

Australian Security  
Intelligence Organisation

Report to  
Parliament  
**2000-2001**

© Commonwealth of Australia

ISSN 0815-4562

ISBN 0-642-48777-4

This document is the property of the Commonwealth of Australia.  
Its contents must not be copied or disseminated.

This is an exempt document under subsection 7(1) of the *Freedom of Information Act 1982*.

Produced and printed by the Australian Security Intelligence Organisation.



**Australian Security Intelligence Organisation**

GPO Box 2176 Canberra City ACT 2601 Telephone 02 6249 6299 Facsimile 02 6257 4501

Office of the Director-General

7 December 2001

The Hon. Daryl Williams, AM, QC, MP  
Attorney-General  
Parliament House, Canberra

Dear Attorney-General

In accordance with section 94 of the *Australian Security Intelligence Organisation Act 1979*, I am pleased to submit the annual report on ASIO for the year ending 30 June 2001.

The distribution of this classified annual report is limited. I also present to you an unclassified version (shorter by about one third) for tabling in the Parliament.

Yours sincerely,

A handwritten signature in cursive script that reads "Dennis Richardson".

Dennis Richardson  
Director-General of Security



# Contents

<b>PART 1: OVERVIEW</b>	<b>1</b>
The Year in Review	3
Agency Overview	8
<b>PART 2: OUTPUT PERFORMANCE</b>	<b>11</b>
Output 1: Security Intelligence Analysis and Advice	14
Output 2: Protective Security Advice	27
Output 3: Security Intelligence Investigation and Capability	34
Output 4: Foreign Intelligence	41
<b>PART 3: MANAGEMENT AND ACCOUNTABILITY</b>	<b>43</b>
Corporate Governance	45
Accountability	46
Our People	51
Information Management	57
Security of ASIO	58
Building Management	60
Purchasing	61
Consultants and Contractors	61
<b>PART 4: FINANCIAL STATEMENTS</b>	<b>63</b>
<b>PART 5: APPENDIXES</b>	<b>97</b>
A. Membership of the Parliamentary Joint Committee on ASIO	98
B. Contact information	99
C. Staffing statistics	100
D. Workplace diversity statistics	101
E. ASIO salary classification structure	102
F. Assumed identities	103
Glossary	104
Compliance Index	105
General Index	106



## **Our Vision**

The intelligence edge for a secure Australia

## **Our Mission**

To provide advice to protect Australia and its people  
from threats to national security

## **Our Values**

Accountability

Integrity

Innovation and Learning

Quality

Respect

Responsiveness

Security

Working Together

# ASIO and its Annual Report

## What ASIO does

The Australian Security Intelligence Organisation - ASIO - is Australia's security service. ASIO was established in 1949 and operates under the *Australian Security Intelligence Organisation Act 1979*.

The *ASIO Act* defines security as protection of Australia and its people from espionage, sabotage, politically motivated violence (including terrorism), promotion of communal violence, attacks on Australia's defence system, or acts of foreign interference. These *heads of security* provide the primary direction for ASIO's work.

ASIO provides security intelligence advice and protective security advice to help Government comprehend and manage the security environment. ASIO also collects foreign intelligence within Australia at the request of the Minister for Foreign Affairs or the Minister for Defence, and contributes to Australia's national counter-terrorism response capability.

ASIO's corporate vision, mission and values are contained in the *Corporate Plan* which is available on our website at [www.asio.gov.au](http://www.asio.gov.au).

ASIO reports to the Attorney-General. Oversight arrangements include the Inspector-General of Intelligence and Security, the Parliamentary Joint Committee on ASIO, and the Auditor-General.

## This Report

ASIO produces two versions of its *Annual Report*. The first version is classified and contains an account of ASIO's performance during the previous 12 months, including sensitive reporting on security risks and investigative outcomes that cannot be released publicly. That report is provided to the Attorney-General, the Prime Minister, members of the National Security Committee of Cabinet, the Leader of the Opposition, and members of the Secretaries Committee on National Security.

An abridged version is then prepared for tabling in the Parliament, excluding classified information in accordance with section 94 of the *ASIO Act*.



Part 1: *The Overview* provides a review of our principal achievements over the reporting period. Part 1 also includes an Agency Overview describing our organisational structure, together with the Government Outcome and the ASIO Outputs that contribute to its achievement.

Part 2: The *Output Performance* report covers:

- security intelligence analysis and advice
- protective security advice
- security intelligence investigation and capability, and
- foreign intelligence.

The Outputs contribute to the achievement of the Government Outcome 'A secure Australia for people and property, for Government business and national infrastructure, and for special events of a national and international significance'.

Part 3: *Management and Accountability* describes performance in respect of accountability arrangements and those key internal service functions that enable ASIO to deliver its Outputs — this includes issues affecting our people, information management, and the security of our working environment.



*The Hon. Daryl Williams  
AM, QC, MO  
Attorney-General*



*Mr Dennis Richardson  
Director-General of Security*

# Part 1

## **overview**



## The Year in Review

Politically motivated violence remained our principal investigative priority - particularly in relation to Middle East terrorist groups, some of which have a small number of supporters in Australia and in our region.

The security of the Sydney 2000 Olympics and the Commonwealth Heads of Government Meeting (CHOGM) was a particular focus of ASIO's work in 2000-01.

Partly as a result of the Olympics, but mainly due to the introduction of a new IT system that was not properly worked through prior to implementation, we fell well short of all benchmarks in personnel security assessments. The problem has been rectified.

We worked with the Attorney-General's Department and the AFP on the espionage-related charges against suspended DIO employee Simon Lappas, and against Sherryll Dowling.

Other issues requiring a response included:

- Giving effect to the recommendations of the *Inquiry into Security Issues*.
- Implementation of a four-year investment program in new capabilities.
- The continuing high rate of unauthorised arrivals requiring security assessments.
- Rapid changes in the telecommunications environment.

## Protecting CHOGM

ASIO worked closely with the CHOGM Task Force, Queensland Police and other Commonwealth agencies to prepare for the protection of CHOGM from terrorism and politically motivated violence.

- An intensive period of training and exercises was conducted for ASIO's CHOGM Security Intelligence Centre (CHOSIC).
- Twenty-five Country Threat Assessments covering 51 countries were issued by 30 June 2001, providing clients with advice on potential threats to CHOGM.
- By 30 June 2001 we had established contact with 84 communities to explain ASIO's role in CHOGM security, and to open a channel of communication.
- Protective security advice was provided to the Queensland Police and the CHOGM Task Force, including advice on security risk management, and venue security plans.

## **Protecting people and property**

ASIO issued 1 342 Threat Assessments in 2000-01 compared to 1 346 in 1999-00. Twenty-six percent were related to the Olympic Games and the World Economic Forum. Sixty-one percent of clients surveyed rated our Threat Assessments 'always useful', and 31% 'usually useful'.

- The threat to US interests in Australia remained a priority.
- There was a significant increase in threats to the Jewish community following the Al Aksa Mosque incident in September 2000. There was no information to indicate the rise in the number and seriousness of anti-Jewish incidents was centrally organised.
- The number of demonstration notifications more than doubled, due largely to protests over globalisation and policy on unauthorised arrivals.

Events in the Middle East continued to have a significant impact on the security environment.

- Sixty-seven percent of clients surveyed considered ASIO's reporting of politically motivated violence issues resulting from events in the Middle East 'always useful', and 33% rated it 'usually useful'.

## **Protecting Government business and national infrastructure**

We fell well short of all benchmarks for personnel security assessments (see page 28). Measures implemented to improve performance should produce a significant improvement in 2001-02.

- Two adverse assessments and ten qualified assessments were issued.

Visa security checks increased by 36.5% to 33 919 — excluding Olympics-specific work and unauthorised arrivals.

- Just over 96% of temporary visa applications, and 88% of permanent visa applications were assessed within agreed timeframes.
- On our advice two visa applicants were refused entry to Australia and a third person had his existing visa cancelled on espionage grounds. A fourth applicant was refused a protection visa on politically motivated violence grounds. A fifth person's visa was cancelled because of an identified link to a terrorist group.
- We issued 3 658 security assessments for unauthorised arrivals compared to 2 739 the previous year — a 34% increase.

Demand for protective security advice increased as agencies began to implement measures required by the new *Protective Security Manual* and the *Inquiry into Security Issues*.

- We advised DoFA, Treasury and the Australian Radiation Protection and Nuclear Safety Authority on appropriate physical and personnel security measures.

With other agencies we completed a threats and vulnerabilities study of four Australian infrastructure sectors.

### **Enhancing capabilities**

Investment in capabilities remained a priority for ASIO in 2000-01.

- Our counter-terrorism response capabilities were further tested in a National Exercise in Queensland in June 2001.
- Our analytical capability was assisted by expanding the range of intelligence data delivered directly to the desktops of intelligence officers.
- Enhancements to our main intelligence database significantly improved the efficiency of key business areas, including in the provision of personnel security assessments advice.
- Our Physical Protective Security work was reviewed, and processes re-engineered to enhance strategic planning capability and establish a better business model with an increased client focus.

### **Management and accountability**

- ASIO's *Security Management Plan 2001-2004* was completed in March 2001, and sets out the objectives and strategies needed to manage security within ASIO.
  - 166 staff security clearance re-evaluations were completed.
  - A Protective Security Risk Review was undertaken of all ASIO offices.
- The *Fraud Control Plan* was revised. A review of the Open Source Unit was completed, and a review of the process of re-evaluating staff security clearances was commenced.
- The separation rate rose to 11.5% from 9.9% in 1999-00. We are seeking to improve our understanding of why people join and leave ASIO through improved exit interview processes.
- To improve our ability to plan for future human resource requirements, an external consultant conducted a comprehensive workforce planning survey.
- We continued to recruit across all job families, with a particular focus on specialist technical, engineering and IT staff, as well as graduate Generalist Intelligence Officers.

- The employment of temporary staff allowed ASIO to meet the increased demands of the Olympic Games and those related to our CHOGM planning and other temporary workload requirements - while maintaining significant flexibility in our staffing profile.
- Developing our staff remained a priority, with corporate investment of 2% of ASIO's budget (excluding on-the-job development and job-specific courses).
- The Parliamentary Joint Committee on ASIO completed its inquiry into *The nature, scope and appropriateness of ASIO's public reporting activities*. The Director-General briefed the PJC on a range of matters as required.

## **The Outlook for 2001-2002**

Terrorism and politically motivated violence will remain the main focus of investigation.

ASIO's support for the security of CHOGM will be a particular priority in 2001-02.

Our *Corporate Plan* will be revised in 2001-02, and will look out to 2005. We will review our *People Management Plan* to identify strategies aimed at providing a supportive and stimulating work environment to attract and retain staff.

Other challenges include:

- Implementing the recommendations of the *Inquiry into Security Issues* to ensure ASIO is a leader in security practice; and working with agencies to implement best security practice across the Australian Intelligence Community and the wider public service.
- Further developing our National Information Infrastructure Protection capability.
- Staying ahead of technological change.
- Fostering partnerships with Australian and overseas agencies.
- Developing the skills and capabilities of our people, our collection technology, our security technology and our information management systems.
- Refining client feedback mechanisms and improving the quality of our services and products.



### **Postscript: The new Counter-Terrorism environment**

The Usama bin Laden terrorist attacks on the USA on 11 September 2001 represent a profound shift in international terrorism, setting new benchmarks in organisation, sophistication and lethality.

Since September 11 the majority of ASIO's investigative and analytical resources have been directed to investigations relating to the attacks.

Australia's strong support for the USA and commitment of military forces to the war on terrorism has raised our profile internationally. Threat levels to Australian interests at home and abroad have risen.

- This threat environment will impose significantly increased demands on ASIO and other Australian agencies.

Dennis Richardson  
Director-General of Security

## Agency Overview

### Organisational Structure

ASIO's chief executive, the Director-General of Security, reports to the Attorney-General. The current Director-General is Dennis Richardson, who was first appointed in October 1996.

ASIO's management structure is at Figure 1.

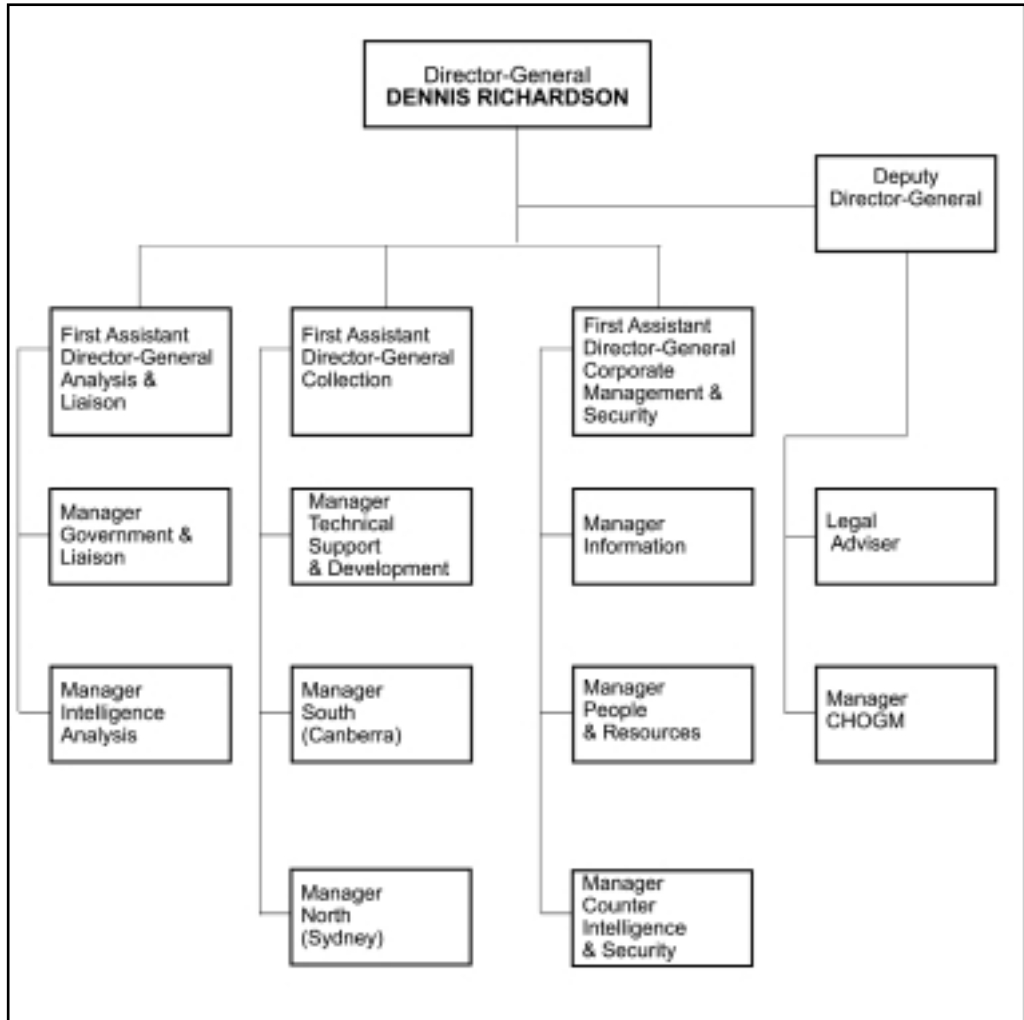


Figure 1. ASIO's management structure

## **The Government Outcome and ASIO's Outputs**

ASIO contributes to the Government Outcome — 'A secure Australia for people and property, for Government business and national infrastructure, and for special events of a national and international significance' which supports the Government's policy aim of 'A secure Australia in a secure region'. The short-hand descriptor 'A secure Australia' is also used.

To support this Outcome ASIO delivers Output Group 1 - Security Intelligence, which includes four Outputs.

### **Output 1.1 Security Intelligence Analysis and Advice**

This Output includes:

- security intelligence analysis and reporting
- Threat Assessments
- advice on visa security checking and archives issues
- advice on deterrence action, and
- contributions to the external policy framework.

### **Output 1.2 Protective Security Advice**

This Output includes:

- advice on personnel security (security clearances)
- advice on physical security, including protective security reporting and risk management
- advice on security equipment standards
- advice on electronic and audio surveillance counter-measures, and
- contributions to the external policy framework.

### **Output 1.3 Security Intelligence Investigation and Capability**

This Output includes:

- collection of information from human sources, open sources and by technical means
- surveillance capabilities
- counter-terrorism response capabilities
- technical research and development
- deterrence action
- national and international liaison, and
- contributions to the external policy framework.

## **Output 1.4 Foreign Intelligence**

This Output includes foreign intelligence collected in Australia at the request of the Minister for Foreign Affairs or the Minister for Defence.

### **Executive Services**

The governance, legal advisory, and coordination functions, including high-level coordination such as is required for the Olympic Games and CHOGM.

### **Enabling Services**

The corporate functions, including people development and management, financial services, information management, facilities management and internal security.

# Part 2

## output performance



## ASIO's Performance

Part 2 reports on the performance of ASIO's four Outputs. The components of each Output are reviewed against:

- their effectiveness, in terms of the utility and credibility of their contribution to client understanding and management of risk to national security, and
- their performance, in terms of the quality, efficiency, and security of the activity involved.

Over the reporting period Outputs 1 (Security Intelligence Analysis and Advice) and 2 (Protective Security Advice) provided advice to Ministers and other clients on the security environment, and on threats to national security related to people, property, and Government business and infrastructure.

Output 3 (Security Intelligence Investigation and Capability) contributed to the Outcome by investigations into threats to security and by maintaining and developing investigative capabilities.

And Output 4 (Foreign Intelligence) supported the Government's foreign intelligence outcomes.

The overall price for our Output Group was \$69.536m (see Figure 2).

*Figure 2. Price of ASIO's Outputs*

Output	Actual 1999-00 \$m	Estimated 2000-01 \$m	Actual 2000-01 \$m
Output Group 1: Security Intelligence	68.384	66.127	69.536

## Output 1: Security Intelligence Analysis and Advice

ASIO contributes to the Outcome of 'A secure Australia in a secure region' by providing useful and timely security intelligence analysis and advice on:

- foreign influenced politically motivated violence
- local politically motivated violence
- threat levels in Australia and to Australian interests abroad
- foreign interference and espionage
- protecting the National Information Infrastructure
- visa security checking, and
- release of archival documents.

ASIO prepares assessments, reports and briefings for Government decision-makers and client agencies to help them manage risks, and take appropriate steps to protect people, property, and Government business and infrastructure.

### PERFORMANCE

ASIO conducted a client feedback survey to assess the satisfaction of clients with the usefulness and timeliness of our reporting. Key clients were identified, incorporating a cross-section of Commonwealth departments, and police services which have responsibilities under the *National Anti-Terrorist Plan*. Interviews were conducted with a sample of clients, and comments sought on ASIO's performance generally, and on our reporting relating to:

- politically motivated violence resulting from events in the Middle East
- Threat Assessments
- Olympics reporting
- pre-CHOGM reporting, and
- anti-globalisation issues.

