

Australian Security Intelligence Organization

# Report to Parliament 1995–96

© Commonwealth of Australia 1996

This work is copyright. Apart from any use permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Australian Security Intelligence Organization. Requests and inquiries concerning reproduction and rights should be addressed to the Director-General of Security, Box 2176, Canberra, ACT 2601.

Produced and printed by the Australian Security Intelligence Organization.



---

**Australian Security Intelligence Organization**

GPO Box 2176 Canberra City ACT 2601 Telephone 06 249 6299 Facsimile 06 257 4501

Office of the Director-General

2 December 1996

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

Dear Attorney-General,

With this letter I submit the annual report on the Australian Security Intelligence Organization (ASIO) for the year ending 30 June 1996, as required by section 94 of the *Australian Security Intelligence Organization Act 1979*.

The report was prepared under the stewardship of my predecessor as Director-General of Security, David Sadleir. Unfortunately the intricacies of ASIO's annual reporting procedures (involving classified and unclassified versions and a less-than-straightforward audit process) meant that Mr Sadleir was unable to sign off the report before his last day of duty on 10 October 1996.

This classified annual report has a very limited distribution. At the same time I present to you an unclassified version (some 20 per cent shorter) for tabling in the Parliament.

Yours sincerely,

Dennis Richardson  
Director-General of Security



# About ASIO

## ASIO'S MISSION STATEMENT

*ASIO provides advice to protect Australia and its people from threats to national security.*



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

The Australian Security Intelligence Organization (ASIO) was established in 1949, and operates under the *Australian Security Intelligence Organization Act 1979* (the ASIO Act). The chief executive is the Director-General of Security, who is responsible to the Attorney-General.

ASIO is an advisory body. Our intelligence and advice are transmitted to government and to executive agencies of government as a basis for decision-making and action. Our main function is to gather information and produce intelligence that will enable us to warn government about activities that might endanger Australia's national security.

Much of this information comes from interviews and publicly available sources. Other material comes from liaison partners. If there is sufficient justification, the Attorney-General may authorise ASIO to use special powers to collect information though intrusive means (such as listening devices or telephone interception).

We do not limit the rights of Australians to engage in lawful advocacy, protest or dissent, and we must stay free of political or sectional bias.

ASIO's other functions include:

- advising government agencies on ways of identifying and managing risks to their organisational (and therefore national) assets, including people, property and information
- contributing to Australia's counter terrorism defences through policy development and maintaining a response capability
- contributing to foreign intelligence collection in Australia.

ASIO's net expenditure in 1995–96 was \$51.5 million.

Address inquiries about ASIO to any of the offices listed on page 101 or to the public liaison number (06) 249 8381, fax (06) 234 1449.



*Mr David Sadleir, AO,  
Director-General of Security  
from April 1992 to October 1996.*

## Contents

About ASIO	iv
Abbreviations used in the report	vi
<b>Corporate Overview</b>	
The world security scene and implications for Australia	3
Security priorities in 1995–96	4
Sharpening our focus	6
Our focus at a glance	10
Our clients	12
Our partners	15
Our technology	17
Our workforce	19
Our efficiency	24
Our reputation	28
<b>Program Reports</b>	
Our program framework	37
Summary of program outcomes	38
Security Intelligence Program	39
Protective Security Program	43
Foreign Intelligence Collection Program	50
Counter Terrorism Support Program	51
Corporate Support Program	53
Information available on request	54
<b>Financial Statements</b>	<b>55</b>
<b>Appendixes</b>	
List of appendixes	79
A: Countries approved for liaison purposes at 30 June 1996	80
B: Staff management statistics	81
C: Equal employment opportunity statistics	86
D: Evaluations	88
E: Public access to ASIO's records	90
F: Program and notional breakdown of expenditure	92
G: Significant threat assessments	93
H: Recommendations against entry or residence	95
Compliance index	96
General index	98
ASIO contact information	101



