives) and methods are reviewed at each balance date and necessary adjustments are recognised in the current, or current and future reporting periods, as appropriate. Residual values are re-estimated for a change in prices only when assets are revalued.

Depreciation and amortisation rates are for 3 to 13 years for each class of depreciable assets.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 1 - Summary of Significant Accounting Policies (cont.)

1.9 Transactions by the Government as Owner

From 1 July 2002, the FMOs require that amounts of appropriations designated as 'Capital - equity injections' (less any savings offered up in Portfolio Additional Estimates Statements) are recognised directly in Contributed Equity as at 1 July or later date of effect of the appropriation.

This is a change of accounting policy from 2002-03 to the extent any part of an equity injection that was dependent on specific future events occurring was not recognised until the appropriation was drawn down.

The change in policy has no financial effect in 2002-03 because the full amounts of the equity injections were recognised in the year it was received.

1.10 Taxation

The office is exempt from taxation except fringe benefits tax and the goods and services tax (GST).

Revenues, expenses and assets are recognised net of GST except for receivables and payables.

1.11 Insurance

The Office of the Inspector-General of Intelligence and Security has insured for risks through the Government's insurable risk managed fund, called 'Comcover'. Workers compensation is insured through the Government's Comcare Australia.

1.12 Comparative Figures

Comparative figures have been adjusted to conform to changes in presentation in these financial statements where required.

1.13 Rounding

Amounts have been rounded to the nearest dollar.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 2 Equity

Item	Contributed equity		Accumulated results		TOTAL EQUITY	
	2002-03 \$	2001-02 \$	2002-03 \$	2001-02 \$	2002-03 \$	2001-02 \$
Balance 1 July	66 000	66 000	(59 330)	(81 284)	6 670	(15 284)
Operating result	-	-	(15 280)	21 954	(15 280)	21 954
Balance 30 June	66 000	66 000	(74 610)	(59 330)	(8 610)	6 670
Total equity attributable to the Commonwealth	66 000	66 000	(74 610)	(59 330)	(8 610)	6 670

Note 3 - Cash Flow Reconciliation

	2002-03 \$	2001-02 \$
Reconciliation of Cash per Statement of Financial Position to Statement of Cash Flows:		
• Cash at year end per Statement of Cash Flows	300 178	264 035
• Statement of Financial Position items comprising above cash - Financial Asset - Cash:		
a) Cash on Hand	73	76
b) Cash at Bank	300 105	263 959
	<u>300 178</u>	<u>264 035</u>
Reconciliation of net surplus to net cash from operating activities:		
Net surplus /(deficit)	(15 280)	21 955
Depreciation	2 379	4 125
Increase/(Decrease) in provision for employee liabilities	45 396	27 501
Increase/(Decrease) in creditors	1 708	(3 103)
(Increase)/Decrease in other assets	595	(981)
(Increase)/Decrease in GST receivable	(41)	2 067
(Increase)/Decrease in accrued income	1 386	(749)
Net cash flow from operating activities	<u>36 143</u>	<u>50 815</u>

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 4 – Appropriations

Note 4 (A) – Agency Appropriations Acts (1/3) 2002-03

Particulars	2002-2003	
	Agency Outputs \$	Total \$
Year Ended 30 June 2003		
Balance carried forward from previous year	198 365	198 365
Appropriation for reporting period (Act 1)	657 000	657 000
GST credits (FMAs 30A)	5 598	5 598
Annotations to 'net appropriations' (FMAs 31)	3 014	3 014
Available for payments	863 977	863 977
Payments made	629 428	629 428
Balance carried to next year	234 549	234 549
Represented by:		
Cash	234 178	234 178
Add: Receivables – Net GST Receivable from the ATO	371	371
Total	234 549	234 549

Year Ended 30 June 2002		
Balanced carried forward from previous year	147 220	147 220
Appropriation for reporting period (Act 1)	634 000	634 000
GST credits (FMAs 30A)	3 918	3 918
Annotations to 'net appropriations' (FMAs 31)	21 917	21 917
Available for payments	807 055	807 055
Payments made	608 690	608 690
Balance carried to next year	198 365	198 365
Represented by:		
Cash	198 035	198 035
Add: Receivables – Net GST Receivable from the ATO	330	330
Total	198 365	198 365

Note 4 (B) Agency Appropriations Acts (2/4) 2002-03

The office received \$66 000 as an equity injection in the financial year ended 30 June 2001. The office did not spend any of this appropriation during the current and prior year.

Note 5 - Reporting of Outcomes

There is only one outcome for this office as detailed in the objectives in note 1.1.

Note 5 (A) Net Cost of Outcome Delivery

The net cost of that outcome to the budget outcome in 2002-03 was \$672 280 (Budget: \$657 000).

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 5 Reporting of Outcomes (cont.)

Note 5 (B) Agency Revenue and Expenses by Output Group

The decision to attribute resources on a 60:40 basis, (60% inspection activities and 40% conducting inquiries and providing a complaint resolution service), originated from the Samuels Inquiry (1995) and has been reinforced by more recent legislative changes.