Overall, 96 percent of clients surveyed rated ASIO's product as always or usually useful — see Figure 3. Several respondents — long-time consumers of ASIO reporting — noted improvements in presentation and readability. Reporting containing unique intelligence was more highly valued than contextual reporting from open sources.

Fifty-four percent considered ASIO product to be always timely, while 41 percent said it was usually on time. We note a greater need for timely information for police clients, who use ASIO's information to inform tactical and resourcing decisions.



**Figure 3. Client feedback survey — usefulness and timeliness of ASIO product**

	Always useful	Usually useful	Sometimes useful	Rarely useful
% of responses	61%	35%	4%	0%
	Always timely	Usually on time	Sometimes late	Usually too late
% of responses	54%	41%	5%	0%

### Threat from foreign influenced politically motivated violence

Politically motivated violence can occur in Australia in response to ethnic, religious or political conflicts overseas.

Groups and individuals may express their concern about events overseas by taking action in Australia, which occasionally spills over into violent protest activity.

And some militant groups internationally view terrorism as a legitimate means of pursuing their cause and have the capability for global reach, for example Usama bin Laden (UBL). Some of them have a small number of supporters in Australia.



*Usama bin Laden*

#### **PERFORMANCE**

Our client feedback survey asked key clients about the value of ASIO's reporting of foreign influenced politically motivated violence resulting from events in the Middle East.

- Sixty-seven percent rated it always useful and 33 percent rated it as usually useful.
- Clients noted the value of the Australian perspective ASIO provides, with several commenting that this was not available from any other source.
- Several police services said they relied on ASIO's Middle Eastern reporting because it provided essential background as well as explanations of how international events could impact locally.

During 2000-01 the following analysis and advice contributed to managing and reducing the threat from foreign influenced politically motivated violence.

- Accurate advice to clients on the likelihood that individuals and groups in Australia would commit acts of politically motivated or communal violence in Australia, including to visiting dignitaries.
- Forewarning of potential threats to CHOGM, the Commonwealth Business Forum, the Olympic Games and the World Economic Forum, which provided a sound risk management basis for security planning by police services and Commonwealth agencies.
- Assistance to foreign liaison partners in their investigation of terrorist threats.

The remainder of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

### **Threat from local politically motivated violence**

*Investigative and analytical priority*

Our investigative focus was to identify and provide advice regarding those Australian groups and individuals assessed to be planning to undertake, or inciting others to undertake, acts of violence in support of their views.

Post-Olympics we placed particular emphasis on violent activities directed against CHOGM and the Commonwealth Business Forum, principally from Issue Motivated Groups.

#### **PERFORMANCE**

Our client feedback survey asked about the value of ASIO's reporting on threats to the Olympics and CHOGM, and reports on anti-globalisation issues.

- Clients commented favourably on ASIO's pre-Olympics reporting, with 71 percent rating it always useful and 19 percent usually useful.
- Police services appreciated receiving tactical information which assisted them to plan their own tactics in response to planned violence, and to more accurately assess resource requirements for particular events.
- A limited number of clients were asked to comment on the usefulness of ASIO's pre-CHOGM reporting. Of those, 87.5 percent found it always useful, and 12.5 percent usually useful.

The following analysis and advice contributed to reducing the threat from local politically motivated violence:

- Forewarning of potential threats to CHOGM, the Commonwealth Business Forum, the Olympic Games and the World Economic Forum which provided a sound risk management basis for security planning.

- Accurate advice of potential threats to Australian high office holders and minority communities.
- Analysis of the impact of anti-globalisation protests overseas, and accurate advice to clients regarding the likelihood of violent protests in Australia. The Commonwealth Business Forum and CHOGM provided a continuing focus for the coalitions of Issue Motivated Groups which emerged prior to the World Economic Forum in September 2000.



*World Economic Forum - September 2000*

The remainder of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

## Threat from foreign interference and espionage

ASIO advises Government on covert activity conducted on behalf of foreign governments. This includes espionage and attempts to interfere in the lives of people in Australia, or in political processes here or overseas.

Foreign agents are posted here to collect intelligence - sensitive official, military or political information, or scientific and technical knowledge or hardware. Foreign agents also report on, and sometimes intimidate people in Australia regarded as 'dissidents' by foreign governments. ASIO monitors the activities of these agents.

### PERFORMANCE

We continued to work closely with the Attorney-General's Department and other departments and agencies to update legislation covering espionage.

The remainder of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

## National Information Infrastructure Protection

ASIO is one of several agencies which carried out further development and research of initiatives on National Information Infrastructure (NII) protection.

Protection of the NII is part of a broader national approach to electronic security.

ASIO's NII protection role relates to its security intelligence and protective security responsibilities. Specific funding was provided for 2000-01.

### PERFORMANCE

We established a dedicated NII protection team, and produced 14 assessments of the threat to specific Government computer systems.

- In conjunction with other agencies we completed a threats and vulnerabilities study of four Australian infrastructure sectors.
- A Security Intelligence Report on computer network attack during the Olympics was issued in conjunction with the Australian Federal Police.

We continued building international relationships in the NII area with traditional intelligence partners on a multi-lateral and bi-lateral basis. Joint Operating Arrangements supporting national and international threat and vulnerability assessment, analysis and response were agreed with AFP and DSD.

The remainder of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

*Outlook*

Funding was provided for 2001-02 to continue development of our NII capability. We will build on the gains made in this reporting period by:

- Further developing our capability to collect information in a coordinated and sustained way, to analyse that information, and provide accurate advice to Government on the threat to public and private sector infrastructure from computer network attack.
- Building knowledge of vulnerabilities in critical infrastructure through further engagement with industry sectors.
- Developing a modest investigative capability, to work with other agencies such as DSD and the AFP as necessary.
- Participating in the development of a protective security program for critical infrastructure.
- Contributing to policy development on NII protection.

**Threat levels in Australia and to Australian interests overseas**

ASIO provides advice in the form of Threat Assessments that seek to provide forewarning of politically motivated violence and foreign intelligence attacks in Australia, and to Australian interests abroad.

Most are prepared in response to requests from the Protective Security Coordination Centre in the Attorney-General's Department.

Many Threat Assessments address threats to Australian high office holders in Australia or overseas, or the safety of foreign dignitaries visiting Australia.



*Prime Minister Howard greets Indonesian President Wahid  
- June 2001*

We also provide longer-term Threat Assessments on:

- threats to diplomatic and consular interests in Australia
- threats to ministerial residences and electorate offices, Government buildings and defence establishments
- threats to aviation interests, and
- the overall threat from politically motivated violence — prepared on a biannual basis.

**PERFORMANCE**

Sixty-one percent of clients surveyed rated ASIO Threat Assessments as always useful, and 31 percent as usually useful.

- While clients generally were satisfied with ASIO's Threat Assessments, they reinforced the need for timeliness, as Threat Assessments are valuable for planning deployment of police resources to prevent or limit the occurrence of violence.
- Several commented favourably on ASIO's willingness to address factors police consider important, and to provide verbal and timely interim advice as required.
- Some clients warned of the need to avoid jargon in our reports, and against a tendency sometimes to over-classify documents.
- Country Threat Assessments issued during the Olympics were used, and indeed still are used by police services as valued background briefing material.

**Trends**

The high number of Threat Assessments noted last year continued in 2000-01 — see Figure 4.

Demonstration notifications more than doubled, due largely to the anti-globalisation protest activity and to protests linked to policy on unauthorised arrivals and refugees.

**CHOGM security**

We produced 25 CHOGM Country Threat Assessments covering 51 countries, providing clients at both the Federal and State level with advice on the threat to the CHOGM member countries and related infrastructure.

These will be reviewed in the lead-up to CHOGM, and updated Threat Assessments will be issued for those countries assessed to be at greatest threat.

A part of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

**Figure 4. Threat Assessments issued**

SUBJECT OF ASSESSMENT	96-97	97-98	98-99	99-00	00-01
Visiting dignitaries	137	106	107	131	79
Australian dignitaries	254	238	347	552	503
Australian interests					122
Demonstration notifications	62	71	63	48	100
Diplomatic premises	90	113	208	164	77
Protective security	43	39	30	34	27
Other threat assessments	58	54	84	69	37
National Information Infrastructure Protection	-	-	-	6	14
Olympic Games 2000	-	-	46	342	354
CHOGM	-	-	-	-	29
<b>TOTAL</b>	<b>644</b>	<b>621</b>	<b>885</b>	<b>1 346</b>	<b>1 342</b>

Note - 'Australian interests' was previously reported in the 'Other Threat Assessments' category

## Visa security checking

Australia's border control mechanisms are an essential tool in minimising the risk of terrorists entering Australia. ASIO is the principal source of advice to DIMA on the entry to Australia of people of security significance.

We assess whether people applying for entry or permanent residence have the potential to conduct terrorist activity, espionage or foreign interference, and provide a security assessment advising whether a person is a risk to national security.

ASIO is represented on the DIMA-chaired Border Control Coordination Group.

### PERFORMANCE

Just over 96 percent of temporary visa applications, and 88 percent of permanent visa applications were assessed within agreed timeframes.

Delays in assessments were largely caused by the need to conduct checks with overseas authorities, and to clarify incomplete visa applicant information.

*Visa refusals*

- On ASIO advice two visa applicants were refused entry to Australia because they were assessed as likely to engage in espionage activities. A third person was also assessed as likely to engage in espionage and the existing visa was cancelled.
- A fourth applicant was refused a protection visa when we assessed an involvement in politically motivated violence represented a risk to national security. A fifth person's visa was cancelled because of an identified link to a terrorist group. — see Figure 5.

**Figure 5. Prejudicial security assessments for visa applicants 96-97 to 00-01**

	1996-97	1997-98	1998-99	1999-00	2000-01
Prejudicial assessments	15	11	9	4	5

*Trends*

Excluding unauthorised arrivals and Olympic-specific work, there was a 36.5 percent increase in the number of visa security checks in 2000-01. This continued the trend noted last year — see Figure 6.

**Figure 6. Visa security assessments 96-97 to 00-01**

Type of entry	1996-97	1997-98	1998-99	1999-00	2000-01
Temporary	11 929	10 364	10 015	16 483	26 527
Permanent	5 552	7 156	8 107	8 371	7 392
<b>Total</b>	<b>17 481</b>	<b>17 520</b>	<b>18 122</b>	<b>24 854</b>	<b>33 919</b>

These figures do not include security assessments of unauthorised arrivals held in detention or of Olympic Family Members

*Unauthorised arrivals*

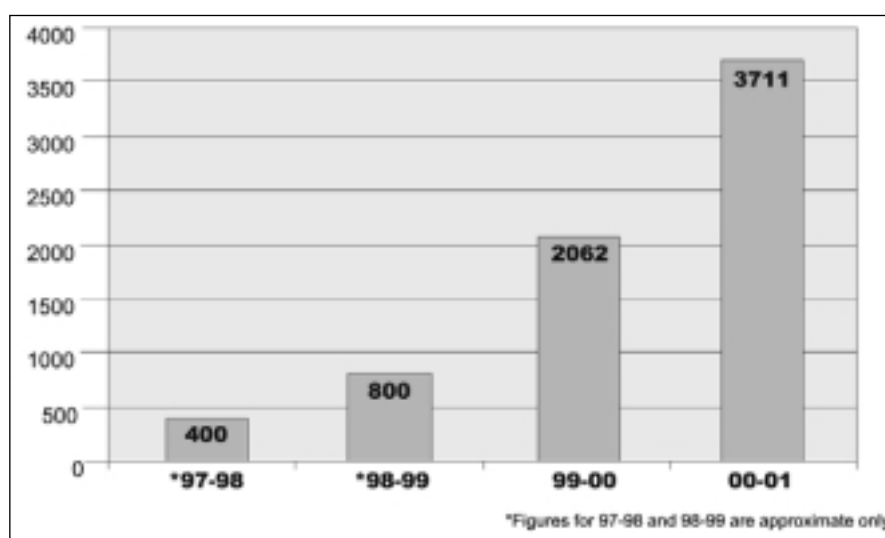
Unauthorised arrivals continued at the high level noted in 1999-00 with 4 141 arrivals by boat and 1 508 by air.

The majority of unauthorised arrivals claimed to have come from Iraq, Afghanistan or Iran. While not all unauthorised arrivals require security assessments, a high proportion do — see Figure 7. ASIO continued to direct additional resources to this task, and efficiencies introduced in cooperation with DIMA the previous year worked well.

We issued 3 658 security assessments compared to 2 739 the previous year — a 34 percent increase.

As of 30 June 2001, 565 cases were awaiting resolution by ASIO. No cases remained in detention for more than six months solely because an ASIO assessment was outstanding.



**Figure 7. Unauthorised arrivals referred to ASIO for security assessment****Olympic Family Members**

In the lead-up to and during the 2000 Olympics ASIO assisted in the prompt resolution of security alerts relating to incoming passengers of potential security concern, and to Olympic Family Members who were subject to the same security checking requirements as other visitors.

The remainder of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

**Release of archival documents**

ASIO is an exempt agency under the *Freedom of Information Act 1982*, but is not exempt from the information access provisions of the *Archives Act 1983*.

**Access to records**

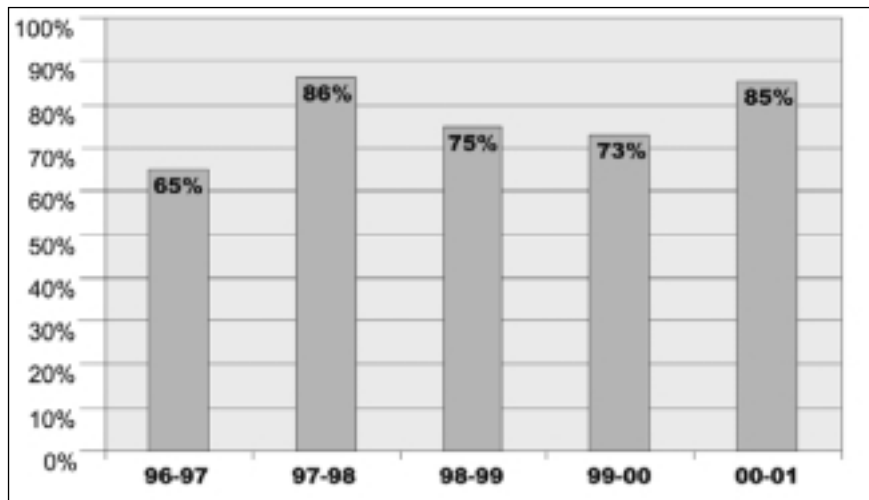
Researchers and other members of the public can apply to the National Archives of Australia for access to ASIO records that are at least 30 years old. When the National Archives does not already hold records on the subject, it passes the access applications to ASIO. We locate and assess relevant records and provide advice to the National Archives about whether or not they contain information that should be exempted from public release under section 33 of the *Archives Act*.

Applicants who are dissatisfied with exemptions claimed by ASIO can request an internal reconsideration of the decision. Applicants can also appeal to the Administrative Appeals Tribunal (AAT) which may uphold the original decision or grant access to all or part of a record.

**PERFORMANCE**

Eighty-five percent of the applications due for completion during the reporting period were completed within the statutory timeframe of 90 days, against a benchmark of 80 percent. This is our best performance since 1997-98, and a considerable improvement over last year — see Figure 8.

*Figure 8. Percentage of Archival requests satisfied within 90 days*



We increased the number of staff working on access assessment in the second half of 2000-01. This was effective in eliminating the backlog that developed over the Olympics period, when all but one of the staff members working on archives matters were re-deployed to other security intelligence priorities.

The 197 applications that were due to be completed in 2000-01 sought access to 231 separate items or subjects. Sixteen percent were for items that were either not recorded in our indexes or for which there were no ASIO records in the open access period.

Forty-three applications were from people seeking records about themselves or members of their family. All were completed within 90 days.

Access applications from one researcher absorbed around 20 percent of ASIO's archives resources during the period. A further 25 percent of resources were devoted to completing requests carried forward from previous years.

Altogether, 220 access applications were completed during the period. Those applications sought access to 270 separate items or subjects. The total number of folios (pages) assessed was 31 289.

*Exemption claims*

Figure 9 shows the distribution of exemption decisions made to folios. ASIO only recommends exemptions where disclosure of the information could damage national security or expose the existence or identity of a confidential source.

**Figure 9. Distribution of exemption claims across assessed folios**

	99-00	00-01
Folios released without exemption	21%	28%
Folios released with part of the text claimed as exempt	60%	58%
Folios claimed as totally exempt and not released	19%	14%
Total folios assessed	100%	100%

**Appeals**

We received 17 applications for internal reconsideration and completed 10. In most cases, they resulted in minor or no change to the original exemption decisions.

No AAT appeals relating to ASIO records were heard during the reporting period. As of 30 June, one appeal was lodged and a hearing was expected to take place in November 2001.

No part of this performance report has been excluded from the unclassified *Report to Parliament*.

### **The Wispelaere case**

Jean-Philippe Wispelaere, an Australian citizen and former Defence Intelligence Organisation (DIO) employee, was arrested at Washington's Dulles Airport on 15 May 1999 and charged with attempted espionage. Wispelaere had unlawfully removed classified documents from DIO, and had attempted to sell them to representatives of a foreign Government in Thailand.

The investigation preceding his arrest was conducted jointly by the FBI, ASIO and the AFP. Following Wispelaere's arrest, ASIO worked closely with the Attorney-General's Department, the AFP and US authorities in relation to the case.

Wispelaere's trial was delayed as a result of concerns about his mental competency. Following medical treatment, on 27 September 2000 the US District Court for the Eastern District of Virginia found Wispelaere was competent to stand trial. On 8 March 2001 he pleaded guilty to one charge of attempted espionage under a plea agreement with the prosecution. Wispelaere was sentenced to 15 years imprisonment. Under the agreement, Wispelaere may request to be transferred to Australia after he has served ten years imprisonment in the USA.

### **The Lappas Dowling case**

In July 2000 the AFP charged Simon Lappas, an employee of DIO, and Sherryll Dowling, an escort with whom Lappas had formed a relationship, with offences under the official secrets provisions of the *Crimes Act 1914*. It was alleged that Lappas removed classified documents from DIO, and passed them to Dowling with instructions to sell the documents to a foreign embassy in Canberra. Lappas and Dowling were granted bail.

On 1 May 2001 Lappas and Dowling were committed for trial in the Supreme Court of the ACT. All the evidence in the committal hearing was taken in camera. The trial is set down to commence in November 2001.

ASIO worked with the Attorney-General's Department and the AFP on aspects of the investigation and prosecution.

## Output 2: Protective Security Advice

ASIO advises Government departments and agencies on the protection of Government business and national infrastructure.

Output 2 contributed to the Government Outcome of 'A secure Australia' by:

- Providing advice on personnel security (security assessments for people who require access to national security classified information or secure places).
- Providing advice on physical security (the security of Government buildings and infrastructure).