## Abbreviations used in the report

AAT	Administrative Appeals Tribunal	MAB	Management Advisory Board
ACC	ASIO Consultative Council	MIAC	Management Improvement Advisory Committee
AEC	Audit and Evaluation Committee	NATEX	National Exercise
AFP	Australian Federal Police	NATP	National Anti-Terrorist Plan
AISA	Australian intelligence and security agencies	NCBW	nuclear, chemical and biological weapons
AM	Member of the Order of Australia	NIG	National Intelligence Group
ANAO	Australian National Audit Office	OASYS	office automation systems
AO	Officer of the Order of Australia	OH&S	occupational health and safety
APS	Australian Public Service	ONA	Office of National Assessments
AQC	Australian Quality Council	OPREX	Operational Response Exercise
ASIO	Australian Security Intelligence Organization	PC	personal computer
ASIS	Australian Secret Intelligence Service	PJC	Parliamentary Joint Committee (on ASIO)
CSIRO	Commonwealth Scientific and Industrial Research Organisation	PM&C	Prime Minister and Cabinet (Department of the)
DFAT	Department of Foreign Affairs and Trade	PSCC	Protective Services Co-ordination Centre
DIMA	Department of Immigration and Multicultural Affairs	SAC-PAV	Standing Advisory Committee on Commonwealth-State Cooperation for Protection Against Violence
DIO	Defence Intelligence Organisation	SES	Senior Executive Service
DoF	Department of Finance	SIDC-PAV	Special Interdepartmental Committee for Protection Against Violence
EEO	equal employment opportunity	SIO	Specialist Intelligence Officer
GAA	Graduate Administrative Assistant	SOCOG	Sydney Organising Committee for the Olympic Games
GIO	Generalist Intelligence Officer	WMD	weapons of mass destruction
IGIS	Inspector-General of Intelligence and Security		
IT	information technology		
JIG	Joint Intelligence Group		

# Corporate Overview

*... in a changing world worthy institutions can  
be conserved only by adjusting them to the  
changing time.*

---

FRANKLIN D. ROOSEVELT, 1936





# The world security scene and implications for Australia

The geopolitical environment of the mid-1990s is characterised by a much reduced threat of global nuclear war, but also by the removal or lessening of constraints on the behaviour of nation States, parts of States and minorities.

The consequence has been a surge in efforts by minorities (religious, racial, cultural, economic or a combination of these) to express and seek recognition of their separate identities and needs, inevitably leading to conflict or stress. All too frequently these conflicts explode into violence, expressed formally by wars, or informally by terrorism.

The environment is further complicated by apprehension about shifts in economic power or influence, constituting a spur on economic espionage and technology acquisition. Advances in communications, transportation and computer technology have also opened the way to new dimensions of transnational crime, terrorism and proliferation of weapons of mass destruction. A particularly disturbing trend is towards large-scale terrorist acts designed to kill as many innocents as possible and a growing disregard for their own lives by perpetrators.

Australia is less and less insulated by its geostrategic position. Rapid advances in technology, continued extensions of global economic interdependence and an increasingly multicultural society mean Australia is obliged to be more sensitive to the pressures of global trends.

Ethnic and cultural tensions and radical conservatism are on the rise in many countries. And Australia is no exception.

The neo-nazi element and covert extreme nationalist militias have captured public attention in recent times through their willingness to threaten violence in order to further their political agendas.

In the region of which Australia is a part, religious extremism is no less evident than elsewhere in the world and draws inspiration from a wide range of sources—often multi-national networks.

Representing a response to the global environment and a new challenge, computing and communications technologies have converged, making communications between countries easier and more secure. Australians have adopted the new technologies enthusiastically, thus negating some of the isolating barriers which once assisted security.

These advances have also created a dependence on infrastructure which are threatened by amateur hackers and hostile governments. 'Information warfare' is now an emerging security issue. In fact, rapid economic development and competition in Asia and the quickening pace of Australia's involvement in the region have already led to increased interest in Australian science and technology.

It is in this environment that ASIO must operate. We need to be alert and responsive to change, sharpening our focus to ensure that human and physical resources are deployed to maximum effectiveness—a challenge all Australians face together.



## Security priorities in 1995–96

Against this background, Australia continued to face a number of security problems which were directly related to overseas events or reflected international movements and trends.

The year began with the prospect of continued violent reaction to the resumption of French nuclear testing in the South Pacific. While there was no further act similar to the June 1995 firebombing of the premises of the Honorary French Consulate in Perth, ASIO continued to provide threat assessments for French interests through the period of protests.

The trend towards extremism emerged as a more serious issue, with successor groups to the Loyal Regiment of Australian Guardians continuing to threaten violence. Public debate over proposed changes to weapons legislation following the Port Arthur shootings in April 1996 gave these groups greater prominence. Federal and state politicians were the target of telephone threats and mock letter bombs.

The activities of these groups and the federal election led to a significant increase in threat assessments issued bearing on the security of Australian holders of high office. The increased demand was only partly counter-balanced by a fall in threat assessments on other subjects, such as visiting overseas dignitaries and controversial figures.