	Output Group 1		Output Group 2		OUTCOME TOTAL	
	2003	2002	2003	2002	2003	2002
	\$	\$	\$	\$	\$	\$
Operating revenues						
Revenues from government	394 200	380 400	262 800	253 600	657 000	634 000
Other income	42 302	60 172	28 201	40 115	70 503	100 287
Total operating revenues	436 502	440 572	291 001	293 715	727 503	734 287
Operating expenses						
Employees	335 972	319 626	223 982	213 084	559 954	532 710
Suppliers	108 533	105 299	72 355	70 199	180 888	175 498
Total operating expenses	444 505	424 925	296 337	283 283	740 842	708 208

Note 6 - Executive Remuneration – in excess of \$100 000

	2002-03	2001-02
	\$	\$
Inspector-General:	306 897	255 836

Note 7 – Remuneration of Auditor

Financial statement audit services are provided free of charge to the office

The fair value of audit services provided was:	13 000	12 000
No other services were provided by the Auditor-General.		

Note 8 – Staffing Level

The average staffing level for the office in 2002-03 was 4.6 (2001-02: 4.6)

Note 9 - Act of Grace Payments, Waivers and Defective Administration Scheme

No 'Act of Grace' payments were made during the reporting period (2001-02 nil).

No waivers of amounts owing to the Commonwealth were made during the reporting period (2001-02 nil).

No payments were made under the 'Defective Administration Scheme' during the reporting period (2001-02 nil).

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 10 – Financial Instruments

(a) Terms, conditions and accounting policies

Financial Instruments	Accounting policies and methods (including recognition criteria and measurement basis)	Nature of the underlying instrument (including significant terms & conditions affecting the amount, timing and certainty of cash flows)
<i>Financial Assets</i>	Financial assets are recognised when control over future economic benefits is established and the amount of the benefit can be reliably measured.	
Cash	Deposits are recognised at their nominal amounts. Interest is credited to revenue as it accrues.	The agency invests funds at a commercial bank at call. Monies in the office's bank accounts are swept into the Official Public Account nightly and interest is earned on the daily balance on rates based on money market call rates. Rates have averaged 1.07% for the year (2001-02 2.5%). Interest is paid at month end.
Receivables for goods and services	Receivables are recognised at their nominal amounts due less any provisions for bad and doubtful debts. Collectability of debts is reviewed at balance date. Provisions are made when collection of the debt is judged to be less rather than more likely.	All receivables are with Commonwealth entities. Credit terms are net 30 days (2001-02 30 days)
Interest Receivable	Interest is accrued as it is earned.	The average interest rate for the year was 1.07% and the frequency of payments are quarterly.
<i>Financial Liabilities</i>	Financial liabilities are recognised when a present obligation to another party is entered into and the amount of the liability can be reliably measured.	
Trade Creditors	Creditors and accruals are recognised at their nominal amounts which are the amounts at which the liabilities will be settled. They are recognised to the extent that the related goods or services have been received (and irrespective of having been invoiced).	All creditors are entities that are not part of the Commonwealth legal entity. Settlement is usually made net 30 days.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS
for the period ended 30 June 2003

Note 10 – Financial Instruments (cont.)

(b) Interest Rate Risk

Financial Instruments (Recognised)	Floating interest rate		Non-Interest Bearing		Total		Weighted Average Effective Interest Rate	
	02-03 \$	01-02 \$	02-03 \$	01-02 \$	02-03 \$	01-02 \$	02-03	01-02
Financial Assets								
Cash on hand	-	-	73	76	73	76	n/a	n/a
Cash at Bank	299 105	262 959	1 000	1 000	300 105	263 959	1.07%	2.50%
Receivables for goods or services	-	-		1 716	-	1 716	n/a	n/a
Total	299 105	262 959	1 073	2 792	300 178	265 751		
Total Assets					304 923	273 099		
Financial Liabilities								
Trade Creditors	-	-	2 735	1 027	2 735	1 027	n/a	n/a
Total	-	-	2 735	1 027	2 735	1 027		
Total Liabilities					313 533	266 429		

No funds were invested at a fixed interest rate.

(c) Net Fair Value of Financial Assets and Liabilities

The office's aggregate net fair values of (identified) financial instruments are the same as their carrying amounts.

1. Credit Risk Exposure

The office's maximum exposure to credit risk at reporting date in relation to each class of recognised financial assets is the carrying amount of those assets as indicated in the Statement of Financial Position.

The office has no significant exposure to any concentrations of credit risk.

All figures for credit risk referred to do not take into account the value of any collateral or other security.

Note 11 – Special Accounts

The office has 2 special accounts established under section 20 of the FMA Act 1997. The accounts established are "Other trust Moneys and Services for the Government" and "Non Agency Bodies Account". These accounts have never been active.

IGIS CONTACT INFORMATION

Location

3-5 National Circuit
BARTON ACT 2600

Written inquiries

The Inspector-General of
Intelligence and Security
PO Box 6181
KINGSTON ACT 2604

Parliamentary and media liaison

Ms Sandy Thomas
Personal Assistant to IGIS
Phone: (02) 6271 5692
Fax: (02) 6271 5696