### Security in Government

The Inspector-General of Intelligence and Security, Mr Bill Blick, undertook a review of security procedures within the Commonwealth following the arrest of Jean-Philippe Wispelaere.

The *Inquiry into Security Issues* (the *Blick Report*) made over 50 major recommendations directed at implementing best security practice across the Commonwealth and the Australian Intelligence Community (AIC).

A key recommendation aimed at enhancing security coordination across the AIC was the establishment of an Inter-Agency Security Forum (IASF). The forum has senior representatives of AIC agencies and major policy departments (Defence, PM&C, the Attorney-Generals' Department, Treasury and DFAT).

The IASF is responsible for:

- providing a high level forum for the consideration of security policy across the AIC
- providing a consultative mechanism to achieve and maintain best security practice
- ensuring that security issues receive timely and comprehensive consideration
- obtaining and communicating information and advice on emerging security issues
- developing advice for agency management of security issues, and
- assisting the Protective Security Policy Committee (PSPC) in its responsibilities for overall security policy across Commonwealth agencies.

#### *Inter-Agency Security Forum*

The IASF held its first three meetings in 2000-01, and several recommendations from the *Blick Report* were implemented - with greatest priority given to recommendations relating to personnel security.

Each agency is required to submit an annual security report to the Secretaries Committee on National Security (SCNS), with ASIO providing an overview of the status of security in each of the agencies. The first report is to be provided to Government in late 2001/ early 2002.

## Personnel security

Before granting a security clearance to a candidate for a 'designated security assessment position' Commonwealth agencies are required to assess the person's general suitability for access. Once that is satisfied, ASIO provides advice to agencies, in the form of a security assessment, on whether anything in the candidate's background or activities is a cause for security concern.

The advice is usually based on an assessment of material provided by the relevant agency. ASIO sometimes interviews people where it is relevant to the resolution of security issues. Psychological testing, where it is part of an agency's procedures, is the responsibility of the agency and does not involve ASIO.

ASIO either advises agencies that it does not recommend against the candidate, or it issues an adverse or qualified assessment.

- An adverse assessment is a recommendation that a person should not be granted the access proposed.
- A qualified assessment does not recommend against access, but provides information that ASIO considers may need to be considered in decision-making. Qualified assessments also provide the requesting agency with information to help minimise the potential for the compromise of sensitive information.

The decision to grant or deny a security clearance rests with the agency.

### PERFORMANCE

We fell well short in our performance against all benchmarks. 55.4 percent of requests were incomplete after 12 weeks, against a benchmark of one percent.

**Figure 10. Personnel security clearances - performance against benchmarks**

Performance measure	Target	Performance
Complete within 14 days	75%	14.7%
Complete within 21 days	90%	15.3%
Remaining incomplete after 12 weeks	1%	55.4%

One factor impacting on our performance was the need to provide security assessment advice for individuals involved in the Sydney Olympics. Between 1 July 2000 and the end of the Games we provided advice to the NSW Police on more than 94 000 people who required access to secure Olympics sites. The major reason for the shortfall, however, was the introduction of a new IT system which was not adequately worked through prior to implementation. The problem was rectified, and the backlog of assessment requests reduced from a peak of 3 500 to 1 900 by 30 June 2001.

An automated checking process being developed with the Defence Department was significantly delayed, but will be progressed in 2001-02 with the aim of providing an improved service to Defence, our main client for security assessment advice, and to other clients in the longer-term.

#### *Trends*

ASIO received 11 107 requests for security assessments in 2000-01 (not including Olympics-related security checks) — a decrease over the previous year and a reversal of the trend noted in recent years — see Figure 11.

*Figure 11. Personnel security clearances - annual workloads*

Level of access	96-97	97-98	98-99	99-00	00-01
Confidential	887	1 169	1 038	1 163	969
Secret	5 304	5 398	5 909	6 658	5 803
Top Secret	3 520	4 280	4 453	4 650	4 335
<b>Total</b>	<b>9 711</b>	<b>10 847</b>	<b>11 400</b>	<b>12 471</b>	<b>11 107</b>

#### *Adverse and qualified assessments*

Two adverse and 10 qualified assessments were issued.

*Figure 12. Adverse and qualified personnel security assessments*

	96-97	97-98	98-99	99-00	00-01
Qualified assessments	2	4	4	12	10
Adverse assessments	1	3	1	1	2
<b>Total</b>	<b>3</b>	<b>7</b>	<b>5</b>	<b>13</b>	<b>12</b>

#### *Appeals*

Individuals have a right of appeal to the Administrative Appeals Tribunal (the AAT) in respect of an adverse or qualified ASIO security assessment.

Three appeals were lodged during 2000-01, with one later withdrawn.

The AAT heard one appeal against a qualified assessment made in 1999-00 and subsequently affirmed the decision made by ASIO. The appeals lodged in 2000-01 had not been heard by 30 June 2001.

**CHOGM**

A process for providing security assessment advice on people requiring access to secure CHOGM sites was developed. The system will use processes developed for the Olympics, although the workload will be much smaller than for the Olympics.

**Polygraph trial**

ASIO began preparations for an internal and voluntary trial of the polygraph to assist in determining its potential future utility as a personnel security tool. The trial was one of the recommendations in the *Blick Report*. There will not be any public reporting on the precise progress of the trial.

The remainder of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

### Protective security advice

ASIO provides protective security policy advice to Government, and specific advice to individual departments and agencies on protective security measures. This advice includes:

- protective security and risk management advice and training
- setting security equipment standards and testing equipment against those standards, and
- electronic and audio surveillance counter-measures advice and action.

### Cost recovery

**PERFORMANCE**

ASIO's protective security advice and services are now provided on a full cost recovery basis. During 2000-01 we provided advice to 108 Commonwealth clients, recovering \$498 000 — a 100 percent increase over the previous year, following the introduction of full cost recovery in February 2000. A notional cost of \$232 000 represented work undertaken for ASIO — see Figures 13 and 14.

*Figure 13. Cost Recovery*

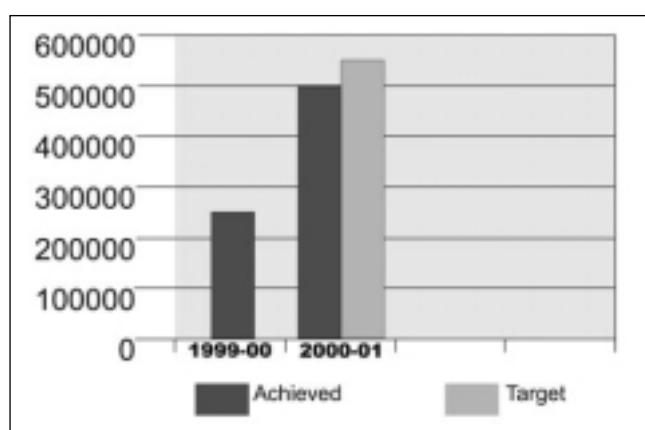
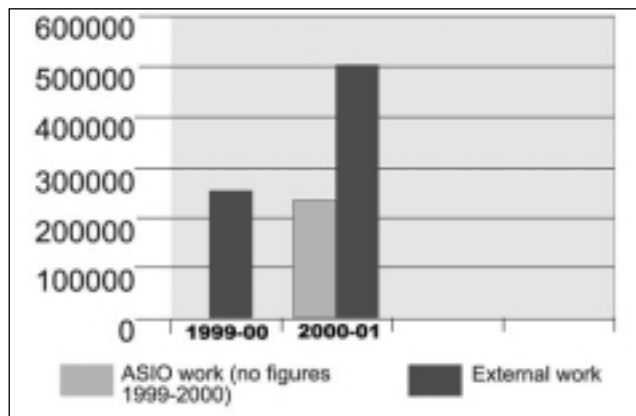




Figure 14. Value of external work and ASIO work



In October 2000, Ernst and Young were engaged to advise on further measures to improve the efficiency of the protective security output and increase the level of cost recovery. A final report is expected in September 2001.

## Protective security and risk management advice and training

### Risk reviews

ASIO provides holistic protective security advice to Government agencies and other clients. These involve comprehensive, integrated reviews of security risks and vulnerabilities, and the development of recommended protective security measures, using risk-based methodology.

During 2000-01 ASIO undertook two large protective security risk reviews and 38 smaller protective security risk reviews. Reviews were undertaken for:

- the Department of Finance and Administration (DoFA) in Canberra
- the Victorian Parliament before the meeting of the combined Houses of the Federal Parliament in May 2001 for the Centenary of Federation celebrations
- the National Archives of Australia regarding the secure storage and display of Centenary of Federation documents
- the Australian Nuclear Science and Technology Organisation on the proposed protective security measures for the new nuclear reactor at Lucas Heights
- the Australian Radiation Protection and Nuclear Safety Agency's offices in Sydney and Melbourne
- the Australian Customs Service regarding the storage, handling and control of firearms
- DoFA regarding the HIH Royal Commission

- the Department of Defence concerning the safe-hand delivery of classified documents to selected overseas destinations
- the Department of the Environment and Heritage on enhanced physical security for its Melbourne facility which contains the largest Halon gas supply in the Southern Hemisphere
- the refurbishment of the Treasury building in Canberra, and
- Queensland Police and the CHOGM Task Force on CHOGM security, including advice on security risk management and venue security plans.

Significant outcomes for clients included:

- a cost saving to Treasury as a result of early engagement in the planning, construction and refurbishment projects.
- enhanced physical and personnel protective security measures in DoFA, Treasury and the Australian Radiation Protection and Nuclear Safety Agency, and
- protective security training for staff at the Civil Aviation Safety Authority.

*Gatekeeper accreditation*

With DSD we conducted Gatekeeper/Public Key Information Accreditation of 10 private sector information technology providers to Government agencies. This compares with 11 in 1999-00 and one in 1998-99.

- One of the accredited companies is now using ASIO's security recommendations for building design and layout as a template for new IT facilities worldwide.

The focus of ASIO's accreditation role began changing in 2000-01 from accreditation of individual sites, to more generic advice through the National Office of the Information Economy.

*Trends*

Demand for ASIO's protective security advice is growing as departments and agencies seek advice on the implementation of measures required by the new *Protective Security Manual*, and as intelligence agencies adopt recommendations from the *Blick Report* to improve standards of physical security.

To meet these demands, ASIO will employ additional contract staff, funded from cost-recovery.

*Top Secret accreditation*

ASIO has a new responsibility to accredit all Top Secret facilities in Australia (over 440 sites including Defence facilities).

In late 2001 we will commence a rolling five-year program of inspections. Priority will be given to AIC and major policy departments.

## Security equipment standards

### *Equipment testing*

ASIO tests security products on behalf of the interdepartmental Security Construction and Equipment Committee (SCEC) which reports to the Protective Security Policy Committee.

The 2000-01 testing program was not completed, and production of the new edition of the *Security Equipment Catalogue* was delayed as resources were diverted to meet the heavy demand for protective security risk reviews. Additional resources will be directed to these tasks in 2001-02.

ASIO tested a range of products, including:

- security briefcases
- security straps, seals and identification labels
- shredders
- security fences, and
- video motion detection systems.

### *Security Construction Reference Manual*

ASIO and the Department of Defence commenced development of a *Security Construction Reference Manual*. This manual has the potential for wider application across Government and is expected to reduce security system design effort and development costs.

The remainder of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

## Output 3: Security intelligence investigation and capability

To investigate threats to national security ASIO must develop and maintain specialised human and technical capabilities in a continually changing security and operational environment.

Output 3 is delivered through a range of integrated activities, each a key contributor to ASIO's security intelligence collection capability. These include:

- warrant operations, which may include:
  - telecommunications interception
  - covert entry and search of premises
  - interception of postal and delivery service articles
  - the use of listening devices and tracking devices
  - computer access
- human source intelligence collection
- surveillance
- collection of information from open sources
- liaison with other Australian stakeholders
- liaison with overseas security and intelligence partners
- support to the National Anti-Terrorist Plan, and
- technical research and development.

All operational activity by ASIO must comply with the Attorney-General's *Guidelines for the Collection of Intelligence* which require ASIO to use only methods of investigation that are appropriate to the assessed risk.

### PERFORMANCE

Output 3 contributed to the Government Outcome of 'A secure Australia' by:

- investigating threats to security - particularly threats from politically motivated violence - to contribute to Outputs 1 and 2 (Security Intelligence Analysis and Advice, and Protective Security Advice), and
- maintaining and developing investigative capabilities.

A large part of this performance report is excluded from the unclassified *Report to Parliament* because of security sensitivity.

## Warrant operations

### *Special powers*

Legislation enables ASIO, subject to approval by the Attorney-General, to use intrusive methods of investigation such as telecommunications interception, listening devices, entry and search of premises, computer access, tracking devices and examination of postal and delivery service articles.

The number of warrants varies over time, in response to the changing security environment.

### *Warrant approvals*

Only the Director-General can seek a warrant. A written statement specifying the grounds on which it is considered necessary to conduct an intrusive investigation must accompany each warrant.

Warrants submitted for approval by the Attorney-General go through a system of checks within ASIO, including examination by the ASIO Legal Adviser. And a senior official of the Attorney-General's Department independently advises the Attorney-General on whether the relevant statutory requirements have been met.

Warrants are issued for specified limited periods. At the expiry of each warrant ASIO must report to the Attorney-General on the extent to which the operation helped ASIO carry out its functions.

All warrant requests put to the Attorney-General were approved, although some proposals were either rejected or modified before being submitted to the Attorney-General, as part of the normal consideration of warrant requests within ASIO.

### *External scrutiny*

The Inspector-General of Intelligence and Security has access to all warrant material and regularly monitors the process.

During the reporting period the Inspector-General continued his audit of ASIO's warrant documentation. In his *2000-01 Annual Report*, the Inspector-General noted that in each of the cases he reviewed he was satisfied that ASIO had:

- reasonable grounds for seeking a warrant for the use of special powers
- provided sufficient information for the Attorney-General to make an informed decision on whether or not to approve the warrant
- put appropriate procedures in place to monitor that the conditions of the warrant were being fulfilled, and
- reported the results of warrant operations to the Attorney-General in a balanced and timely manner.

The Inspector-General noted four cases of inadvertent unauthorised telephone interception. In each case he found that ASIO had taken

appropriate action to correct the error, and that product from the interception had been destroyed.

## **Telecommunications interception**

Telecommunications interception can only occur subject to a warrant approved by the Attorney-General. The *Telecommunications Act 1997* requires all telecommunications carriers (which own parts of the physical network) and carriage service providers (which only provide communications services) to provide interception capabilities - unless specifically exempted. Internet service providers also have to provide interception capability. The purpose of telecommunications interception is to capture communications to or between people of security interest.

### *Funding*

Telecommunications providers are responsible for the development costs of interception capabilities, with intercepting agencies required to pay delivery and any agency-specific formatting costs.

### *Encryption*

Publicly available robust encryption, driven principally by e-commerce requirements, is expected to be a major challenge in coming years.

### *The commercial environment*

Volatility in the telecommunications sector continued during 2000-01. Growth in the number of carriers and carriage service providers continued to require a significant investment to ensure the interceptibility of new services. By 30 June 2001 there were 76 licensed telecommunications carriers in Australia, compared to 46 in June 2000, and three in 1995. Carriage service providers number in the hundreds.

### *Foreign ownership*

2000-01 also saw investment by telecommunications companies with links to foreign governments. In particular, SingTel made a bid for Optus, Australia's second largest carrier, and one with investments across the telecommunications industry.

### *Partnerships with industry*

The Australian Communication Authority's Law Enforcement Advisory Committee continued to be a valuable forum for exchanges between intercepting agencies, regulators, and industry representatives.

## **Human source intelligence collection**

ASIO collects intelligence by recruiting and managing human sources - people who are willing to provide information about individuals, groups or foreign governments of security interest.

We also conduct declared overt interviews of members of the public or targets to assist with our investigations.

A well-placed human source can provide ASIO with valuable information about security issues, but they can take a long time to recruit and develop. We invest significant resources to develop expert human source management skills in our intelligence officers.

*CHOGM  
security*

Our Olympics interview program, in which we established overt contact with 98 different communities, provided the basis of our CHOGM interview program.

By 30 June 2001 we had established overt contact with 84 communities, to explain ASIO's role in CHOGM security, and to gather information about possible threats.

*Preventative &  
disruption  
operations*

We will undertake a sharply focused Preventative Interview Program prior to CHOGM. The program will focus on people associated with targets with a current or past connection to politically motivated violence.

A number of disruption operations were conducted as part of our pre-Olympics planning.

*Human source  
management*

We continually review our human source base to ensure we are obtaining maximum returns against resource allocations. During 2000-01 a review of human sources resulted in the de-registration of several sources who were no longer providing information relevant to intelligence requirements.

## **Surveillance**

ASIO surveillance teams report on people of security interest.

Surveillance operations provided pre-emptive intelligence in the lead-up to, and during the Sydney 2000 Olympics, and provided good intelligence in support of ongoing investigations and operational planning.

## **Open source information collection**

ASIO's use of open source information increased markedly during 2000-01. Information publicly available through commercial publications and electronic sources provided a valuable adjunct to our covert collection strategies, particularly in terms of monitoring the global and strategic environment.

An evaluation of the Open Source Unit which was established in 1999-00 found it played a pivotal role in ASIO's ability to report on global issues and developments, and monitor rapidly evolving situations.

Electronic delivery to the desktop was improved through the use of an electronic document management system.

## **Liaison with Australian agencies**

ASIO continued to rely on strong cooperative partnerships with Commonwealth and State agencies to help advance investigations and provide access to information to identify and monitor individuals of security interest.

The sharing of information between ASIO and other agencies is regulated by the *ASIO Act*, and monitored by the Inspector-General of Intelligence and Security.

The benefit of establishing and maintaining effective strategic partnerships was particularly evident in the context of the Sydney 2000 Olympics. Significant support was provided to ASIO's Olympics-related investigations from a range of agencies including the NSW Police, AFP, DSD, DIMA, ASIS, DFAT, Defence and a number of communication carriers. And many agencies contributed staff to the Federal Olympic Security Intelligence Centre. The closeness of these relationships significantly contributed to a safe and secure Olympics.

ASIO is working hard to ensure these effective relationships are maintained and utilised to similar effect for CHOGM.

ASIO's senior management continued to meet biannually with the senior management teams of ASIS, DSD and the AFP. The meetings focused on reviewing cooperative arrangements, identifying opportunities to share resources and capabilities, and strategic directions.

### *Law enforcement agencies*

Law enforcement agencies continued to provide support for ASIO security investigations and operations. This support included protection to ASIO officers interviewing violence-prone individuals, and support for ASIO Entry and Search operations where there was a likelihood that weapons would be present.

Law enforcement agencies also provided protection to ASIO surveillance officers on deployment against individuals known or suspected of carrying firearms.

### *NSW Police*

A particularly strong relationship was established with the NSW Police in preparation for the Olympics. We engaged in several pre-Olympic exercises, undertook a number of joint investigations, and seconded officers to the NSW Police Olympic Intelligence Centre. Regular briefings on the security environment were provided to the NSW Police Commissioner and his deputies.

### *Victorian Police*

A close and mutually productive relationship was maintained with the Victorian Police in relation to the World Economic Forum in Melbourne in September 2000. This included the exchange of information, and ASIO support to the police intelligence cell.



*Queensland  
Police*

ASIO's relationship with the Queensland Police strengthened as we focused on preparations for CHOGM. And we expanded our reporting mechanisms to ensure the Queensland Police Force is informed on emerging security issues.

*Defence*

Defence staff participated in the Federal Olympic Security Intelligence Centre.

## **Liaison with overseas partners**

ASIO's legislation authorises communication with security and intelligence authorities of other countries approved by the Attorney-General. Foreign services provide ASIO with access to security and intelligence information we cannot collect by other means, particularly in relation to threats to Australia's security originating off-shore, or in response to events overseas. Foreign services also provide ASIO with access to leading-edge technology and benchmarking opportunities with similar organisations.

*Strategic  
relationships*

ASIO liaison staff maintain strategic partnerships with agencies in their regions. During 2000-01, 12 new relationships were established. At 30 June 2001 we had liaison relationships with 228 organisations in 104 countries and territories.

*Significant  
visits*

During 2000-01 we hosted visits of senior officers from several liaison partners. The visits addressed matters of mutual interest, as well as Olympics and CHOGM-related arrangements.

*Olympics  
support*

ASIO is a member of the Greek Olympic Security Advisory Group (OAG). The OAG was formed by the Greek Government to provide security advice to Greek authorities in relation to the Athens 2004 Olympic Games. This assistance will continue in 2001-02.

## **Joint operations**

The support of overseas intelligence agencies is essential to ASIO's work. In return we respond to requests for information and assistance.

A decision to communicate information about Australian citizens to a foreign service is only made after a range of factors are considered, particularly the foreign government's regard for human rights, and the strength of the intelligence relationship between ASIO and the foreign service. Any intelligence passed must be relevant to the security of the country requesting the information.

The Inspector-General of Intelligence and Security monitors the flow of such information.

## Counter Terrorism Support

ASIO is a member of the two major committees coordinating Australia's counter-terrorist capability:

- the Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence (SAC-PAV), and
- the Special Inter-Departmental Committee on Protection Against Violence (SIDC-PAV).

Our role is twofold. We help in the prevention of terrorism through our intelligence collection and reporting, and through our participation in counter-terrorism training courses and exercises. We also contribute to counter-terrorism policy development, and crisis contingency planning.

### *CTORG*

ASIO is also a member of the DFAT-chaired Counter-Terrorist (Overseas) Response Group (CTORG) which coordinates policy development and management of Australia's response to terrorist incidents overseas involving Australian citizens, or requests for assistance from foreign governments. In the event of an incident, ASIO is responsible for coordinating security intelligence.

During 2000-01 ASIO worked with other CTORG agencies to develop our response capability.

### *National Anti-Terrorist Plan*

Under the *National Anti-Terrorist Plan* ASIO hosts and maintains the National Intelligence Group (NIG) which coordinates intelligence collection and strategic assessments during terrorist incidents and counter-terrorism exercises. We also participate in the Joint Intelligence Group, an operational intelligence unit established by the State or Territory police.

### *National counter-terrorism exercises*

During 2000-01 we focused on refining and testing our counter-terrorism response capabilities prior to the Olympic Games and CHOGM.

Our capabilities were fully tested in a SAC-PAV National Exercise in Queensland in June 2001. Our involvement included participation in exercise planning and control, and activated the full range of national, regional and incident site machinery, including the NIG, and deployment of the Technical Support Unit.

We participated in three other major SAC-PAV training exercises - two in Queensland and one in Western Australia, as well as a range of other counter-terrorist exercises with various police services.

## Technical Development

Investment in technical capability remained critical to our ability to undertake technical collection operations.

ASIO maintains a small technical development group, which conducts limited, in-house development work and manages technical equipment acquisition, and outsourced development projects. We also develop effective technology-sharing arrangements with our liaison partners.

Technical collection capabilities maintained and developed during the year included telecommunications interception and related delivery, processing and monitoring systems.

## Output 4: Foreign Intelligence

Output 4 contributes to the Government Outcome of 'A secure Australia' by collecting foreign intelligence in Australia on behalf of ASIS and DSD under warrant, and incidentally through ASIO's security intelligence investigations and liaison with overseas partners.

**PERFORMANCE**

This performance report is excluded, in its entirety, from the unclassified *Report to Parliament* because of security sensitivity.



Part 3  
**management  
and  
accountability**

Figure 15. Corporate governance structure



## Corporate Governance

Corporate governance is exercised through a Corporate Executive that supports the Director-General in managing and setting the strategic direction for ASIO. An Audit and Evaluation Committee and other corporate committees which review security, intelligence, human resource and information management issues support the Corporate Executive. A Consultative Council, comprising representatives from management and ASIO staff provides a forum for employment and conditions of service issues.

The Director-General chairs the Corporate Executive, which includes the Deputy and First Assistant Directors-General, an SES branch head on a rotational basis, and the President of the ASIO Staff Association as an observer. The Corporate Executive meets twice monthly and otherwise as required.

The Audit and Evaluation Committee is chaired by the Deputy Director-General, and includes an SES officer from the Australian National Audit Office (ANAO). Other corporate committees are shown in Figure 15.

ASIO reports annually to the Attorney-General by means of a classified *Annual Report* which is also provided to the National Security Committee of Cabinet, and an unclassified *Report to Parliament*. Financial activities are regularly audited, and certain budgetary details published in the annual Budget Papers.

### *Corporate planning*

We began revising ASIO's *Corporate Plan 1998-2000*. The revised plan will be completed early in the next reporting period, and will look out to 2005. Staff input to the plan will be sought through a series of meetings to discuss ASIO's mission, vision, values, objectives and performance indicators. The revised plan will be a public document, and will be included on our website at [www.asio.gov.au](http://www.asio.gov.au).

ASIO has a range of other plans in place, including the *Information Management Strategy*, the *Security Management Plan*, and the *People Management Plan*.

- The *Information Management Strategy* is being revised for consideration by the Corporate Executive in late 2001. The plan will build on that developed in 1998 and will project out to 2005.
- ASIO's *Security Management Plan 2001-2004* was approved by ASIO's Security Committee and endorsed by the Corporate Executive in March 2001. The plan sets out the objectives and strategies needed to manage security within ASIO.
- Our *People Management Plan* is being updated with emphasis on the need to attract and retain high quality staff. The new plan will span the period 2001-2005 and will be completed in the next reporting period.

## Accountability

ASIO's effectiveness lies in our ability to collect and make use of secret information, which those under investigation may try to hide. ASIO investigations can be intrusive, so we adhere to a range of accountability measures and safeguards that govern the way we operate - internal evaluation, audit and fraud control measures, external accountability — including through the Inspector-General of Intelligence and Security — and arrangements governing our interface with the public.

### **Audit, Evaluation and Fraud Control**

ASIO's program of internal and external reviews and evaluations continued, overseen by the Audit and Evaluation Committee.

#### *Fraud Control Plan*

The *Fraud Control Plan* was revised. The Interdepartmental Fraud Control Evaluation Committee, chaired by the Attorney-General's Department, assessed the plan as meeting the requirements of the Fraud Control Policy of the Commonwealth. The plan draws on a Fraud Risk Assessment conducted in 1999-00 by consultants Walter and Turnbull, which rated ASIO's overall risk as moderate (on a scale of low, moderate, high and extreme). A range of measures were put in place to address areas identified as at most risk.

A series of seminars, and the inclusion of fraud control segments on other internal training courses, raised staff awareness of the issue.

#### *Evaluations*

Three evaluations were conducted in 2000-01:

- Consultants Ernst and Young reviewed the Physical Protective Security (T4) business structure which resulted in the re-engineering of a number of business processes to enhance T4's strategic planning capability and establish a better business model with an increased client focus.
- A review of the Open Source Unit, which was established in 1999-00, identified opportunities for the unit to be more effectively utilised. Recommendations from the review will be considered by the Corporate Executive in 2001-02.
- We commenced a review of ASIO's process of re-evaluating staff security clearances to assess its effectiveness as an internal security control, and to determine whether the process continued to meet its core objective of assessing the suitability of staff to have access to classified material.

Twelve internal audits were completed, including:

- telecommunications interception expenditure
- Olympics expenditure
- controls regulating allowances paid to staff



- the administration of frequent flyer points
- controls to safeguard data received from other agencies (commenced in the previous reporting period)
- salary packaging
- the adequacy of the National Intelligence Group to support the *National Anti-Terrorist Plan* (commenced in 1999-00)
- compliance with the *NSW Law Enforcement and National Security (Assumed Identities) Act 1988*
- the Mobile Surveillance Detachment, and
- personnel security assessments and advice.

No loss of monies or assets was reported. Remedial action to redress some administrative and procedural shortcomings has been finalised or is underway.

## External Scrutiny

External scrutiny of ASIO's activities is exercised through Ministerial oversight, the Inspector-General of Intelligence and Security (the Inspector-General), the Auditor-General and the Parliamentary Joint Committee on ASIO.

A copy of ASIO's classified *Annual Report* is made available to the Leader of the Opposition, who also receives briefings from the Director-General as required under the *ASIO Act*.

ASIO's financial program is included in the Attorney-General's Portfolio Budget Statement, which is scrutinised by the Senate Legal and Constitutional Reference and Legislation Committee. The Director-General attends Committee hearings.

*The Minister*

The Attorney-General is responsible for Ministerial oversight of ASIO.

- All warrants for the exercise of ASIO's special powers must be approved by the Attorney-General.
- In addition to warrant requests, in 2000-01 we provided the Attorney with 149 briefing papers and submissions on significant security and ASIO-related issues.
- All operational activity by ASIO must comply with the Attorney-General's *Guidelines for the Collection of Intelligence*, which require ASIO to use methods of investigation which are appropriate to the perceived risk.
- The Attorney-General also receives reports from the Inspector-General on inquiries relating to ASIO, including complaints.

*The Inspector-General*

The Inspector-General may inquire into matters concerning ASIO on his own motion, at the request of the Attorney-General or the Government, or in response to complaints. His role is to ensure that ASIO acts legally and with propriety, complies with ministerial guidelines, and acts with due regard for human rights.

The Inspector-General undertakes regular reviews of ASIO's activities, including:

- access to operational files
- monitoring of ASIO's use of intrusive powers under warrant
- provision of information to, and liaison with, law enforcement agencies
- access to, and use of financial transaction reporting information obtained from the Australian Transaction Reports and Analysis Centre
- access to, and use of information obtained from the Australian Taxation Office
- the official use of alternative documentation to support assumed identities, and
- compliance with the *Archives Act*.

The Inspector-General meets as required with the Director-General, senior managers and the President of the ASIO Staff Association.

In his 2000-01 report the Inspector-General noted he had inquired into nine new complaints about ASIO (compared with nine in 1999-00, and 12 in 1998-99). He conducted preliminary inquiries into eight matters, and a full inquiry into one complaint. He also dealt with two outstanding matters carried over from 1999-00 and handled a further 19 complaints administratively.

The Inspector-General's *Annual Report* can be found at [www.igis.gov.au](http://www.igis.gov.au).

*The PJC*

The Parliamentary Joint Committee on ASIO (the PJC) reviews matters referred by the Attorney-General or the Parliament. The Committee membership is listed at Appendix A.

During 2000-01 the PJC completed a public inquiry into *The nature, scope and appropriateness of ASIO's public reporting activities*. The Director-General appeared as a witness before the Committee at a public hearing in July 2000. The Committee reported in September 2000, and found that:

- ASIO's *Annual Report* is probably the most comprehensive publicly available annual report from an intelligence agency anywhere in the world.
- ASIO's website contains a breadth and depth of information that compares favourably with overseas-based intelligence agencies.

- The total package of information available to the Australian community about ASIO's operations exceeds that available to citizens in other countries about their domestic intelligence agencies.
- That is not to say that ASIO should be complacent about its public reporting: it is important that ASIO, like all taxpayer-funded organisations, constantly strives to improve the way that it communicates with the public.

The Committee made five recommendations:

**Recommendation 1.** ASIO should ensure that an overview of key points of interest from its work over the last 12 months is available on its internet site.

- An overview of key points of interest from ASIO's work over the past 12 months was added to the ASIO website.

**Recommendation 2.** Before July 2001, ASIO should conduct a review of its internet site, taking into regard its effectiveness as a primary communication tool, considering arguments for adding further information about the Organisation, and making additions and improvements to the site as appropriate.

- ASIO completed an internal review of the website, updating the content and adding several new sections including The Year in Review, Media Releases and a section describing ASIO's role in CHOGM. In the next reporting period an independent consultant will be engaged to review the site and make recommendations for its further improvement as a communications tool.

**Recommendation 3.** ASIO should produce paper versions of all information available on its internet site, for distribution (on request) to people who do not have access to the internet.

- Paper versions of all parts of the website are available on request.

**Recommendation 4.** ASIO should produce *ASIO Now* or a similar publication in a number of community languages. These versions should be made available in hard copy and on ASIO's internet site.

- ASIO has examined the feasibility of translating an updated version of *ASIO Now* into several community languages. In the next reporting period these will be made available on the website, and in hard copy on request.

**Recommendation 5.** ASIO should provide to the National Archives of Australia a list of its files over 30 years old, excluding the names of files which may contain sensitive information as defined by the *Archives Act*.

- The Attorney-General did not accept this recommendation on the grounds that the potential benefit to researchers did not justify the significant resource costs.

During 2000-01 the Director-General also provided the PJC with regular briefings, including on the Olympics.

On 27 June 2001 the Minister for Foreign Affairs introduced the *Intelligence Services Bill 2001* into the Parliament. The legislation provides for a new Parliamentary Joint Committee on ASIO, ASIS and DSD, which will replace the PJC on ASIO and will have expanded oversight functions dealing with the expenditure and administration of the three agencies.

## **Interface with the Public**

ASIO's effectiveness depends, in large part, on the cooperation of the Australian public. We can provide people with information about our role and functions; however, for security reasons we have to limit public information on subjects of investigation, operational methods and sources of information.

ASIO receives a large quantity of unsolicited correspondence and numerous telephone calls from members of the public. These approaches generally fall into two categories - an offer of information that might be relevant to security, or complaints about ASIO.

All approaches from the public are carefully examined and appropriate action taken. Some letters and telephone calls reflect misconceptions about ASIO's roles and powers. Sometimes discussion with an ASIO officer can clarify issues or resolve concerns. In other cases, complainants are referred to the Inspector-General.

ASIO officers sometimes interview members of the public in the course of intelligence investigations, in order to explore national security issues. In recent years some people have falsely presented themselves as ASIO officers to gain credibility while pursuing improper or criminal activities.

- Bona fide ASIO officers operate under a strict code of conduct, particularly when interviewing members of the public. The officer must show proof of identity.
- If the person to be interviewed is concerned, they can telephone the public ASIO line to confirm the identity of the officer. (see Appendix B)
- A person interviewed may also complain to ASIO or to the Inspector-General if they have concerns about the behaviour of an ASIO officer.

ASIO publishes brochures and pamphlets about its work, in addition to its *Annual Report*. Members of the public can call ASIO's public telephone number and request information about the Organisation.

*www.asio.gov.au*

Our website provides information about ASIO's work and accountability arrangements, significant events in ASIO's history, and current employment opportunities.

The website provides links to related sites including those of the Attorney-General, the Inspector-General, the Parliamentary Joint Committee on ASIO and the sites of other members of the Australian Intelligence Community.

Interest in the website remained high. By the end of the reporting period the site recorded an average of 380 visitor sessions each day, and 11 338 hits per day. The employment pages were clearly the most popular throughout the year, with the exception of November 2000 when the annual *Report to Parliament* attracted considerable interest.

## Media Policy

In response to media inquiries, ASIO has a modified policy of 'neither confirm nor deny'. While ASIO does not normally comment on matters of national security, in some circumstances the Attorney-General (or the Director-General, with the Attorney's agreement) will provide public comment where this may help to promote public confidence in the legality, propriety and effectiveness of ASIO's conduct.

*Media interviews*

In June 2001 the Director-General was interviewed for an article in *The Australian Magazine*.

## Our People

ASIO's performance as an organisation is dependent on the quality of its people. Recruiting, developing and retaining highly skilled people remained an important corporate priority.

*Priorities*

Our people management focus for 2000-01 included:

- a detailed strategic examination of workforce planning issues to guide the direction of recruitment strategies
- preparation and delivery of new or expanded development courses to improve the capability of our staff
- examination of staff retention issues, and
- significant recruitment and internal staff movement in the post-Olympics period.

*People Management Plan*

We began reviewing our strategic *People Management Plan*. The new plan will look out to 2005, and will be completed during the next reporting period. The plan will identify strategies aimed at making ASIO an 'employer of choice'.

Key drivers are:

- the requirement to attract and retain highly skilled and motivated staff in a changing and competitive employment market, with a growing demand for intelligence and security expertise, and
- our need to identify future staffing requirements - and structure our recruitment and development programs to meet these needs.

## **Workplace Relations and Reform**

ASIO's *Fifth Workplace Agreement* has entered its second year and remains in force until March 2003. All non-SES ASIO staff are covered by the Agreement. Staff received a three percent pay rise in March 2001 with a further three percent to be paid in March 2002. All Senior Executive Service officers have individual Workplace Agreements with the Director-General.

Work commenced on a range of initiatives which will be completed during the next reporting period:

- updating dispute resolution procedures
- reviewing performance management systems
- development of a proposal for a service allowance for ASIO staff
- developing a 'plain English' document detailing terms and conditions of service in ASIO
- reviewing and streamlining pay and conditions processes, including testing of a new electronic pay and leave management system, and
- reviewing the method of payment and acquittal of travel allowances.

### *Performance Pay*

Performance Pay is available to Senior Executive Service officers. The amount paid is based on a percentage range of gross salary. In 2000-01 nine SES officers received Performance Pay in recognition of a high level of performance in the 1999-00 financial year. Individual payments ranged from \$7 563 to \$20 805. The average payment was approximately \$11 000, and the total amount paid was \$99 052.

## **Recruitment and Staffing**

### *Staffing profile*

Continuing the trend established in recent years, the employment of temporary staff remained an important element in ASIO's staffing strategy. In particular, it has provided the flexibility needed to meet the increased demands of the Olympic Games, and of CHOGM.

At 30 June 2001 17 percent of ASIO's staff were temporary employees compared to 18 percent in June 2000, and seven percent in June 1998 (see Appendix C for staffing statistics).