General inquiries

Phone: (02) 6271 5692
Fax: (02) 6271 5696
E-mail: info@igis.gov.au

Internet address

<http://www.igis.gov.au>

ANNEX 1 - COMPLAINT AND INQUIRY STATISTICS

Table 1 - IGIS Act inquiries actioned between 1 July 2002 – 30 June 2003

Agency	Source	Date of Receipt	Type of Inquiry ²	Decision Notified	Current Status
DIO	Minister	20/12/00	Full	30/05/03	Closed
ASIS	Human Source	29/01/02	Full	10/04/03	Closed
ASIO	Public	09/05/02	Preliminary	13/02/03	Closed
ASIO	Public	10/05/02	Preliminary	08/08/02	Closed
ASIO	Public	12/07/02	Preliminary	11/09/02	Closed
ASIO	Public	15/07/02	Preliminary	15/08/02	Closed
AIC	Public	17/07/02	Preliminary	27/08/02	Closed
ASIO	Employee	20/08/02	Preliminary	03/09/02	Closed
ASIO	Public	20/08/02	Preliminary	12/12/02	Closed
ASIS	Public	20/08/02	Preliminary	12/12/02	Closed
ASIO	Public	01/10/02	Preliminary		Open
AIC	Minister	16/10/02	Full	09/12/02	Closed
ASIO	Public	21/10/02	Preliminary	19/12/02	Closed
ASIS	Public	13/11/02	Preliminary	20/01/03	Closed
ASIO	Public	22/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	24/11/02	Preliminary		Open
ASIO	Public	20/01/03	Preliminary	28/01/03	Closed
DSD	Employee	21/01/03	Preliminary	28/01/03	Closed

² A preliminary inquiry allows the Inspector-General to conduct a quick review of a complaint, to determine whether the issues raised fall within the jurisdiction of the Inspector-General and to address complaints where the use of formal powers is considered unnecessary. A full inquiry allows the Inspector-General to use the complete range of statutory powers in the IGIS Act.

Agency	Source	Date of Receipt	Type of Inquiry²	Decision Notified	Current Status
ASIO	Public	28/02/03	Preliminary	12/06/03	Closed
ASIO	Public	06/03/03	Preliminary	16/04/03	Closed
DSD	Public	19/03/03	Preliminary	09/05/03	Closed
ASIS	Public	19/03/03	Preliminary	10/06/03	Closed
ASIO	Public	28/03/03	Preliminary	30/05/03	Closed
DSD	Public	14/04/03	Preliminary		Open
ASIS	Employee	16/04/03	Preliminary	16/06/03	Closed
ASIO	Public	24/04/03	Preliminary	21/05/03	Closed
DSD	Own motion	30/04/03	Full	30/06/03	Closed

**Table 2 -Concerns about agencies that were handled without need for inquiry action
1 July 2002 – 30 June 2003**

Agency	Source	Date of complaint	Former complainant	Current status
ASIO	Public	08/07/02	No	Closed
ASIO	Public	16/07/02	No	Closed
ASIO	Public	27/07/02	No	Closed
ASIO	Public	26/08/02	No	Closed
ASIS	Public	26/08/02	No	Closed
ASIO	Public	27/08/02	No	Closed
ASIO	Public	30/08/02	No	Closed
ASIO	Public	20/09/02	Yes	Closed
ASIS	Public	26/09/02	No	Closed
ASIO	Public	27/09/02	No	Closed
ASIO	Public	30/09/02	Yes	Closed
ASIO	Public	02/10/02	No	Closed
ASIO	Public	04/10/02	No	Closed
ASIO	Public	04/10/02	Yes	Closed
DIO/DSD	Public	08/10/02	No	Closed
ASIO	Public	14/10/02	No	Closed
ASIO	Public	18/10/02	No	Closed

Agency	Source	Date of complaint	Former complainant	Current status
ASIO	Public	21/10/02	Yes	Closed
ASIO	Public	31/10/02	Yes	Closed
DSD	Public	31/10/02	No	Closed
ASIO	Public	04/11/02	No	Closed
DSD	Public	08/11/02	No	Closed
ASIO	Public	17/11/02	Yes	Closed
ASIO	Public	20/11/02	No	Closed
DSD	Public	03/12/02	Yes	Closed
ASIO	Public	13/12/02	No	Closed
ASIO	Public	20/12/02	No	Closed
ASIO/ASIS	Public	20/12/02	No	Closed
ASIO	Public	02/01/03	No	Closed
ASIO	Public	06/01/03	No	Closed
ASIO	Public	20/01/03	No	Closed
ASIS	Public	05/02/03	No	Closed
ASIO	Public	08/02/03	Yes	Closed
ASIS	Public	10/02/03	Yes	Closed
ASIO	Public	11/02/03	No	Closed
ASIO	Public	27/02/03	No	Closed
ASIS	Public	04/03/03	No	Closed
ASIO	Public	26/03/03	No	Closed
ASIO	Public	04/04/03	No	Closed
ASIO	Public	06/06/03	No	Open

ANNEX 2 - BALI INQUIRY REPORT

Scope and method of inquiry

1. Shortly after the attack the intelligence and security agencies³ searched their records to ascertain whether there was any information that warned of the attack. The Director-General of ONA, who coordinated the search, reported to the Prime Minister that no material that specifically warned of the attack was identified.
2. The Australian Federal Police (AFP) conducted a similar search, with the same negative result.
3. Following media suggestions that there had been such intelligence, on 23 October 2002 the Prime Minister wrote asking me to:
 - review all relevant intelligence available to Australian intelligence and security agencies, and associated intelligence assessment processes, to establish whether there was any information that warned of the bomb attack in Bali on 12 October 2002; and
 - propose relevant recommendations in the light of my findings.
4. The intelligence and security agencies are not normally taken to include the AFP. In view of the possibility that the AFP might have been in a position to receive relevant intelligence I sought and obtained clarification from the Secretary of the Department of the Prime Minister and Cabinet that I should include the AFP in the inquiry.
5. The agencies all maintain detailed, searchable electronic records of the great bulk of the intelligence they receive. There are also, in some agencies, some hard copy records that are not converted to electronic form.
6. The inquiry identified approximately 170 search terms one or more of which would be likely to be contained in intelligence that could have warned of the attack. They ranged from broad, obvious terms like “terrorism” and “Bali” to relatively obscure ones, such as aliases of possible perpetrators (the full list of terms is at Annex 1 to this report).
7. They included the terms that the agencies had used previously (see paragraph 1), as well as terms identified since the attack, such as names of suspects. More names were added, and fresh searches done, as investigations into the attack continued.