*Separations*

There were 67 separations in 2000-01 out of a workforce of 584 staff. This represented a separation rate of 11.5 percent - up from 9.9 percent last financial year and 6.5 percent in 1998-99.

The increased attrition rate is of concern. The reasons behind separations varied from promotion opportunities to lifestyle choices to dissatisfaction with ASIO's corporate direction. The skills of ASIO officers are in increasing demand and it will be important to seek to reduce the separation rate. To some extent, however, it is possible that the higher turnover rate may also reflect changing attitudes to work and careers in Australian society generally.

*Recruiting*

While ASIO continued to recruit across all job families, 2000-01 saw a particular focus on recruitment of specialist technical, engineering and IT staff, as well as Generalist Intelligence Officers (GIOs). This was driven by the need to replace separating staff, recruit people with different skill sets to meet new organisational responsibilities, and increased movement within ASIO - primarily from internal promotion processes.

- Competition to attract staff from technical and IT areas has been difficult, although towards the middle of 2001 the numbers of IT applicants began to rise in response to changes in the external job market.
- Fifteen GIO trainees commenced a 12 month traineeship in February 2001 - slightly more than in previous years. And in February 2001 we commenced our national recruitment campaign for subsequent intakes. The campaign attracted twice as many applicants as in 1999-00. The increase was a result of extending our newspaper advertisements to major regional centres with university campuses, advertising through our website, and increased media coverage of the campaign.

Recruitment of skilled staff will remain a high priority in 2001-02 and we continue to explore ways of streamlining the recruitment process. However, ASIO's stringent selection and security requirements mean the process will take longer than most other private and public sector organisations.

The launch of the ASIO website in June 2000 generated efficiencies in our recruitment processes. All publicly advertised ASIO vacancies were listed on the website which provided potential applicants with greater access to information regarding ASIO's role and functions. It also provided a better opportunity to assess whether ASIO represented an attractive career alternative - and saved ASIO resources through improved 'self selection' by potential applicants.

*Advertising*

Advertising costs, primarily in the print media, increased from \$113 000 in 1999-00 to \$180 000 in 2000-01. This reflected the increased number of positions requiring external advertising and a deliberate decision to advertise more widely for some job categories.

*Workforce  
planning and  
retention*

To improve our ability to plan for future human resource requirements, an external consultant conducted a comprehensive workforce planning survey. The report highlighted a number of planning issues for ASIO over the coming years. These include the need to recruit increased numbers of GIOs (given a growing need and increasing separation rates) and the implications of over 20 percent of ASIO's workforce being eligible to elect to retire within the next five years.

To address these issues we are developing a strategy to improve our ability to access and analyse staffing data.

We are also seeking to improve our understanding of why people join (and leave) ASIO through improved exit interview processes and a staff survey planned for 2001-02.

## **Developing our people**

During the early part of 2000-01 investment in training and development was scaled back as resources were redirected to meet ASIO's Olympics commitments.

The period after the Olympics was characterised by significant staff movement, brought about by internal transfers, a larger than usual number of promotions, and a higher than normal attrition rate. In response ASIO made a significant investment in training and developing staff for new or changing roles.

We directed \$1.2m - about two cent percent of budget - to corporate training and development. In addition, significant on-the-job training was provided to staff, while work groups sponsored a wide range of job-specific courses. In addition, 46 people were provided with support for their tertiary studies.

*Leadership  
development*

Over 130 people participated in a range of leadership development programs, including:

- SES programs addressing leadership capabilities and organisational values
- the PSMPC Senior Executive development program
- financial and contract management
- ASIO's Frontline Management in Action program, and
- 'time-outs' to review lessons learned from the Olympics.

*Corporate  
training*

Other significant training and development activities included:

- the development of intelligence collection and analysis capabilities, with emphasis on basic and advanced analytical programs, and advanced operational skills
- crisis management



- our traineeship programs for Generalist Intelligence Officers - the traineeships run for 12 months and involve a mix of formal coursework and a three month placement in each of ASIO's Divisions - Collection, Analysis and Liaison, and Corporate Management and Security
- CHOGM related training, and
- Ethics Awareness programs - addressing organisational and individual accountability, ASIO's values, fraud awareness, and ethics in an operational environment. This program also includes a segment delivered by the Inspector-General.

All staff were encouraged to prepare Individual Development Plans to guide their own training and development, as well as helping to shape the direction of ASIO's future corporate training strategies. Secondments and exchanges with other agencies continued.

#### *Evaluation*

All training and development programs are formally evaluated to ensure they are delivering the skills enhancement we require. The evaluation process includes assessment of trainee learning against competency standards, trainee surveys and individual program reports. Longer term effectiveness is assessed by seeking feedback from, and consulting with, organisational stakeholders.

### **Workplace diversity**

ASIO continued to encourage workplace diversity in 2000-01. A new policy explaining the roles of staff and management in promoting diversity was released. This policy complements our *Workplace Diversity Program (1998-02)*.

We continued our commitment to a harassment-free work environment. A revised policy aimed at eliminating all forms of workplace harassment will be issued in the second half of 2001 (in concert with an education campaign).

#### *Family friendly initiatives*

A childcare assistance rebate was provided to staff who had to make alternative childcare arrangements as a result of changed work commitments during the core Olympic period. A similar scheme is in place for CHOGM.

We continued to offer a range of initiatives to assist people to meet their family commitments, including:

- employing officers on a part time and casual basis
- job sharing
- the ability of staff to 'purchase' extra leave, and
- allowing officers to utilise their Personal Leave (previously sick leave, special leave and carer's leave) to care for members of their immediate family who are ill.

*EEO target groups*

The representation of some EEO target groups declined slightly in 2000-01 while others have remained relatively static. At 30 June 2001:

- the percentage of female employees remained at 40 percent
- the representation of staff from Non English Speaking Backgrounds decreased from 8 to 6 percent
- the percentage of women at senior officer level declined from 16.3 to 15.3 percent, and
- the increased employment of females in the GIO employment stream (noted in last year's report) continued.

The representation of women at SES and senior officer levels remains well below the APS average. Down the track, it is hoped that the continuing growth in the percentage of female Generalist Intelligence Officers - now 39.8 percent of the total - will help improve this situation.

Appendixes C, D and E provide statistical data about ASIO's total staffing numbers, composition of the workforce, Senior Executive Service, representation of designated work groups, and salary structure.

## **Disability Strategy**

We began developing a *Disability Strategy* (and action plan) aimed at removing unnecessary barriers for clients with a disability who wish to access ASIO and the services it provides. The Strategy will include key performance indicators to monitor implementation and will be completed in 2001-02.

ASIO already has in place some of the elements outlined by the Office of Disability in its guide for agencies.

ASIO's Consultative Council, which comprises representatives from management and staff, has an Occupational Health and Safety sub-committee that addresses disability concerns, including employment and conditions of service matters.

ASIO also:

- is an equal opportunity employer
- has facilities for those with a disability and is actively investigating ways of improving them
- provides reading material in appropriate formats
- has informal and formal complaints mechanisms with access to external reviews for all staff
- raises awareness of workplace diversity through in-house publications, and
- has produced a new Human Resources Management Circular *Workplace Diversity in ASIO* which is available to all staff.

## Occupational Health and Safety

ASIO's Occupational Health and Safety sub-committee oversaw the implementation of the *2000 OH&S Agreement*, which included ten OH&S audits. Significant health and safety initiatives included:

- Evaluation of the OH&S policy and practice audit tool SafetyMAP. Implementation of SafetyMAP is expected by February 2002.
- Testing for staff who may have come into contact with asbestos at ASIO's test site. All staff tested to date have been given a clean bill of health.
- An annual Health Week focused on improving health, managing stress and educating staff on health and safety issues.
- Influenza vaccinations were again offered to promote health in the workplace, and
- Ten first aid officers and nine health and safety representatives were selected and trained.

### *Reportable incidents*

There were no accidents causing death or serious personal injury recorded during the reporting period. And there were no incidents involving incapacity of 30 days or more as a result of accident, incident or disease arising out of an employee's work. No dangerous occurrences were reported.

### *Compensation claims*

In 2000-01 there were eight compensation claims compared with 12 in 1999-00.

Our 1999-00 *Report to Parliament* referred to a compensation matter relating to an ASIO staff member, and noted Comcare had accepted liability for the payment of incapacity payments. An agreement on the amount of compensation (and associated costs) was reached between the officer and Comcare. The process of final settlement was completed early in 2001-02.

## Information Management

ASIO is critically dependent on rapid and reliable access to intelligence information. As a result, the information technology and information management components of our business remained a high priority.

Our capability enhancement strategies continued to deliver results during 2000-01. In the lead-up to the Olympics we focused on bedding down the major improvements that were implemented over the past three years, with the result that uninterrupted services were provided throughout the critical Olympics period.

Post-Olympics, our priority was to refine and enhance existing systems to ensure our information management capability was able to meet CHOGM needs.

*Intelligence information*

We enhanced our main intelligence database by simplifying data entry screens. This significantly improved the efficiency of key business areas, including the provision of personnel security assessments advice.

Our analytical capability was improved by expanding the range of intelligence data delivered directly to desktops. Officers with a 'need to know' now have much faster access to relevant reports and intelligence information.

*Corporate information*

We developed an Intranet to improve the desktop availability of corporate information, including people management circulars, internal security instructions, and the *ASIO Policies and Procedures Manual*. Implementation will be completed early in 2001-02.

*Infrastructure development*

The ageing Local Area Network infrastructure was replaced, to improve maintenance procedures and maximise the use of new technology.

Planning and delivery of IT projects was improved with the introduction of a common project management methodology, PRINCE 2. And we developed a separate Test network to reduce the risk of untested changes impacting on our critical intelligence systems.

*Looking ahead*

In 2001-02 we will give priority to:

- improving external connectivity while maintaining appropriate levels of security, and
- further reducing the backlog of archival information.

## Security of ASIO

*Security Management Plan*

ASIO's ability to function as an effective and credible security intelligence organisation is dependent on rigorous internal security policies and procedures. ASIO's *Security Management Plan 2001-2004* was approved by ASIO's Security Committee and endorsed by the Corporate Executive in March 2001.

The Plan sets out objectives and strategies to manage security within ASIO, and reflects the principal themes of the *Inquiry into Security Issues* (the Blick Report). It fulfils the revised *Commonwealth Protective Security Manual* (PSM) requirement for all departments and agencies to establish a clear and concise security plan that supports the agency's goals through security risk management.

A range of internal policies and procedures support the Plan. These include basic measures such as electronic pass checking and random bag searches, to more complex practices, including the isolation of the ASIO computer networks from outside contact, and the security clearance and re-evaluation of all staff.

These strategies aim to minimise risk from:

- foreign intelligence services attempting to penetrate ASIO or gain access to ASIO information

- unauthorised disclosure of information by ASIO staff, and
- targeting of ASIO by hostile groups or individuals.

*Security  
clearance  
re-evaluation*

Staff security clearance is an exhaustive process, covering detailed examination of an officer's background, including financial checks, police checks, interviews of nominated and un-nominated referees, mandatory psychological testing, annual supervisor security reports, and interviews of the officers themselves. The clearance is then re-evaluated at least every five years, or more regularly on a needs basis. A program of revalidations (30 month security checks) has also been introduced.

- 166 re-evaluations were completed in 2000-01.

*Supporting  
our staff*

ASIO maintains a Counter Intelligence and Security Staffing section, which provides support to staff on personal and professional matters which may have implications for security. This is designed to ensure that issues which might not initially appear to be a security concern are properly managed, and that officers feel confident to approach the section to resolve their own and other officers' problems before they do become a matter of security concern. Psychological counselling and other staffing assistance is also made available.

*Physical  
security*

In 2000-01 we enhanced audit and physical security mechanisms for access to offices, staff movements, computer systems and office equipment including photocopies, facsimile machines and printers. A Protective Security Risk Review was undertaken of all ASIO offices to ensure a consistently high standard of security practices across ASIO.

*Security  
audits*

ASIO conducts regular security audits of access to offices and staff operations to ensure they conform to the policies and procedures governing ASIO's operational activity. The audits examine security, tradecraft, documentation and consistency. ASIO conducted 120 operational audits in 2000-01. In addition, a program of audits was implemented for physical, personnel, administrative and information technology security.

*Security  
policies*

We developed or revised a range of policies designed to enhance our internal security, and heighten awareness of security issues. The policies were circulated to all staff, and are easily accessible from the desktop.

Major policies addressed:

- Security Breaches - to ensure staff understand the revised PSM requirement for reporting breaches, and to minimise the occurrences of internal security violations.
- Performance Agreements - which must address adherence to security policies and procedures.
- ASIO Documentation - policies and procedures governing the use of official documentation are rigorously enforced.
- Security Audits - to provide guidance to staff on the ASIO security audit program.

- Overseas Travel - to remind staff of the personal security precautions, briefings and debriefings required.
- Contact with Foreign Nationals - to ensure staff are aware of their reporting requirements.
- Revised restrictions on the AUSTEO and AGAO caveats - to ensure staff are aware of the releasability restrictions on these caveats.

## Building management

In 2000-01 we commenced the market testing of our building maintenance and contract management facilities. And in the next reporting period we will undertake a major refurbishment of parts of the Central Office basement to provide improved accommodation and facilities.

Our provision of co-tenancy for the Office of National Assessments continued to prove successful for both parties.

## Ecologically sustainable development and environmental performance

### *Environmental initiatives*

A range of recycling, waste and water management initiatives were introduced to minimise the impact of ASIO on the environment, including:

- improvements to the switching system for lighting and general power
- recycling of paper and cardboard (where security requirements permit)
- design and development of a paper destructor system that drastically reduced water usage
- the use of some recycled paper products in the print-room, and
- staff awareness of ASIO's environmental responsibilities was raised, including through our internal staff newsletter.

We continued to provide energy management data to the Department of Industry, Science and Resources for the annual *Whole of Government Energy Report*. This has increased our commitment to improved monitoring of energy usage.

Energy demand in Central Office increased markedly during the period of the Olympics when staff worked extended hours. Our building energy monitoring system provided the flexibility to meet additional energy requirements, within managed parameters which kept waste to a minimum.

## Purchasing

All purchasing activity within ASIO is conducted in accordance with the *Chief Executive Instructions*. These instructions are designed to ensure that, as far as security restrictions permit, all *Commonwealth Procurement Guidelines* are met, and in particular, value for money achieved. As far as possible, value for money is achieved by obtaining a number of competitive quotations for purchases between \$2 000 and \$50 000 and restricted tenders for any purchases in excess of \$50 000.

During 2000-01 our annual investment program was progressed. Our purchasing objectives focused on investment in key business areas, including technical capabilities enhancement and information technology.

## Consultants and Contractors

Expenditure on consultancy contracts in 2000-01 fell to \$548 000 compared with \$1.4m in 1999-00.

The lower level of expenditure in 2000-01 was predominantly due to a tighter application of the definition for consultancy services. A review of the entries totalling \$1.4m in the *1999-00 Report to Parliament* revealed that a number of the entries included were in fact contracts for services rather than consultancy services. The term consultancy services is used to describe the application of expert professional skills to:

- investigate or diagnose a defined issue or problem
- carry out defined research, reviews or evaluations, or
- provide independent advice, information or creative solutions to assist the agency in decision making.

In 2000-01 external consultants were used primarily for the development of information technology projects and various management and infrastructure reviews. The scope for outsourcing was restricted due to national security considerations.

A partial list of the 32 consultancy contracts, excluding elements removed for security reasons, is available on request.

A small part of this report is excluded from the unclassified *Report to Parliament* because of security sensitivity.



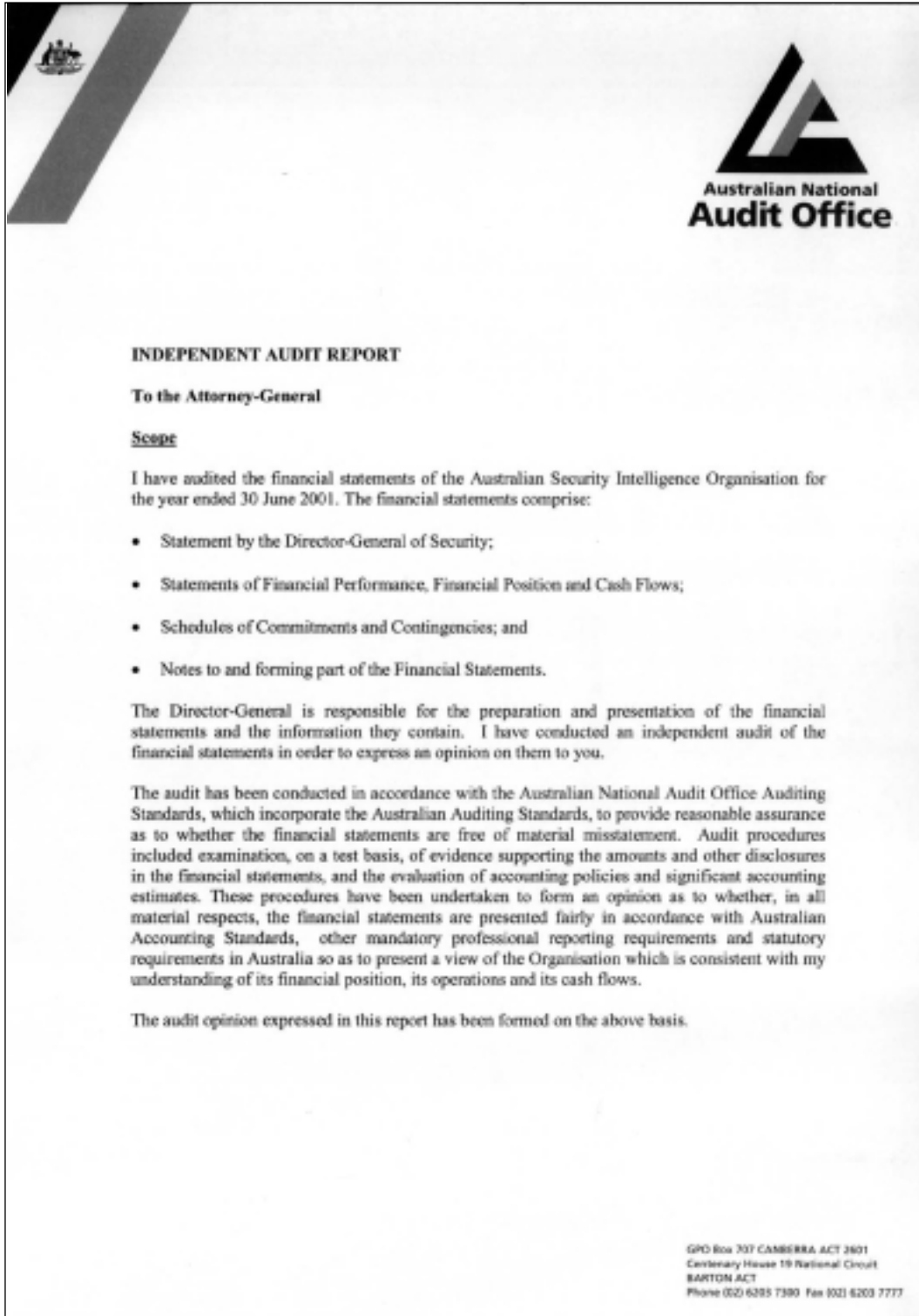


# Part 4

## **financial statements**



## Audit Report on the Financial Statements of the Australian Security Intelligence Organisation



**Audit Opinion**

In my opinion,

- (i) the financial statements have been prepared in accordance with Schedule 1 of the *Financial Management and Accountability (Financial Statements 2000-2001) Orders*; and
- (ii) the financial statements give a true and fair view, in accordance with applicable Accounting Standards, other mandatory professional reporting requirements and Schedule 1 of the *Financial Management and Accountability (Financial Statements 2000-2001) Orders*, of the financial position of the Australian Security Intelligence Organisation as at 30 June 2001 and the results of its operations and its cash flows for the year then ended.

Australian National Audit Office



David C McKean  
Executive Director

Delegate of the Auditor-General

Canberra  
20 September 2001

## Statement by the Director-General of Security

In my opinion, the attached financial statements have been prepared in accordance with an agreement between the Finance Minister and the Attorney-General which complies with Schedule 1 of the Financial Management and Accountability (Financial Statements 2000-2001) Orders made under section 63 of the *Financial Management and Accountability Act 1997*.

A handwritten signature in black ink that reads "Dennis Richardson". The signature is written in a cursive style with a long horizontal flourish at the end.

Dennis Richardson  
Director-General of Security

20 September 2001

## Statement of Financial Performance for the period ended 30 June 2001

	Notes	2000-01 \$ '000	1999-00 \$ '000
<b>Revenues from ordinary activities</b>			
Revenues from government	3A	64 152	65 003
Sales of goods and services	3B	3 345	340
Proceeds from disposal of assets	3C	586	1 398
Interest		431	489
Other		1 022	1 154
<b>Total revenues from ordinary activities</b>		<b>69 536</b>	<b>68 384</b>
<b>Expenses from ordinary activities</b>			
Employees	4A	41 937	37 462
Suppliers	4B	27 552	21 753
Depreciation and amortisation	4C	6 369	6 134
Write-down of assets	4D	111	396
Disposal of assets	3C	624	1 398
<b>Total expenses from ordinary activities</b>		<b>76 593</b>	<b>67 143</b>
<b>Borrowing cost expense</b>		<b>76</b>	<b>—</b>
<b>Net operating surplus (deficit) from ordinary activities</b>		<b>(7 133)</b>	<b>1 241</b>
<b>Net surplus or (deficit)</b>		<b>(7 133)</b>	<b>1 241</b>
<b>Equity Interests</b>			
<b>Net surplus (deficit) attributable to the Commonwealth</b>		<b>(7 133)</b>	<b>1 241</b>
Net credit (debit) to asset revaluation reserve	12	(205)	—
Assets not previously recognised	5	—	426
<b>Total revenues, expenses and valuation adjustments recognised directly in equity</b>		<b>(205)</b>	<b>426</b>
<b>Total changes in equity other than those resulting from transactions with owners as owners</b>		<b>(7 338)</b>	<b>1 667</b>

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

## Statement of Financial Position as at 30 June 2001

	Notes	2000-01 \$ '000	1999-00 \$ '000
<b>ASSETS</b>			
<b>Financial assets</b>			
Cash		2 944	15 331
Receivables	6A	2 037	262
Capital use receivable		331	—
<b>Total financial assets</b>		<b>5 312</b>	<b>15 593</b>
<b>Non-financial assets</b>			
Land and buildings	7A, 7D	7 441	8 181
Infrastructure, plant and equipment	7B, 7D	17 023	16 456
Intangibles	7C, 7D	2 320	2 757
Other	8	819	1 566
<b>Total non-financial assets</b>		<b>27 603</b>	<b>28 960</b>
<b>Total assets</b>		<b>32 915</b>	<b>44 553</b>
<b>LIABILITIES</b>			
<b>Interest bearing liabilities</b>			
Leases	9	711	878
<b>Total debt</b>		<b>711</b>	<b>878</b>
<b>Provisions</b>			
Capital use		—	3 161
Employees	10A	12 708	13 022
<b>Total provisions</b>		<b>12 708</b>	<b>16 183</b>
<b>Payables</b>			
Suppliers	11A	1 880	1 196
Other	11B	21	255
<b>Total payables</b>		<b>1 901</b>	<b>1 451</b>
<b>Total liabilities</b>		<b>15 320</b>	<b>18 512</b>
<b>EQUITY</b>			
<b>Parent entity interest</b>			
Capital		13 168	12 928
Reserves		1 930	2 135
Accumulated surpluses		2 497	10 978
<b>Total parent entity interest</b>	12	<b>17 595</b>	<b>26 041</b>
<b>Total equity</b>	12	<b>17 595</b>	<b>26 041</b>
<b>Current liabilities</b>		<b>7 527</b>	<b>10 495</b>
<b>Non-current liabilities</b>		<b>7 793</b>	<b>8 017</b>
<b>Current assets</b>		<b>6 131</b>	<b>17 159</b>
<b>Non-current assets</b>		<b>26 784</b>	<b>27 394</b>

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

## Agency Statement of Cash Flows for the period ended 30 June 2001

	Notes	2000-01 \$ '000	1999-00 \$ '000
<b>OPERATING ACTIVITIES</b>			
<b>Cash received</b>			
Appropriations		62 695	76 990
Interest		527	377
Other		2 262	1 756
GST refunds		1 508	—
Total cash received		66 992	79 123
<b>Cash used</b>			
Employees		42 251	36 312
Suppliers		26 804	21 872
Total cash used		69 055	58 184
Net cash from/(used by) operating activities	13	(2 063)	20 939
<b>INVESTING ACTIVITIES</b>			
<b>Cash received</b>			
Proceeds from sales of property, plant and equipment		184	187
Total cash received		184	187
<b>Cash used</b>			
Purchase of property, plant and equipment		5 741	9 033
Total cash used		5 741	9 033
Net cash used by investing activities		(5 557)	(8 846)
<b>FINANCING ACTIVITIES</b>			
<b>Cash received</b>			
Proceeds from equity injections		240	—
Total cash received		240	—
<b>Cash used</b>			
Repayment of debt		167	—
Capital use paid		4 840	—
Total cash used		5 007	—
Net cash used by financing activities		(4 767)	—
Net increase/(decrease) in cash held		(12 387)	12 093
Cash at the beginning of the reporting period		15 331	3 238
Cash at the end of the reporting period		2 944	15 331

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



## Schedule of Commitments as at 30 June 2001

	Notes	2000-01 \$ '000	1999-00 \$ '000
<i>BY TYPE</i>			
<b>Capital commitments</b>			
Land and buildings		-	-
Infrastructure, plant and equipment		2 245	565
Other capital commitments		-	-
Total capital commitments		2 245	565
<b>Other commitments</b>			
Operating leases		33 654	9 086
Other commitments		516	13 812
Total other commitments		34 170	22 898
<b>Commitments receivable</b>		6 020	—
Net commitments		30 395	23 463
<i>BY MATURITY</i>			
<b>All net commitments</b>			
One year or less		3 822	13 420
From one to five years		10 717	9 573
Over five years		15 856	470
Net commitments		30 395	23 463
<b>Net operating lease commitments</b>			
One year or less		2 902	2 572
From one to five years		10 717	6044
Over five years		15 856	470
Net commitments		29 475	9 086

Commitments are GST inclusive where relevant.

Operating leases included are effectively non-cancellable and comprise:

<i>Nature of lease</i>	<i>General description of leasing arrangement</i>
leases for office accommodation	<p>Various options apply to the review of lease payments:</p> <ul style="list-style-type: none"> <li>• Annual review based on upwards movement in Consumer Price Index (CPI)</li> <li>• Biennial review based on CPI</li> <li>• Biennial review based on market appraisal</li> </ul>

The above schedule should be read in conjunction with the accompanying notes

## Schedule of Contingencies as at 30 June 2001

	Notes	2000-01 \$ '000	1999-00 \$ '000
<i>CONTINGENT LOSSES</i>			
Claims for damages/costs		-	-
Total contingent losses		-	-

The above schedule should be read in conjunction with the accompanying notes

## Notes to the Financial Statements for the year ended 30 June 2001

### NOTE 1: Objective

To provide advice, in accordance with the *ASIO Act* to Ministers and appropriate agencies and authorities, to protect Australia and its people from threats to national security.

ASIO is structured to meet the following Outcome:

A secure Australia for people and property, for government business and national infrastructure, and for special events of national and international significance.

### NOTE 2: Summary of significant accounting policies

#### A. 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 financial statements have been prepared in accordance with the agreement between the Finance Minister and the Attorney-General. This agreement states that ASIO's financial statements must be prepared in accordance with the *Financial Management and Accountability Orders (Amendment No3) 1999* except where the disclosure of information in the notes to the financial statements would, or could reasonably be expected to be operationally sensitive. The financial statements are prepared:

- in compliance with Australian Accounting Standards and other authoritative pronouncements of Australian Accounting Standards Boards and the consensus views of the Urgent Issues Group;
- having regard to Statements of Accounting Concepts; and
- the Explanatory Notes to Schedule 1 issued by the Department of Finance and Administration.

The Statements of Financial Performance and Financial Position have been prepared on an accrual basis and are in accordance with the historical cost convention except for certain assets which, as noted, are at valuation. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position.

The continued existence of ASIO in its present form, and with its current programs, depends on Government policy and on continuing appropriations by Parliament.

#### B. Revenues from Government

Revenues from Government are revenues relating to core operating activities.

Policies for accounting for revenue from Government follow; amounts and other details are given in Note 3.

*Agency appropriation.*

Appropriations for departmental outputs are recognised as revenue to the extent that the Finance Minister is prepared to release appropriations for use (that is, the full amount of the appropriation passed by the Parliament less any savings offered up at Additional Estimates and not subsequently released).

*Resources received free of charge*

Resources received free of charge are recognised as revenue in the Agency Operating Statement where the amounts can be reliably measured. Use of those resources is recognised as an expense.

**C. Other revenue**

Revenue from the sale of goods is recognised upon the delivery of goods to customers. Interest revenue is recognised on a proportional basis taking into account the interest rates applicable to the financial assets. Revenue from disposal of non-current assets is recognised when control of the asset has passed to the buyer.

Revenue from the rendering of a service is recognised by reference to the stage of completion of contracts or other agreements to provide services to other government bodies.

The stage of completion is determined according to the proportion that costs incurred to date bear to the estimated total costs of the transaction.

All revenues described in this note are revenues relating to the core operating activities of ASIO. Details of revenue amounts are given in Note 3.

**D. Leases**

A distinction is made between finance leases which effectively transfer from the lessor to the lessee substantially all the risks and benefits incidental to ownership of leased non-current assets and operating leases under which the lessor effectively retains substantially all such risks and benefits.

Where a non-current asset is acquired by means of a finance lease, the asset is capitalised at the present value of minimum lease payments at the inception of the lease and a liability recognised for the same amount. Leased assets are amortised over the estimated useful life of the asset. Lease payments are allocated between the principal component and the interest expense.

Operating lease payments are expensed on a basis which is representative of the pattern of benefits derived from the leased assets.

**E. Cash**

Cash includes notes and coins held and any deposits held at call with a financial institution.

## **F. Acquisition of assets**

Assets are recorded at cost on acquisition. The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken.

### *Asset recognition threshold*

Purchases of property, plant and equipment with a historical cost equal to or in excess of \$500 are capitalised in the year of acquisition and included in the financial statements. Assets with a historical cost under \$500 are expensed in the year of acquisition.

### *Revaluations*

Land, buildings, infrastructure, plant and equipment are revalued progressively in accordance with the 'deprival' method of valuation in successive three-year cycles.

ASIO has implemented its revaluations program as follows:

- Land and buildings, including leasehold improvements at State offices, have been revalued as at 30 June 1999.
- Infrastructure, plant and equipment comprises computing and communications equipment, technical and operational equipment, office furniture, office equipment and motor vehicles. Computing and communications equipment was revalued during 2000-2001 and all other equipment items were revalued at 30 June 1999. Motor vehicles are changed over every two years and their value is disclosed at cost of acquisition.

Assets in each class acquired after the commencement of the progressive revaluation cycle will be reported at cost until the next progressive revaluation.

The financial effect of the move to progressive revaluations is that carrying amounts of assets will reflect current values and that depreciation charges will reflect the current cost of the service potential consumed in each period.

With the application of the deprival method, ASIO values its land at its current market buying price and its other assets at their depreciated replacement cost. Any assets which would not be replaced or are surplus to requirements are valued at net realisable value. At 30 June 2001, ASIO had no assets in this situation.

All valuations are independent except where specifically noted otherwise.

### *Recoverable amount test*

Schedule 1 requires the application of the recoverable amount test to departmental non-current assets in accordance with AAS 10 Accounting for the Revaluation of Non-Current Assets. The carrying amounts of these non-current assets have been reviewed to determine whether they are in excess of their recoverable amounts. In assessing recoverable amounts, the relevant cash flows have been discounted to their present value.

### G. Depreciation of non-financial assets

Depreciable property, plant and equipment assets are written-off to their estimated residual values over their estimated useful lives to ASIO using, in all cases, the straight line method of depreciation. Leasehold improvements are amortised on a straight line basis over the lesser of the estimated useful life of the improvements or the unexpired period of the lease.

Depreciation/amortisation 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 applying to each class of depreciable asset are as follows:

	<b>2000-01</b>	1999-00
Buildings on freehold land	<b>25-40 years</b>	25-40 years
Leasehold improvements	<b>Lease term</b>	Lease term
Plant and equipment	<b>3 to 15 years</b>	3 to 15 years

The aggregate amount of depreciation allocated for each class of asset during the reporting period is disclosed in Note 4C.

### H. Employee entitlements

#### *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 annual sick leave taken in future years by employees is estimated to be less than the annual entitlement for sick leave.

The liability for annual leave reflects the value of total annual leave entitlements of all employees at 30 June 2001 and is recognised at the nominal amount.

The non-current portion of the liability for long service leave is recognised and measured at the present value of the estimated future cash flows to be made in respect of all employees at 30 June 2001. In determining the present value of the liability, ASIO has taken into account attrition rates and pay increases through promotion and inflation.

#### *Superannuation*

Staff of ASIO contribute to the Commonwealth Superannuation Scheme and the Public Sector Superannuation Scheme. Employer contributions amounting to \$3 856 000 (1999-2000: \$3 654 000) in relation to these schemes have been expensed in these financial statements.

No liability is shown for superannuation in the Statement of Financial Position as the employer contributions fully extinguish the accruing liability which is assumed by the Commonwealth.

Employer Superannuation Productivity Benefit contributions totalled \$725 000 (1999–2000: \$678 000).

#### **I. Taxation**

The Agency is exempt from all forms of taxation except fringe benefits tax and the goods and services tax.

#### **J. Capital usage charge**

A capital usage charge of 12% is imposed by the Commonwealth on the net departmental assets of the agency. The charge is adjusted to take account of asset gifts and revaluation increments during the financial year.

#### **K. Foreign currency**

Transactions denominated in a foreign currency are converted at the exchange rate at the date of the transaction. Foreign currency receivables and payables are translated at the exchange rates current as at balance date.

Associated currency gains and losses are not considered material to the Organisation's operations.

#### **L. Insurance**

In accordance with the agreement with the Commonwealth, assets are not insured and losses are expensed as they are incurred. Workers Compensation is insured through Comcare Australia.

#### **M. Bad and doubtful debts**

Bad debts are written off during the year in which they are identified.

Where necessary, provision is raised for any doubtful debts based on a review of all outstanding accounts as at year end.

#### **N. Comparative figures**

Where necessary, comparative figures have been adjusted to conform with changes in presentation in these financial statements.

**O. Rounding**

Amounts have been rounded to the nearest \$1 000 except in relation to the following items:

- appropriations
- act of grace payments and waivers
- remuneration of executives, and
- remuneration of auditor.

**P. Administered items**

ASIO does not have any administered items.