³ Australia’s intelligence and security agencies are: The Office of National Assessments (ONA); The Australian Security Intelligence Organisation (ASIO); The Australian Secret Intelligence Service (ASIS); the Defence Signals Directorate (DSD); The Defence Intelligence Organisation (DIO); and the Defence Imagery and Geospatial Organisation (DIGO).

8. A team established for the purpose in each agency searched the agency's electronic records back to 11 September 2001 using all these terms.

9. The inquiry supervised these searches and, where necessary, authorised modifications to take account of the agencies' different information technology systems.

10. Each team identified and examined possibly relevant records listed as a result of the searches. The inquiry did likewise. Thousands of records were examined in this way.

11. Much intelligence is shared between the intelligence and security agencies. In the unlikely event, therefore, of one agency's records not revealing the existence of a particular item of intelligence, this methodology would be likely to identify the item in the records of other agencies.

12. The inquiry also had direct access, from a computer terminal located in our office, to ASIS and DSD intelligence reports and conducted separate searches of those records as necessary.

13. The inquiry also examined each agency's hard copy holdings. For this purpose it accessed subject indexes maintained by the agencies and perused files that appeared likely to contain intelligence warning of the attack if such intelligence existed.

14. It was possible that, notwithstanding the breadth of the searches, someone in an agency might recall seeing relevant intelligence. Each of the intelligence and security agencies, at my request, circularised staff asking that anyone who had seen or heard of, or who believed they may have seen or heard of, such intelligence, bring it to the notice of the agency or this inquiry. The AFP had previously taken similar action, without result, so I did not repeat the request there.

15. At the time of the searches referred to in paragraph 1, the agencies contacted cooperating overseas agencies that would have been likely to provide relevant intelligence. Each searched its records and confirmed that it did not have such intelligence and could not, therefore, have passed it to Australia.

16. The inquiry concluded that there was nothing to be gained by repeating the requests to overseas agencies, noting also that in the United States, the United Kingdom and New Zealand there had been official statements to the effect that no such intelligence was collected.

17. The Defence Imagery and Geospatial Organisation does not collect intelligence of the kind that would have forewarned of the Bali attack. At the start of the inquiry I confirmed with the Director that it had no such intelligence and that its collection activities would not have provided any. It was not necessary to do searches of the kind undertaken in the other agencies.

18. One agency has a number of electronic records of foreign language intelligence, collected shortly before the attack, that was not reported on because it did not meet the criteria for high interest intelligence at the time.

19. Under normal circumstances this material would have been discarded but the agency head decided, before the inquiry was announced, to retain the records in case they contain something significant. It is unlikely that they do, but to exclude the possibility the records will be examined in detail.

20. Rather than wait for that process to be completed, which will take some time, I have decided to report the results of the inquiry to date. A second and final report will be produced as soon as possible.

Results

21. The electronic searches resulted in thousands of “hits” on the various terms used. The nature of the searches, however, caused many records to appear multiple times on the lists generated.

22. A small proportion of these appeared, on the basis of the record summaries, to be possibly relevant. Nevertheless, the majority of the records were individually examined.

23. In the months before the attack there were numerous intelligence indications of possible terrorist activity, including activity in Indonesia, with foreign interests or foreigners as likely targets.

24. Annex 3 contains samples of intelligence records and assessments identified by the inquiry as indicative of the kind of intelligence related to the terrorist threat available in the months before the attack.

25. One intelligence report, obtained from foreign liaison sources, mentioned various places, including Bali, as possible loci of terrorist activity should certain specified circumstances eventuate. Those circumstances did not eventuate in the time between receipt of the intelligence and the attack. I am advised that it is clear from the Bali investigation that these circumstances were not relevant to the attack.

26. No other intelligence was received that specified Bali as a likely or possible location for a terrorist attack.

27. Furthermore, even with the benefit of hindsight and knowledge of possible and likely perpetrators, the inquiry could not construe any intelligence, even intelligence not mentioning Bali, as possibly providing warning of the attack.

28. ASIO’s threat assessments during the period covered by the inquiry appropriately reflected the risks suggested by the available intelligence.

Assessments by other agencies also contained realistic appreciations of the risks to Australian interests from action by extremists.

29. One person came forward as a result of the invitation to members of the agencies referred to at paragraph 14. This person did not, however, have any information about intelligence warning of the attack but wished to offer views on intelligence collection and analysis.

30. The inquiry noted, and where necessary followed up, instances of public allegations that warnings had been issued before the attack. None of these proved to have any substance.

31. The inquiry's conclusion, therefore (subject to the further work mentioned in paragraphs 19-20), is that there was no intelligence warning of the attack.