	2000-01 \$ '000	1999-00 \$ '000
<b>NOTE 3: Operating revenues</b>		
<b>NOTE 3A: Revenues from Government</b>		
Appropriations for outputs	62 695	64 062
Resources received free of charge	1 457	941
Total	<u>64 152</u>	<u>65 003</u>
<b>NOTE 3B: Sales of goods and services</b>	<u>3 345</u>	<u>340</u>
<b>NOTE 3C: Proceeds and expenses from sales of assets</b>		
Non financial assets - Infrastructure, plant and equipment		
Revenue (proceeds) from sale	586	1 398
Expenses from sale	624	1 398
Total	<u>(38)</u>	<u>—</u>
<b>NOTE 4: Operating expenses</b>		
<b>NOTE 4A: Employee expenses</b>		
Basic remuneration	38 946	34 987
Separation and redundancy	750	227
Total remuneration	<u>39 696</u>	<u>35 214</u>
Other employee expenses	2 241	2 248
Total	<u>41 937</u>	<u>37 462</u>
<b>NOTE 4B: Suppliers' expenses</b>		
Supply of goods and services	21 461	15 790
Operating lease rentals	6 091	5 963
Total	<u>27 552</u>	<u>21 753</u>

	2000-01 \$ '000	1999-00 \$ '000
<b>NOTE 4C: Depreciation and amortisation</b>		
Depreciation of property, plant and equipment	6 171	6 134
Amortisation of leased assets	198	—
Total	<u>6 369</u>	<u>6 134</u>

The aggregate amount of depreciation or amortisation expensed during the reporting period for each class of depreciable asset are as follows:

Buildings	42	39
Leasehold improvements	922	898
Plant and equipment	4 391	3 748
Intangibles	1 014	1 449
Total	<u>6 369</u>	<u>6 134</u>

**NOTE 4D: Write down of assets**

Non-financial assets,		
– Plant and equipment — revaluation decrement	<u>111</u>	<u>396</u>

**NOTE 5: Assets not previously recognised**

Non-financial assets,		
– Buildings	—	246
– Plant and equipment	—	180
	<u>—</u>	<u>426</u>

	2000-01 \$ '000	1999-00 \$ '000
<b>NOTE 6: Financial assets</b>		
<b>NOTE 6A: Receivables</b>		
Goods and services	1 665	262
GST receivable	372	—
Less provision for doubtful debts	—	—
	<hr/>	<hr/>
Total	2 037	262
	<hr/>	<hr/>
Receivables (gross) are aged as follows:		
Not overdue	1 796	238
Overdue:		
– less than 30 days	7	17
– 30 to 60 days	190	—
– 60 to 90 days	7	5
– more than 90 days	37	2
	<hr/>	<hr/>
	2 037	262
	<hr/>	<hr/>
<b>NOTE 7: Non-financial assets</b>		
<b>NOTE 7A: Land and buildings</b>		
Freehold land—at June 1999 valuation	720	720
	<hr/>	<hr/>
	720	720
	<hr/>	<hr/>
Buildings in progress—at cost	—	66
Accumulated depreciation	—	—
	<hr/>	<hr/>
	—	66
	<hr/>	<hr/>
Buildings at cost	100	—
Accumulated depreciation	(4)	—
	<hr/>	<hr/>
	96	—

	<b>2000-01</b> <b>\$ '000</b>	1999-00 \$ '000
Buildings on freehold land—at 1999-02 valuation	965	965
Accumulated depreciation	(281)	(243)
	<hr/> 684	<hr/> 722
Leasehold improvements—at cost	7 981	7 815
Accumulated amortisation	(2 440)	(1 671)
	<hr/> 5 541	<hr/> 6 144
Leasehold improvements—at 1999-02 valuation	949	925
Accumulated amortisation	(549)	(396)
	<hr/> 400	<hr/> 529
Total	<hr/> 7 441	<hr/> 8 181

**NOTE 7B: Infrastructure, plant and equipment**

Plant and equipment—at cost	8 196	12 114
Accumulated depreciation	(1 056)	(1 111)
	<hr/> 7 140	<hr/> 11 003
Plant and equipment—at 1998-01 valuation	—	5 560
Accumulated depreciation	—	(3 429)
	<hr/> —	<hr/> 2 131
Plant and equipment—at 1999-02 valuation	7 197	9 371
Accumulated depreciation	(5 105)	(6 049)
	<hr/> 2 092	<hr/> 3 322
Plant and equipment—at 2001-04 valuation	17 848	—
Accumulated depreciation	(10 057)	—
	<hr/> 7 791	<hr/> —
Total	<hr/> 17 023	<hr/> 16 456

	<b>2000-01</b> <b>\$ '000</b>	1999-00 \$ '000
<b>NOTE 7C: Intangibles</b>		
Purchased computer software—at cost	<b>5 698</b>	2 786
Accumulated amortisation	<b>(3 378)</b>	(455)
	<hr/> <b>2 320</b>	<hr/> 2 331
Purchased computer software—at June 1998 valuation	—	2 335
Accumulated amortisation	—	(1 909)
	<hr/> —	<hr/> 426
Total	<hr/> <b>2 320</b>	<hr/> 2 757

**NOTE 7D: Analysis of property, plant and equipment and intangibles****Table A — Movement summary for 2000-01 for all assets irrespective of valuation basis.**

<i>Item</i>	<i>Land</i>	<i>Buildings</i>	<i>Buildings- Leashold Improvements</i>	<i>Total buildings</i>	<i>Total land and buildings</i>	<i>Plant and equipment</i>	<i>Intangibles</i>	<i>Total</i>
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>Gross value as at 1 July 2000</b>	720	1 031	8 740	9 771	10 491	27 045	5 121	<b>42 657</b>
Additions-purchases	—	34	190	224	224	5 908	577	<b>6 709</b>
Disposals	—	—	—	—	—	(804)	—	<b>(804)</b>
Revaluations	—	—	—	—	—	1 256	—	<b>1 256</b>
Write-offs	—	—	—	—	—	(164)	—	<b>(164)</b>
<b>Gross value as at 30 June 2001</b>	720	1 065	8 930	9 995	10 715	33 241	5 698	<b>49 654</b>
<b>Accumulated depreciation/ amortisation as at 1 July 2000</b>	n/a	243	2 067	2 310	2 310	10 589	2 364	<b>15 263</b>
Disposals	n/a	—	—	—	—	(180)	—	<b>(180)</b>
Depreciation/ amortisation charge for the year	n/a	42	922	964	964	4 391	1 014	<b>6 369</b>
Revaluations	n/a	—	—	—	—	1 571	—	<b>1 571</b>
Write-offs	n/a	—	—	—	—	(153)	—	<b>(153)</b>
<b>Accumulated depreciation/ amortisation as at 30 June 2001</b>	n/a	285	2 989	3 274	3 274	16 218	3 378	<b>22 870</b>
<b>Net book value as at 30 June 2001</b>	720	780	5 941	6 721	7 441	17 023	2 320	<b>26 784</b>
<b>Net book value as at 1 July 2000</b>	720	788	6 672	7 461	8 181	16 456	2 757	<b>27 394</b>

Table B — Summary of balances of assets at valuation as at 30 June 2001

<i>Item</i>	<i>Land</i>	<i>Buildings</i>	<i>Buildings- Leashold Improvements</i>	<i>Total buildings</i>	<i>Total land and buildings</i>	<i>Plant and equipment</i>	<i>Intangibles</i>	<i>Total</i>
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>As at 30 June 2001</b>								
Gross value	720	965	948	1 913	2 633	25 045	—	<b>27 678</b>
Accumulated depreciation/ amortisation	—	281	550	831	831	15 162	—	<b>15 993</b>
Net book value	720	684	398	1 082	1 802	9 883	—	<b>11 685</b>
<b>As at 30 June 2000</b>								
Gross value	720	965	925	1 890	2 610	14 931	2 335	<b>19 876</b>
Accumulated depreciation/ amortisation	—	243	396	639	639	9 478	1 909	<b>12 026</b>
Net book value	720	722	529	1 251	1 971	5 453	426	<b>7 850</b>

**Table C — Summary of balances of assets held under finance lease as at 30 June 2001**

<i>Item</i>	<i>Land</i>	<i>Buildings</i>	<i>Buildings- Leashold Improvements</i>	<i>Total buildings</i>	<i>Total land and buildings</i>	<i>Plant and equipment</i>	<i>Intangibles</i>	<i>Total</i>
	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000	\$'000
<b>As at 30 June 2001</b>								
Gross value	—	—	—	—	—	987	—	<b>987</b>
Accumulated depreciation/ amortisation	—	—	—	—	—	198	—	<b>198</b>
Net book value	—	—	—	—	—	789	—	<b>789</b>
<b>As at 30 June 2000</b>								
Gross value	—	—	—	—	—	998	—	<b>998</b>
Accumulated depreciation/ amortisation	—	—	—	—	—	—	—	—
Net book value	—	—	—	—	—	998	—	<b>998</b>

**2000-01**                      1999-00  
**\$ '000**                        \$ '000

**NOTE 8: Other**

Prepayments	<u>819</u>	<u>1 566</u>
-------------	------------	--------------



	2000-01 \$ '000	1999-00 \$ '000
<b>NOTE 9: Interest bearing liabilities</b>		
Finance lease commitments		
Not later than one year	240	240
Later than one year and not later than five years	600	839
	<hr/>	<hr/>
Minimum lease payments	840	1 079
Deduct: future finance charges	129	201
	<hr/>	<hr/>
Lease liability	711	878
	<hr/>	<hr/>
Lease liability is represented by:		
Current	182	167
Non-current	529	711
	<hr/>	<hr/>
	711	878
	<hr/>	<hr/>

**NOTE 10: Provisions****NOTE 10A: Employee provisions**

Salaries and wages	900	1 419
Leave	11 396	11 201
Superannuation	99	118
Other	313	284
	<hr/>	<hr/>
Total	12 708	13 022
	<hr/>	<hr/>

**NOTE 11: Payables****NOTE 11A: Supplier payables**

Trade creditors	1 880	1 196
	<hr/>	<hr/>

**NOTE 11B: Other payables**

Prepayments received	21	255
	<hr/>	<hr/>

**NOTE 12: Equity**

	<i>Accumulated results</i>		<i>Asset revaluation reserves</i>		<i>Total reserves</i>		<i>Capital</i>		<i>Total equity</i>	
	2000/01 \$000	1999/00 \$000	2000/01 \$000	1999/00 \$000	2000/01 \$000	1999/00 \$000	2000/01 \$000	1999/00 \$000	2000/01 \$000	1999/00 \$000
Balance 1 July 2000	10 978	12 472	2 135	2 135	2 135	2 135	12 928	8 928	26 041	23 535
Net surplus/(deficit)	(7 133)	1 241	—	—	—	—	—	—	(7 133)	1 241
Equity injection —										
Appropriation	—	—	—	—	—	—	240	4 000	240	4 000
Capital use charge	(1 348)	(3 161)	—	—	—	—	—	—	(1 348)	(3 161)
Net revaluation										
Increments/decrements	—	—	(205)	—	(205)	—	—	—	(205)	—
Asset adjustment	—	426	—	—	—	—	—	—	—	426
Balance 30 June 2001	2 497	10 978	1 930	2 135	1 930	2 135	13 168	12 928	17 595	26 041

	2000-01 \$ '000	1999-00 \$ '000
--	--------------------	--------------------

**NOTE 13: Cash flow reconciliation**

Reconciliation of Cash per Statement of Financial Position to Statement of Cash Flows:

• Cash at year end per Statement of Cash Flows	2 944	15 331
• Statement of Financial Position items comprising above cash: 'Financial Asset — Cash'	2 944	15 331

Reconciliation of operating surplus/(deficit) to net cash provided by operating activities:

Net surplus (deficit)	(7 133)	1 241
Depreciation/Amortisation	6 369	6 134
Write down of assets	149	396
(Increase)/Decrease in receivables	(1 775)	8 823
(Increase)/Decrease in prepayments	336	(768)
Increase/(Decrease) in employee liabilities	(314)	1 150
Increase/(Decrease) in suppliers liability	539	(292)
Increase/(Decrease) in other liabilities	(234)	255
Equity injection	—	4 000

Net cash provided/(used) by operating activities	(2 063)	20 939
--	---------	--------

	2000-01 Actual	1999-00 Actual
--	-------------------	-------------------

**NOTE 14: Services provided by the Auditor-General**

Financial statement audit services are provided free of charge to ASIO.

No other services were provided by the Auditor-General.

The fair value of audit services provided was:	51 000	51 000
--	--------	--------

**NOTE 15: Executive remuneration**

The number of executive officers who received or were due to receive a total remuneration package of \$100 000 or more (including performance pay and separation and redundancy payments):

	<b>2000-01 Number</b>	1999-00 Number
\$110 000 to \$120 000	—	4
\$120 000 to \$130 000	1	5
\$130 000 to \$140 000	4	1
\$140 000 to \$150 000	3	3
\$150 000 to \$160 000	1	—
\$160 000 to \$170 000	1	—
\$170 000 to \$180 000	1	—
\$180 000 to \$190 000	—	1
\$210 000 to \$220 000	1	—
\$230 000 to \$240 000	—	1
\$260 000 to \$270 000	1	—
\$290 000 to \$300 000	1	—
\$330 000 to \$340 000	1	—
 The aggregate amount of total remuneration of executive officers shown above.	 <b>\$ 2 692 132</b>	 <b>\$ 2 063 313</b>
 Total remuneration includes:		
The aggregate amount of performance pay paid during the year to executive officers shown above	<b>\$ 99 053</b>	\$ 33 125
 The aggregate amount of separation and redundancy payments made during the year to executive officers shown above	 <b>\$ 327 609</b>	 —

**NOTE 16: Act of Grace payments, Waivers and Defective Administration Scheme payments**

No Act of Grace payments were made during the reporting period.

No waivers of amounts owing to the Commonwealth were made pursuant to subsection 34(1) of the *Financial Management and Accountability Act 1997*.

No payments were made during the reporting period under the Defective Administrative Scheme.

	<b>2000-01 Number</b>	1999-00 Number
<b>NOTE 17: Average staffing levels</b>		
Average staffing levels	<u>560</u>	<u>538</u>

**NOTE 18: Appropriations**

Annual appropriations for Departmental items (outputs)

	<b>2000-01 \$</b>	1999-00 \$
Add: Appropriation Acts No 1 & 3 credits:		
Section 7-Act 1-basic appropriations (budget)	62 695 000	63 990 000
Section 7-Act 3-basic appropriations	—	72 000
Total Current Appropriation Acts	<u>62 695 000</u>	<u>64 062 000</u>
Add: FMA Act appropriations		
s31 appropriations	2 973 466	2 320 000
s30A appropriations (GST recoverables)	2 247 648	—
Total appropriated in the year	<u>67 916 114</u>	<u>66 382 000</u>
Balance brought forward from previous period	<u>1 633 596</u>	<u>—</u>
Total appropriations available for payments	69 549 710	66 382 000
Payments during the year	69 104 000	64 748 404
Balance of appropriations at 30 June carried to next period	<u>445 710</u>	<u>1 633 596</u>

**NOTE 18: Appropriations (continued)**

Annual appropriations for Departmental Capital items

	<i>Equity injections</i>		<i>Loans</i>		<i>Carryovers</i>		<i>Total</i>	
	<i>2000-01</i>	<i>1999-00</i>	<i>2000-01</i>	<i>1999-00</i>	<i>2000-01</i>	<i>1999-00</i>	<i>2000-01</i>	<i>1999-00</i>
	\$	\$	\$	\$	\$	\$	\$	\$
Appropriation Act No 2& 4								
Section 10 - Act No 2 (Budget)	<b>240 000</b>	—	—	—	—	—	<b>240 000</b>	—
Section 10 - Act No 4	—	4 000 000	—	—	—	8 928 000	—	12 928 000
<b>Total Current Appropriation Acts</b>	<b>240 000</b>	4 000 000	—	—	—	8 928 000	<b>240 000</b>	12 928 000
Add: FMA Act appropriations								
s30 appropriations	—	—	—	—	—	—	—	—
s30A appropriations (GST recoverables)	—	—	—	—	—	—	—	—
<b>Total appropriated in the year</b>	<b>240 000</b>	4 000 000	—	—	—	8 928 000	<b>240 000</b>	12 928 000
Balance available at 1 July brought forward from previous period	<b>4 000 000</b>	—	—	—	<b>6 459 000</b>	—	<b>10 459 000</b>	—
<b>Total appropriations available for payments</b>	<b>4 240 000</b>	4 000 000	—	—	<b>6 459 000</b>	8 928 000	<b>10 699 000</b>	12 928 000
Payments during the year	<b>4 240 000</b>	—	—	—	<b>6 459 000</b>	2 469 000	<b>10 699 000</b>	2 469 000
Balance of appropriations for capital at 30 June carried to next period	—	4 000 000	—	—	—	6 459 000	—	10 459 000

**NOTE 19: Reporting of Outcomes**

	<b>Budget \$'000</b>	<b>Actual \$'000</b>
Net cost of entity outputs	70 115	71 285
Extraordinary items	—	—
Net cost to Budget outcome	<u>70 115</u>	<u>71 285</u>
Total assets deployed as at 30/6/01	<u>24 451</u>	<u>32 584</u>

**Major Revenues and Expenses****Operating Revenues**

Revenue from Government	62 695	64 152
Sale of goods and services	598	3 345
Other non-taxation revenues	2 834	2 039
	<u>66 127</u>	<u>69 536</u>
Total operating revenues	<u>66 127</u>	<u>69 536</u>

**Operating Expenses**

Employees	37 447	41 937
Suppliers	29 621	27 628
Other	6 479	7 104
	<u>73 547</u>	<u>76 669</u>
Total operating expenses	<u>73 547</u>	<u>76 669</u>

**NOTE 20: Financial Instruments****NOTE 20A: Terms, conditions and accounting policies**

<i>Financial Instrument</i>	<i>Notes</i>	<i>Accounting policies and methods (including recognition criteria and measurement basis)</i>	<i>Nature of underlying instrument (including significant terms and conditions affecting the amount, timing and certainty of cash flows)</i>
Financial assets		Financial assets are recognised when control over future economic benefits is established and the amount of the benefit can be reliably measured.	
Cash – deposits at call		Deposits are recognised at their nominal amounts. Interest is credited to revenue as it accrues.	ASIO invests funds with the Reserve Bank of Australia. Monies in the Agency's bank accounts are swept into the Official Public Account nightly and interest is earned on the daily balance at rates based on money market call rates. Rates have averaged 4.9% for the year.
Receivables for goods and services	6A	These receivables are recognised at the nominal amounts due less any provision for bad or 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.	Credit terms are net 30 days (1999-00: 30 days).
Accrued revenue		Interest is credited to revenue as it accrues. Interest on ASIO's operating bank account is payable quarterly. Interest on fixed interest deposits is payable on maturity.	Interest: as for cash.
Financial liabilities		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	11A	Creditors and accruals are recognised at their nominal amounts, being the amounts at which the liabilities will be settled. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced).	Settlement is usually made net 30 days.
Finance lease liabilities	9	Liabilities are recognised at the present value of the minimum lease payments at the beginning of the lease. The discount rates used are estimates of the interest rates implicit in the leases.	At reporting date, ASIO had one finance lease with a term of 5 years. The interest rate implicit in the lease is 7.08%. The lease assets secure the lease liabilities.



NOTE 20B: Interest rate risk: agency

Financial Instrument	Notes	Floating Interest Rate	Fixed Interest Rate				Non-Interest Bearing	Total	Weighted Average Effective Interest Rate
			1 year or less	1 to 2 years	2 to 5 years	> 5 years			
		2000-01 \$'000	99-00 \$'000	2000-01 \$'000	99-00 \$'000	2000-01 \$'000	99-00 \$'000	2000-01 %	99-00 %
<b>Financial Assets</b>									
Cash at Bank		2 944	5 331	—	—	—	—	4.9	4.8
Receivables for goods and services	6A	—	—	—	—	2 037	262	N/A	N/A
<b>Total Financial Assets (Recognised)</b>		2 944	5 331	—	—	2 037	262	4 981	15 593
<b>Total assets</b>								32 915	44 553
<b>Financial Liabilities</b>									
Finance lease liabilities	9	—	—	711	878	—	—	711	878
Trade creditors	11A	—	—	—	—	1 880	1 196	1 880	1 196
<b>Total Financial Liabilities (Recognised)</b>		—	—	711	878	1 880	1 196	2 591	2 074
<b>Total liabilities</b>								15 320	18 512

**NOTE 20C: Net fair values of financial assets and liabilities**

	Note	2000-01		1999-00	
		Total carrying amount \$'000	Aggregate net fair value \$'000	Total carrying amount \$'000	Aggregate net fair value \$'000
<b>Departmental Financial Assets</b>					
Cash at Bank		2 944	2 944	15 331	15 331
Receivables for Goods and Services	6A	2 037	2 037	262	262
<b>Total Financial Assets</b>		<b>4 981</b>	<b>4 981</b>	<b>15 593</b>	<b>15 593</b>
<b>Financial Liabilities (Recognised)</b>					
Finance lease liabilities	9	711	711	878	878
Trade creditors	11A	1 880	1 880	1 196	1 196
<b>Total Financial Liabilities (Recognised)</b>		<b>2 591</b>	<b>2 591</b>	<b>2 074</b>	<b>2 074</b>

*Financial assets*

The net fair values of cash and non-interest-bearing monetary financial assets approximate their carrying amounts.