Agency functions

32. It was apparent from media reporting in the period after the attack that there is much ignorance and confusion about the respective functions and responsibilities of the agencies in relation to terrorism.

33. The inquiry therefore prepared, on the basis of information provided by the agencies, a summary of these functions and responsibilities. It is Annex 2 to this report

34. It is also evident that there is a perception in some quarters that the Inspector-General of Intelligence and Security is not sufficiently independent, or lacks sufficient powers, to conduct an inquiry of this kind. This is incorrect.

35. The Inspector-General is an independent office created under the *Inspector-General of Intelligence and Security Act 1986*. The Inspector-General is appointed by the Governor-General in Council for a fixed term. Although a minister can ask the Inspector-General to undertake an inquiry, the conduct of inquiries is entirely at the Inspector-General's discretion and cannot be directed by anyone.

36. In conducting inquiries the Inspector-General has powers equivalent to those of a royal commission, provided by the *Inspector-General of Intelligence and Security Act*. These include the power to compel production of information and documents and to take evidence on oath. The Inspector-General has full and unfettered access to the premises, personnel and records of the intelligence and security agencies.

37. All the agencies provided complete cooperation and assistance during this inquiry. They each provided substantial dedicated resources to conduct the various search tasks that the inquiry required and they complied energetically and enthusiastically with all the inquiry's requests.

Recommendations

38. The Prime Minister asked me (see paragraph 1) to propose relevant recommendations in light of my findings. I do not believe any recommendations are necessary.

Inspector-General of Intelligence and Security
December 2002

ANNEX 3- REPORT INTO ALLEGATIONS THAT DSD INTERCEPTED COMMUNICATIONS OF THE HON LAURIE BRERETON MP

BACKGROUND

1. This inquiry came about as a result of allegations in the Australian media relating to DSD cooperation with an investigation into leaks of intelligence material in 1999-2000.

2. The allegations were summarised in an article in *The Australian* newspaper on 30 April 2003, which stated that:

The nation's most powerful spy agency, the Defence Signals Directorate, eavesdropped on Labor's former affairs spokesman, Laurie Brereton, as part of an investigation into material leaked on the East Timor militia rampages in 1999, a report claims.

3. The article from which the above quotation was taken referred to a piece in *The Bulletin* magazine of 6 May*, headed *OPERATION BRERETON*.

4. This was an account of an episode said to have occurred during an investigation by the Australian Federal Police (AFP) into leaks of intelligence material about East Timor.

5. According to *The Bulletin*, the AFP wanted to: *install a listening device in the Parliament House switchboard and listen to the calls of Brereton, his adviser Dr Philip Dorling and his receptionist.* Unable to obtain permission to do so itself, the AFP asked the Australian Security Intelligence Organisation (ASIO) to assist.

6. The article says that ASIO refused the request:

But the plot thickened: in the course of the investigation, it appears recourse was made to intelligence obtained by foreign governments. Because of its sensitivity, some of the investigators looking at Brereton's office formed a secret task force and set up an office in the Canberra HQ of the Defence Signals Directorate, Australia's eavesdropping agency.

7. Although this article did not, in fact, claim that DSD monitored Mr Brereton's or his staff's communications, that was the interpretation placed upon it by commentators in other media outlets as exemplified by the quotation at paragraph 2. There were also suggestions that DSD might have asked a cooperating agency overseas to monitor Mr Brereton's communications because it would have been illegal for DSD to do so itself.

*Actual date of publication was 30 April

8. In view of this widespread perception I concluded that an independent investigation was warranted. Accordingly I decided to conduct an inquiry, as provided for under subsection 8(2) of the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act).

Object and scope of the inquiry

9. The IGIS Act provides the Inspector-General with powers equivalent to those of a royal commission for the purpose of conducting inquiries into the activities of Australia's intelligence and security agencies.

10. The object of the inquiry was to establish whether DSD had engaged in any improper or illegal activity in relation to Mr Brereton or his staff, including monitoring or attempting to monitor their communications.

11. This inevitably involved examining all relevant surrounding circumstances, including the conduct of investigations into leaks of intelligence material, as described below.

Inquiry methodology

12. As is customary with inquiries under the IGIS Act, I first sought comments from the head of the relevant agency ie the Director, DSD. Mr Merchant replied, inter alia, that:

The claims by the media that DSD monitored the communications of Mr Brereton or his staff are totally without foundation, as are the allegations that DSD attempted to gather information on Mr Brereton or his staff through its international partners.

13. The Director also informed me that the Defence Department's Defence Security Branch (DSB) and the AFP were responsible for conducting the investigation into the 1999 leaks of intelligence material about East Timor. He said that the joint DSB/AFP team was located within DSD headquarters in order to allow it access to the highly classified material that had been the subject of the original leaks. The team did not have the ability or the authority to task the signals intelligence system.

14. DSD still had custody of the files of the leak investigation and the inquiry accessed these.

15. The inquiry also accessed the draft and final reports compiled by the leader of the Defence side of the investigation and the separate AFP report prepared at the conclusion of the investigation.

16. The Director, DSD at the time of establishment of the investigation was Mr Martin Brady, who left DSD in September 1999 and has since retired. I obtained from him a written account of his recollection of the circumstances of

the location of the investigation team in DSD premises and whether the team made or sought to make any use of DSD collection capabilities.

17. The inquiry obtained an affidavit from Mr Ron Bonighton, who succeeded Mr Brady in September 1999 and affidavits from four DSD staff who would have been responsible for processing any requests to overseas agencies for assistance in relation to the investigation.

18. I took sworn evidence from the head of DSB at the time of the investigation, the person engaged as a consultant by DSB to lead the team conducting the investigation and from the DSD officer who was primarily responsible for assisting the investigation team while it was located in DSD premises.

19. The inquiry also obtained a statement from an ASIO officer about an incident in which an officer involved in the investigation asked whether ASIO could obtain a warrant to intercept the telecommunications of possible recipients of leaked material.

20. The results of the inquiry are summarised below.

Operation Arbite/Keeve

21. In April 1999 the Secretary of the Department of Defence tasked the Defence Security Branch of the department (DSB) to investigate the leak of a Defence Intelligence Organisation (DIO) document relating to East Timor that had been the source for media reporting.

22. The task fell to a special investigation unit that DSB had just established following a direction from the Secretary that all leaks of classified information be investigated.

23. More leaks in subsequent weeks led to further tasking and in June 1999, with the investigation becoming wider and more complex, DSB engaged a consultant to lead the investigation, which became known as Operation Arbite.

24. Also in June, DSB approached ASIO for assistance with the investigation and ASIO agreed to help. The Director-General of Security informed the Attorney-General of this.

25. In July 1999 DSB also sought assistance from the Australian Federal Police (AFP), which had separately been investigating leaks of other sensitive Timor-related material at the request of another agency in an operation known as Keeve.

26. The AFP continued with Operation Keeve, while also providing advice and assistance to Operation Arbite.

27. In August 1999 DSB engaged a second consultant to assist its investigation.

28. In October 1999, with the original Keeve investigation drawing to a close, Defence decided that it was desirable to retain AFP involvement and arranged for its minister to refer additional leaks to the AFP through the Minister for Justice and Customs.

29. In December 1999 the DSB and AFP investigations were combined into a joint operation, which effectively concluded early in 2001. In its latter stages the investigation was under AFP control and direction although the consultants referred to at paragraphs 23 and 27 remained part of the investigation team and, as noted at paragraph 15, the first consultant produced a final report for DSB.

30. It is not possible to describe in an unclassified report specific details of the investigative methodologies applied by the Arbite/Keeve investigations. In general terms, however, they involved:

- identifying the likely documentary sources of the large number of media reports apparently relying on classified information;
- establishing, so far as possible, who would have had access to the documents; and
- identifying and following up likely connections between people with access to the documents and those who made public use of the classified information, such as journalists.

31. On 15 December 1999, at a meeting attended by ASIO, a member of the team asked whether ASIO was able to assist the investigation by obtaining a warrant to intercept certain telephone services at Parliament House.

32. The ASIO representatives replied in the negative and provided a report to the Director-General of Security. The Director-General annotated the report saying, *inter alia*: *It is important that the AFP and Defence understand that, unless there is relevance to our functions under the Act, we cannot engage in such activity.*

33. The Director-General subsequently directed that, since it had become clear that the investigation did not raise security intelligence issues, ASIO should have no further role in the investigation.

34. In due course the Arbite/Keeve team's work led it to tentative conclusions about possible involvement of particular individuals in the transmission of classified information.

35. In September 2000, consequently, the AFP obtained and executed search warrants on premises associated with people whom the team had identified.

36. By the time the investigation concluded in 2001 it had identified to its satisfaction at least one person as a source of leaked classified material and one or more likely means whereby such material had found its way into the public domain.

37. The consultant appointed to head the Arbite operation and the responsible AFP officer both prepared detailed reports of the investigation, including recommendations for further action, both in relation to individual personnel and at the systemic level.

DSD involvement

38. At the time of establishment of the Arbite investigation the officer in charge of DSB approached the Director, DSD (Mr Brady) who offered DSD assistance.

39. The Director agreed that the leader of the Arbite team could be located on DSD premises and be provided with certain facilities. He instructed the DSD security officer to provide any necessary assistance.

40. The file document containing the nearest thing to a description of the arrangements is a note from the head of DSB in May 1999, seeking cooperation from the Director, DIO. The note says: *The investigation is being undertaken with the assistance of DSD for those distribution systems under its control.* The reference to distribution systems is evidently to the systems whereby DSD disseminates its product, either electronically or in hard copy.

41. In the absence of further details on file the inquiry asked each of those involved what they could recall of the reasons for DSD providing such assistance. Their accounts provided the following reasons:

the investigation would require access to material with the highest classification as it would be necessary to examine a range of documents, including DSD-sourced documents, to determine the origins of the leaked information. DSD premises are highly secure and suitable for storage of such material and DSB did not have available accommodation with this level of security;

- the team leader would need ready access to DSD personnel who were familiar with the arrangements for creating and distributing DSD product;
- the team would also have access to DSD's considerable in-house expertise in information technology to assist in analysing the material it accumulated;
- there were space restrictions within DSB premises; and
- it was necessary for security reasons to restrict knowledge of and access to the activities of the investigation, even to the extent of segregating it physically from other DSB activities. Since DSD appeared a less likely source of the leaks than other agencies, location in DSD improved the chances of the investigation not becoming known to possible perpetrators.

42. From June 1999 the Arbite team leader was located in an office adjacent to that of the DSD security officer. DSD provided him with a stand-alone

computer and printer and a secure telephone. The other members of the team were in another Defence building close by.