*Financial liabilities*

The net fair value of the finance lease is based on discounted cash flows using current interest rates for liabilities with similar risk profiles. (Where the liability is on a floating rate of interest, the method returns the principal amount).

The net fair values for trade creditors are short-term in nature, are approximated by their carrying amounts.

**NOTE 20D: Credit Risk Exposures**

The Agency's maximum exposures 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 Assets and Liabilities.

ASIO has no significant exposures 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.

# Part 5

## **appendixes**

## Appendix A

### Membership of the Parliamentary Joint Committee on ASIO

Membership of the PJC during the reporting year comprised:

- Hon. David Jull, MP (LP, Fadden, QLD) - Presiding Member
- Senator Paul Calvert (LP, TAS)
- Senator Sandy Macdonald (NP, NSW)
- Hon. Senator Robert Ray (ALP, VIC)
- Mr Stewart McArthur, MP (LP, Corangamite, VIC)
- Mr John Forrest, MP (NP, Mallee, VIC)
- Hon. Leo McLeay, MP (ALP, Watson, NSW)

## Appendix B

### Contact information

#### **Written inquiries**

The Director-General of Security

ASIO Central Office

GPO Box 2176

CANBERRA ACT 2601

#### **Website**

[www.asio.gov.au](http://www.asio.gov.au)

#### **General inquiries**

Central Office switchboard

Tel: (02) 6249 6299

1800 020 648 (toll free)

Fax: (02) 6257 4501

#### **Media inquiries**

Media Liaison Officer

Tel: (02) 6249 8381

Fax: (02) 6262 9547

#### **Collection office telephone inquiries**

Australian Capital Territory (02) 6249 7415

Victoria (03) 9654 8985

New South Wales (02) 9281 0016

Queensland (07) 3831 5980

South Australia (08) 8223 2727

Western Australia (08) 9221 5066

Northern Territory (08) 8981 2374

Tasmanian residents may call

ASIO Central Office toll free 1800 020 648

## Appendix C

## Staffing statistics

*Table A. Staffing levels and number at 30 June, 1996-97 to 2000-01*

	96-97	97-98	98-99	99-00	00-01
Average staffing level (ASL) for each Financial Year (FY)	537	488	513	538	560
Full time staff equivalent (FSE) at end of each FY	524	480	525	565	551
Number of staff at the end of each FY	571	536	566	605	584

*Table B. Composition of the workforce (number at 30 June each year)*

	96-97	97-98	98-99	99-00	00-01
Permanent full-time	519	469	473	469	453
Temporary full-time	16	13	30	77	63
Permanent part-time	18	23	22	20	26
Temporary part-time	—	3	6	10	14
Casual	8	22	21	22	25
Non-operational (including unattached and on compensation)	10	6	14	7	3
<b>Total</b>	<b>571</b>	<b>536</b>	<b>566</b>	<b>604</b>	<b>584</b>

*Table C. SES equivalent staff classification and gender (positions at level) at 30 June each year*

		96-97	97-98	98-99	99-00	00-01
Band 1	Female	2	2	1	1	1
	Male	8	7	9	9	9
Band 2	Female	2	1	1	1	1
	Male	2	2	2	2	2
Band 3	Male	1	1	1	1	1
<b>Total</b>		<b>15</b>	<b>13</b>	<b>14</b>	<b>15</b>	<b>14</b>

Note - this table does not include an unattached SES officer.

## Appendix D

## Workplace diversity statistics

**Table A. Representation of designated groups within ASIO occupational groups at 30 June 2001**

Group	Total staff <sup>1</sup>	Women <sup>2</sup>	NESB	ATSI	PWD	Staff with EEO data <sup>2</sup>
SES	14	2	0	0	1	12
Senior Officers <sup>3</sup>	98	15	2	0	1	97
AO5 <sup>4</sup>	236	82	28	1	7	223
AO1-4 <sup>5</sup>	217	134	7	1	8	212
ITO1-2 <sup>6</sup>	18	3	2	0	0	18
ENG1-2 <sup>7</sup>	1	0	0	0	0	1
<b>TOTAL</b>	<b>584</b>	<b>235</b>	<b>39</b>	<b>2</b>	<b>17</b>	<b>563</b>

Source: CHRIS (Complete Human Resource Information System, ASIO's computerised personnel system)

- <sup>1</sup> Based on staff salary classifications recorded in CHRIS.
- <sup>2</sup> Provision of EEO data by staff is voluntary. ASIO made a concerted effort to collect missing data during this financial year.
- <sup>3</sup> The Senior Officer group is the equivalent to the APS EO1 to EO2 classifications and includes equivalent officers in the Engineer and Information Technology classifications.
- <sup>4</sup> The AO5 (ASIO Officer Grade 5) group is equivalent to APS Level 6 and includes ASIO Generalist Intelligence Officers.
- <sup>5</sup> The AO1-4 group spans the APS 1-5 salary range. Salaries for Generalist Intelligence Officer Trainees are included in this group (equivalent to APS grade 3).
- <sup>6</sup> Information Technology Officers Grades 1 and 2.
- <sup>7</sup> Engineers Grades 1 and 2.

**Table B: Percentage representation of designated groups in ASIO 2000-01**

Group	June 1997	June 1998	June 1999	June 2000	June 2001
Women <sup>1</sup>	36	37	38	40	40
Race or Ethnicity	8	8	8	8	6
ATSI	0.2	0.4	0.4	0.4	0.3
PWD	4	4	4	4	3

Source: CHRIS (Complete Human Resource Information System, ASIO's computerised personnel system)

- <sup>1</sup> Percentages for women based on total staff; percentages for other groups based on staff for whom EEO data was available.

**Key to abbreviations:**

- R or E Race or Ethnicity (previously NESB - Non-English Speaking Background)  
 ATSI Aboriginal and Torres Strait Islander.  
 PWD People with a disability.

## Appendix E

### ASIO salary classification structure at 30 June 2001

#### **ASIO MANAGERS**

SES Band 3	131 922		minimum point
SES Band 2	104 539		minimum point
SES Band 1	87 597		minimum point
AEO 2.2	79 871		
AEO 2	72 385	to	77 438
AEO 1	63 736	to	72 385

#### **ASIO OFFICERS**

ASIO Officer 5	48 413	to	56 188
ASIO Officer 4	40 628	to	45 811
ASIO Officer 3	35 429	to	38 176
ASIO Officer 2	31 200	to	34 512
ASIO Officer 1	27 653	to	30 484

#### **ASIO ITOs**

SITOA	79 871		
SITOB	72 385	to	77 438
SITOC	63 736	to	68 859
ITO2	49 260	to	56 188
ITO1	38 176	to	43 863

#### **ASIO ENGINEERS**

SIO(E)5	81 152		
SIO(E)4	68 859	to	77 438
SIO(E)3	63 736	to	65 415
SIO(E)2	49 260	to	54 736
SIO(E)1	33 221	to	46 300



## Appendix F

### Assumed identities

During the year 21 assumed identity approvals were granted in accordance with the *NSW Law Enforcement and National Security (Assumed Identities) Act 1998*. None were varied or revoked.

The general nature of the duties undertaken by officers under the assumed identities concerned:

- surveillance duties
- intelligence officer duties, and
- support officer duties.

The most recent audit required in accordance with section 11 of the Act was conducted in July 2001 for the preceding financial year. The audit did not disclose any fraudulent or other criminal behaviour.

## Glossary of acronyms and abbreviations

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
ANAO	Australian National Audit Office
APS	Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
CHOGM	Commonwealth Heads of Government Meeting
DFAT	Department of Foreign Affairs and Trade
DIMA	Department of Immigration and Multicultural Affairs
DIO	Defence Intelligence Organisation
DSD	Defence Signals Directorate
EEO	Equal Employment Opportunity
MP	Member of Parliament
NAA	National Archives of Australia
NATP	National Anti-Terrorist Plan
NIG	National Intelligence Group
NII	National Information Infrastructure
OFMs	Olympic Family Members
OH&S	Occupational Health and Safety
ONA	Office of National Assessments
PJC	Parliamentary Joint Committee (on ASIO)
PSM	Protective Security Manual
QC	Queen's Counsel
SAC-PAV	Standing Advisory Committee on Commonwealth-State Cooperation for Protection Against Violence
SES	Senior Executive Service
TSU	Technical Support Unit
UBL	Usama bin Laden
WEF	World Economic Forum

# Compliance index

<b>Annual Report requirement</b>	<b>Page</b>
Assumed identities	103
Advertising and market research	53
Consultants and contractors	61
Contact details	99
Corporate governance	45
Disability strategy	56
Environmental performance	60
External scrutiny	25, 29-30, 35, 38, 39, 45, 46-50, 51
Financial performance	13
Financial statements	63
Freedom of Information	23
Glossary	104
Index	106
Industrial democracy	45
Internet home page address and Internet address for report	52
Letter of transmittal	iii
Management of human resources	51-57
Occupational health and safety	57
Organisational structure	8
Outcome and Output structure	9-10
Performance pay	52
Purchasing	61
Report on performance	11-41
Review by Director-General	3-7
Staffing statistics	100-101
Summary resource table	13
Table of contents	v
Workplace agreements	52

## General index

### A

accountability, 5, 6, 35, 38, 39, 45-50, 98  
Administrative Appeals Tribunal, 23, 25, 29-30  
advertising costs, 53  
Al Qaida. *See Usama bin Laden.*  
anti-globalisation protests, 14, 16-17, 20  
appeal mechanisms, 23, 25  
archival records, access to, 23-25, 49  
ASIO Act, vii, 36  
ASIO staff. *See staff*  
assumed identities, 103  
Attorney-General, accountability to, viii, 35, 39, 45, 47  
audio counter-measures. *See electronic and audio counter-measures*  
audit and evaluation, 5, 45, 46, 55, 59  
Auditor-General, viii  
Australian agencies, liaison with. *See liaison with Australian agencies*  
Australian National Audit Office, 45

### B

Blick Report. *See Inquiry into Security Issues*  
border control. *See visa checking*  
building management, 60

### C

capabilities. *See investment in capabilities*  
Centenary of Federation, 31  
CHOGM, 3, 6, 14, 15, 16, 17, 20, 30, 32, 37, 38, 39, 40, 52, 57  
Comcare, 57  
Commonwealth Heads of Government Meeting. *See CHOGM*  
communications. *See information management.*  
community interview program, 3, 37  
compensation claims, 57

complaints about ASIO, 48, 50  
compliance index, 105  
computer attack. *See National Information Infrastructure Protection, computer exploitation*  
computer exploitation, 34, 36  
consultants and contractors, 61  
contact information, 99  
controversial visitors. *See visa checking - recommendations against entry*  
corporate governance, 45  
corporate planning, 5, 6, 45  
cost recovery, 30  
counter-espionage, 18  
counter-intelligence. *See internal security*  
counter-terrorism capability, 5, 40  
Counter-Terrorist Overseas Response Group. *See CTORG*  
critical infrastructure protection. *See National Information Infrastructure Protection*

### CTORG, 40

### D

diplomatic interests, threats to, 20  
disability strategy, 56  
disruption operations, 37  
Dowling, Sherryl, 3, 26

### E

ecologically sustainable development, 60  
EEO. *See workplace diversity*  
electronic and audio counter-measures, 30  
encryption, 36  
engineering development. *See technical development*  
entry and search of premises, 34, 35, 38  
entry to Australia, controls on. *See visa checking*

**General index (continued)**

- environmental performance, 60
- equal employment opportunity. *See workplace diversity*
- equipment testing, 33
- e-security. *See National Information Infrastructure Protection*
- espionage, 3, 18, 22, 26
- Espionage Act, 18
- ethics, 55
- evaluation. *See audit and evaluation*
- examination of postal and delivery service articles, 34, 35
- external scrutiny. *See accountability*
- F
- financial performance, 13
- financial statements, 63-96
- foreign intelligence collection, 41
- foreign intelligence service activity in Australia, 3, 18, 22, 26
- foreign interference, 18
- foreign liaison. *See liaison with overseas services*
- FOSIC. *See Olympics*
- fraud control, 5, 46
- Freedom of Information, 23
- G
- 'Gatekeeper' accreditation, 32
- glossary, 104
- H
- human resource development. *See staff training and development*
- human resource management, 51-57
- human source intelligence collection, 36-37
- I
- illegal arrivals. *See unauthorised arrivals*
- industrial democracy, 45, 52
- information management, 5, 57-58
- Inquiry into Security Issues, 3, 4, 6, 27, 30, 32, 58
- Inspector-General of Intelligence and Security, viii, 35, 38, 39, 47, 48, 55.  
*See also Inquiry into Security Issues*
- intelligence collection, 34-39
- intelligence service activity in Australia.  
*See foreign intelligence service activity in Australia.*
- Intelligence Services Bill, 50
- Inter-Agency Security Forum, 27-28
- internal security, 5, 58-60
- internet interception, 36
- intrusive methods of investigation. *See warrant operations*
- investment in capabilities, 3, 5, 40-41, 57-58
- Israeli/Palestinian conflict, 4
- Issue Motivated Groups, 16, 17
- L
- Lappas, Simon, 3, 26
- Leader of the Opposition, 47
- legislation. *See ASIO Act, Telecommunications Act 1977, Espionage Act, Intelligence Services Bill*
- liaison with
- Australian agencies, 3, 14, 18, 19, 21, 22, 23, 26, 27, 28, 29, 31-32, 38-39, 41
  - overseas services, 15, 16, 18, 26, 39
  - police, 3, 14, 15, 16, 18, 19, 26, 38-39
  - listening devices, 34, 35
- M
- management and accountability, 5, 43-61
- management structure chart, 8
- media policy, 51
- Middle East Peace Process. *See Israeli/Palestinian conflict*
- mission statement, vii

**General index (continued)**

N

National Anti-Terrorist Plan (NATP), 14, 40

National Information Infrastructure Protection, 5, 6, 18

National Security Committee of Cabinet, viii, 45

O

occupational health and safety, 57

Office of National Assessments, shared tenancy, 60

Olympic Games

Sydney 2000 Olympics, 3, 4, 14, 15, 16, 17, 18, 20, 23, 29, 37, 38, 39, 40, 52, 54, 57

Athens 2004 Olympics, 39

open source information, 5, 37

organisational structure chart. *See management structure chart*

Osama bin Laden. *See Usama bin Laden*

Outcome, 9

Outlook, 6

Output performance, 11-41

Outputs

enabling, 10

foreign intelligence, 10, 41

protective security advice, 9, 27-33

security intelligence analysis & advice, 9, 14-25

security intelligence investigation & capability, 9, 34-41

P

Palestinian/Israeli conflict. *See Israeli/Palestinian conflict*

Paralympics. *See Olympics*

Parliamentary Joint Committee on ASIO, 6, 48-50, 98

people management. *See staff*

performance pay, 52

performance report, 11-41

personnel security assessments, 3, 4, 28-30

adverse and qualified assessments, 4, 28, 29

appeals, 29-30

CHOGM, 30

Olympic Games, 29

physical security, 5, 30-33, 59

cost recovery, 30

PMV. *See politically motivated violence*

police, liaison with. *See liaison with police*

politically motivated violence, 3, 4, 6, 7, 14-17, 19-20, 22

foreign influenced, 3, 4, 7, 14-16

local, 14, 16-17

polygraph trial, 30

postal and delivery service articles, examination of, 34, 35

prevention and disruption operations, 37

protective security, 3, 4, 5, 19, 27-33

Protective Security Manual, 4, 32

Protective Security Policy Committee, 27

protective security risk reviews. *See physical security*

protest activity. *See violent protest activity*

public, ASIO's contact with, 48-49, 50-51, 99

purchasing, 61

R

recruitment. *See staff recruitment*

risk management advice, 31-32

S

SAC-PAV, 40

salary classification structure, 102

search of premises. *See entry and search of premises*

Secretaries Committee on National Security, viii, 28

**General index (continued)**

- security of ASIO. *See internal security*
- security assessments
- illegal arrivals. *See visa checking, unauthorised arrivals*
  - Olympic Family Members. *See Olympics*
  - Olympics accreditation. *See Olympics*
  - personnel. *See personnel security assessments*
  - visa checking. *See visa checking*
- security clearances. *See staff security clearances*
- Security Equipment Catalogue, 33
- security equipment testing and standards, 33
- security intelligence analysis and advice, 9, 14-25
- Security Construction Reference Manual, 33
- Senate Estimates, 47
- separations. *See staff separations*
- September 11 terrorist attack. *See terrorism*
- SIDC-PAV, 40
- special powers. *See warrant operations*
- staff , 51-57
- People Management Plan, 51
  - people management priorities, 51
  - performance pay, 52
  - salary classification structure, 102
  - staff recruitment, 5, 52-53
  - staff security clearances, 5, 59
  - staff separations, 5, 53
  - staff training and development, 6, 54-55
  - staffing profile, 6, 52, 100-101
  - staffing statistics, 56, 100-101
  - workplace diversity, 55-56
  - workplace relations, 45, 52
- staff development. *See training and staff development*
- strategic planning, 5, 6, 45
- surveillance, 37, 38
- sweeps. *See electronic and audio counter-measures*
- T
- technical development, 40
  - Technical Support Unit, 40
  - technical surveillance counter-measures. *See electronic and audio counter-measures*
- Telecommunications Act 1977, 36
- telecommunications environment, 3, 36
- foreign government investment, 36
- telecommunications interception, 34, 35, 36-37
- terrorism, 3, 6, 7, 15, 22
- September 11 terrorist attack, 7
  - Usama bin Laden, 7, 15
- threat assessments, 4, 7, 14, 19-21
- threat levels in Australia. *See threat assessments*
- Top Secret accreditation, 32
- tracking devices, 34, 35
- training and development. *See staff training and development*
- U
- UBL. *See terrorism*
  - unauthorised arrivals. *See visa checking*
  - Usama bin Laden. *See terrorism*
- V
- values, vii
  - vetting. *See personnel security assessments*
  - violent protest activity, 20
  - visa checking, 4, 21-23
    - Olympic Family Members, 23
    - recommendations against entry, 4, 22
    - unauthorised arrivals, 3, 4, 22
- vision, vii

**General index (continued)**

W

- warrant operations, 34, 35-36, 41
  - approvals, 35
  - computer access, 34, 36
  - entry and search, 34, 35, 38
  - examination of postal and delivery service articles, 34, 35
  - foreign intelligence warrants, 41
  - listening devices, 34, 35
  - security intelligence warrants, 35
  - tracking devices, 34, 35
  - telecommunications interception, 34, 35, 36-37
- website, 48-49, 51, 53
- Wispelaere, Jean-Philippe, 26
- women in ASIO, 56
- workforce planning, 5, 54
- Workplace Agreement, 52
- workplace diversity, 55-56, 101
- workplace relations, 45, 52
- World Economic Forum, 4, 15, 16, 17, 38