43. Plans for demolition of this building led in March 2000 to a request for the balance of the team to be located in DSD premises. A file note records that accommodation would be needed for 2 case officers, 2 investigators and an analyst and that the Arbite team leader could continue to work from the DSD security office.

44. The note also records the equipment for which accommodation would be needed. This included a dedicated local area network, several stand-alone computers and a computer linked to the AFP by modem.

45. DSD provided the requested accommodation and facilities and the team moved in in April 2000.

46. DSD also provided some assistance from members of its staff:

- The DSD security officer, who was familiar with DSD systems and personnel, acted as a liaison point between the team and DSD: and
- Several DSD personnel with analytical and information technology skills, including IT security specialists, assisted with analysis of data the team obtained and provided audit information from DSD's report distribution systems.

47. A statement to the inquiry from one of these specialists describes how he received data from the team, processed the material and copied the results of his analysis to floppy disk because the team had no access to DSD's computer systems. At the conclusion of the exercise he removed all data from the DSD computer systems.

48. Another specialist described in his statement how his primary role was to provide responses to requests from the investigation team for audit records of DSD's IT-based systems for delivery of its end product reports. He also helped the team understand the report delivery systems and how the auditing records were processed.

Use of DSD signals intelligence collection capability

File records

49. There is no evidence or suggestion on the investigation files of any use, or proposed use, of DSD's signals intelligence collection facilities to target the communications of Mr Brereton, members of his staff or, indeed, anyone.

50. There was, however, material on the files and in the reports referred to at paragraph 37 to lend weight to the view that such action was never contemplated and, if contemplated, would not have taken place.

51. The file that contains records of meetings, consultations and briefings about the investigation has several documents that, at various times during the

investigation, discussed the lines of inquiry the investigation was pursuing, the methods it was using and what the next steps might be.

52. Some of these documents included discussion of the concept and practicalities of obtaining warrants, including telecommunications interception warrants. Had there been any thought that DSD's interception capabilities might be useful to the investigation one would expect there to be references to it in these documents.

53. The files also contain records of specific requests to DSD for assistance with analysis of data and audit material and the results of the analysis. Had DSD been using its interception capabilities to assist the investigation, similar records would need to have been generated.

54. The reports compiled after completion of the investigation by the AFP and the DSB consultant (see paragraph 23) both alluded to the proposals during the investigation to seek telecommunications interception warrants and the reasons for not pursuing such warrants. In addition, they described in detail the other methodologies and lines of inquiry considered and used during the investigation. Again, had use of DSD interception capabilities taken place or been contemplated one would have expected it to be mentioned in these reports.

55. As to whether, if the proposal had been put to DSD, it would have attempted to comply, a file note of a conversation in August 1999 involving the Director DSD is relevant.

56. In that conversation, the note records, the team leader briefed Mr Brady on the progress of the investigation and discussed a number of issues relating to it including DSD's access to intelligence on East Timor.

57. The note also records that the team was contemplating, in relation to a leaked DSD report, a process that would lead to a case being made to the Attorney-General and/or ASIO for warrants against telecommunications services of known individuals.

58. Mr Brady's response was that for DSD the damage from a leak about the intelligence services being involved in an intrusive operation against a journalist or politician's office would be far greater than the damage from the leaked DSD report. It was clear from the note that he was not supportive of the warrant proposal.

59. The rules applying at the time required approval from the Director, DSD for any operation involving collection of intelligence on Australians. That approval could only be provided in certain restricted circumstances. One can infer from Mr Brady's comments that, had he received a request to use DSD interception capabilities to assist the investigation, he would not have agreed.

Statements

60. Paragraph 12 above reports the comments of the current Director, DSD to the effect that claims that DSD monitored the communications of Mr Brereton or his staff are totally without foundation.

61. As mentioned at paragraphs 16 and 17 the inquiry also received statements from Mr Brady, the Director, DSD at the time the leak investigation began and his immediate successor Mr Bonighton.

62. Mr Brady's statement included the following:

I have no recollection that any possibility of using DSD's interception capabilities was ever raised with me. Such use would be contrary to law and to extant Government instructions. And in practice DSD had no relevant capabilities.

63. Mr Bonighton's statement included the following:

At no time was there any suggestion by [the consultant] that he had access or required any access to DSD computing facilities or operational systems. My recollection is that the team of about three had their own stand-alone PC network.

At no time did [the consultant] approach me for assistance in tasking DSD systems to assist with the investigation: in particular, no request or suggestion was made that we should do anything in relation to Mr Brereton or his communications. Nor did any DSD officer approach me with any such request. I would like to make clear that had anyone actually approached me with a request to target Parliament House in relation to an internal security investigation, they would have swiftly received counselling on DSD's role and the illegality of any such action.

You might recall that the terms of the cabinet-approved rules under which DSD operated at that time required that any proposal to target the communications of an Australian had to be referred to me for consideration. Without my written authorisation it was forbidden to use DSD facilities to target or report on the communications of Australians. As a practical aside, I would add that the particular accusation apparently relates to DSD intercepting communications from Parliament House: our systems are focused on international connections, so it is unclear to me how we could have achieved this even if we had tried - which we did not.

64. The inquiry also took sworn testimony from the head of DSB at the time and the consultant who led the investigation team. Both denied that any consideration was given to accessing DSD interception capabilities.

65. A number of respondents to the inquiry also made the point that the Arbite/Keeve leak investigations were into leaks of material within Australia

and had a strictly domestic focus. There was, therefore, no logical reason for the investigation to seek to access foreign communications of people who might have been involved with disseminating leaked material.

66. The former directors quoted at paragraphs 62 and 63 also pointed out that DSD does not have the technical capability to intercept domestic telecommunications. Such interception, undertaken under warrants issued by, for example, the Attorney-General in the case of ASIO, is a terrestrial activity utilising the facilities of the Australian domestic telecommunications carriers.

Inspections

67. The rules that applied at the time of the Arbite/Keeve investigations required DSD to keep records of all instances of targeting of Australian citizens' communications, for inspection by the Inspector-General of Intelligence and Security. I regularly inspected these records and reported on the results in my annual report.

68. Had there been any targeting of Mr Brereton's or his staff's communications, therefore, it would have come to our notice as part of the inspection regime. No such activity came to our notice.

Use of overseas agencies' facilities

69. An implication of some of the media reporting was that, rather than conduct interception of Australians' communications itself, DSD might have asked cooperating agencies overseas to do so.

70. The Director, DSD informed me that this suggestion was totally without foundation.

71. Mr Bonighton's statement contained the following:

There is also a suggestion that we might have asked a cooperating agency of a foreign government to undertake such a task. At no time was any suggestion made to me that we should make such a request in respect of Mr Brereton. Nor is it clear to me how another government could hope to successfully target internal Australian communications. And my experience is that cooperating governments are extremely wary of targeting nationals of partner countries and require high level assurance that any such request has a legal basis.

72. Mr Brady did not cover this issue in his original statement but, after reading the first draft of this report, wrote:

My response is the same as Ron's [Mr Bonighton], that is, it wasn't raised with me. If it had been, my response would have been that we don't ask partners to undertake tasks that we are not prepared to do ourselves from Australian resources, that they wouldn't have any relevant capabilities, and that they

would want to be satisfied at a high level as to the legality and authority of any request to target Australians.

73. The inquiry also received statutory declarations from each of the liaison officers who would have needed to pass on, or at least be aware of any such requests. None knew of any requests and all said they did not believe there were any.

74. It would have been possible to approach the overseas agencies to obtain confirmation but, in light of the above statements and the abundant evidence that the leak investigators had no interest in utilising DSD's collection resources, that was unnecessary.

Conclusion

75. Leak investigations carried out by the department of Defence and the AFP in 1999-2001 received technical and other assistance from DSD, including assistance with accommodation.

76. The assistance did not, however, extend to providing access to DSD's overseas collection capabilities and the investigation team did not seek such access.

77. Although the investigation team had an interest in obtaining information about domestic telecommunications it pursued this with ASIO, not DSD. DSD has no capacity to intercept communications passing over the domestic network.

78. The investigation team did not ask DSD to seek assistance from international partner agencies and DSD did not do so.

Inspector-General of Intelligence and Security

June 2003

ANNEX 4 - INTERNATIONAL OVERSIGHT MECHANISMS: FUNCTIONS, POWERS AND FREEDOMS⁴

Inspector-General Functions	Australia	Canada	New Zealand	South Africa	UK ISC	USA
Ensures compliance with current legislation	Yes	Yes	Yes	Yes	No	Yes
Ensures compliance with standards of propriety	Yes	Yes	Yes	Yes	Yes	Yes
Carries out audits, investigations and inspections	Yes	Yes	Yes	Yes	Yes	Yes
Prevents and detects waste, fraud and abuse	No	No	No	I/U	No	Yes
Promotes economy, effectiveness and efficiency	No	No	No	No	Yes	Yes
Reviews compliance with executive directives and operational policies	Yes	Yes	No	Yes	No	Yes
Ensures compliance with warrant authorisations	Yes	I/U	Yes	No	No	No
Reviews operational activities	Yes	Yes	Yes	No	No	Yes
Reviews pending legislation and regulation	Yes	No	No	No	Yes	Yes
Reports regularly to the agency head(s)	No	No	No	No	No	Yes
Reports regularly to executive, legislature or oversight commission	Yes	Yes	Yes	Yes	Yes	Yes
Reports in response to requests by legislature or oversight commission	Yes	Yes	Yes	Yes	Yes	Yes
Investigates complaints about the agency	Yes	No	Yes	Yes	Yes	Yes
Ensures proper regard to human rights	Yes	No	No	I/U	Yes	Yes
Ensures compliance with regulations on release of records & information	Yes	No	No	I/U	No	Yes
Is immune from arbitrary sacking	Yes	Yes	Yes	No	No	Yes
Hires and controls own staff and contract resources	Yes	No	No	No	Yes	Yes
Has ready access to the agency head(s)	Yes	No	No	No	Yes	Yes
Has access to all records and information of the agency	Yes	Yes	Yes	Yes	No	Yes
Initiates investigations on own initiative	Yes	No	No	Yes	Yes	Yes
Issues subpoenas for information/documents outside the agency	Yes	No	No	Yes	No	Yes
Administers oaths for taking testimony	Yes	No	No	Yes	No	Yes

⁴ This table is adapted from a matrix developed by the United Kingdom's Intelligence Services Committee, following a survey in 2001-2002. *I/U* in the table means that the power or function was inapplicable in the relevant jurisdiction, or it was unclear whether it existed.