Despite the reduction in numbers, such visits still demanded considerable effort

by ASIO and law enforcement agencies. In this regard the visit of author Salman Rushdie required a high level of confidentiality and dedicated resources. (Rushdie has been under threat from Islamic extremists since publication of *The Satanic Verses* in 1989; his Japanese translator has been killed and two publishers injured in separate attacks.) Protests, such as that against the visit by Vietnamese Vice-President Do Muoi, and others against various Indonesian officials, though prompted by events overseas, required attention from ASIO and the law enforcement community.

The continued resource implications of providing threat assessments to protect Australian public figures and foreign visitors was significant. Work was begun to draw on this experience in planning for the Sydney Olympic Games and the centenary of Federation. Security planning for these events began in earnest during 1995–96, directed particularly at the Olympic Games; and the implementation of better threat assessment processes also gained pace.

A corollary to this planning was the attention given to Australia's visitor entry system. In March 1996 the Parliamentary Joint Standing Committee on Migration, reporting on its inquiry into Australia's visitor visa system, recommended the testing of electronic visas. The change has implications for ASIO, which worked closely with the Department of Immigration and Multicultural Affairs (DIMA) to ensure the security

requirements of the visa system were adequate to protect Australia while having minimal impact on legitimate travel.

As well as contributing to the safety of people within Australia, ASIO played a part in ensuring their safety overseas, by providing threat and protective security assessments and through general security intelligence reporting.

ASIO's role in threat assessment and visa checking is part of a joint effort involving many other agencies, and we continued to work with them to support government commitments to security, both inside Australia and overseas. Multi-agency cooperation works well in reducing potential community unrest and protest violence, while effective visa checking procedures do much to identify and prevent terrorists entering or remaining in the country.

This security intelligence cooperation was enhanced in 1995–96 by ASIO participation in several national and international conferences and seminars.

ASIO's investigations and advice also respond to an active and sometimes subtle intrusion by foreign intelligence services. Hostile intelligence activity can take several forms: espionage, attempts to influence émigré communities or communities holding opposing political or religious views, the fostering of communal violence or acts directed against the Australian government to influence its decision-making in ways detrimental to Australian interests.

Australia remains a target for such activities. The interest of foreign intelligence services may be motivated by a perception that Australia is a competitor, economic or otherwise.

Globally the trend is towards a greater concentration on economic, scientific and technological espionage, although traditional political and military espionage is still attempted. In addition, there is the attraction of sensitive information Australia holds about our region and our allies.

The increased emphasis that hostile intelligence services place on science and technology complements the continued interest of other agencies of foreign governments in using Australia covertly to assist their nuclear, chemical and biological weapons (NCBW) development programs. Investigations during the reporting period underlined the continued risk of proliferators acquiring dual-use technology from Australia, obtaining knowledge applicable to NCBW programs here, or using Australia as a conduit for the transfer of related technology.

Action was taken to increase awareness of the proliferation risk and to give researchers and manufacturers a better understanding of how their activities might be manipulated to help make weapons of mass destruction. A project to better define the threat from espionage directed at Australian science and technology was also undertaken.

Further details of investigative outcomes are contained in the Security Intelligence Program report (page 39), although they have been mostly excluded from the unclassified *Report to Parliament*.



# Sharpening our focus

The theme of this year's report on ASIO's performance is 'sharpening our focus'. In October 1995 a new edition of our corporate plan was published (*ASIO Corporate Plan 1995–96 to 1998–99*). The plan sets out six corporate goals and associated broad strategies as a framework for all our activities.

The plan arose from a two-day workshop in which ASIO's higher management group explored ways of using resources, products and services more creatively and effectively; and examined the key issues of clients, relationships, technology and people management. Managers agreed that ASIO needed to sharpen its focus on linking strategic priorities to corporately agreed goals and structures, within the budgetary blueprint of ASIO's forward estimates.

In 1995–96 three imperatives directed our business and strategic priorities. They are described below.

## **National security intelligence strategy**

The first imperative was to maintain the national security intelligence strategy developed during the last reporting period. The strategy is our fundamental planning instrument, used to decide priorities, report to government, and link assessments to forward budget estimates.

Security priorities and planning are part of a wider national interest involving many other agencies, including the

departments of Defence, Foreign Affairs and Trade, and Immigration and Multicultural Affairs. ASIO's security intelligence planning forms part of a strategic planning structure encompassing foreign, security and law enforcement intelligence which dovetails ASIO's corporate strategies with those of relevant departments, other members of the Australian intelligence and security community, and the law enforcement agencies. ASIO works with all these bodies to meet security objectives and minimise duplication.

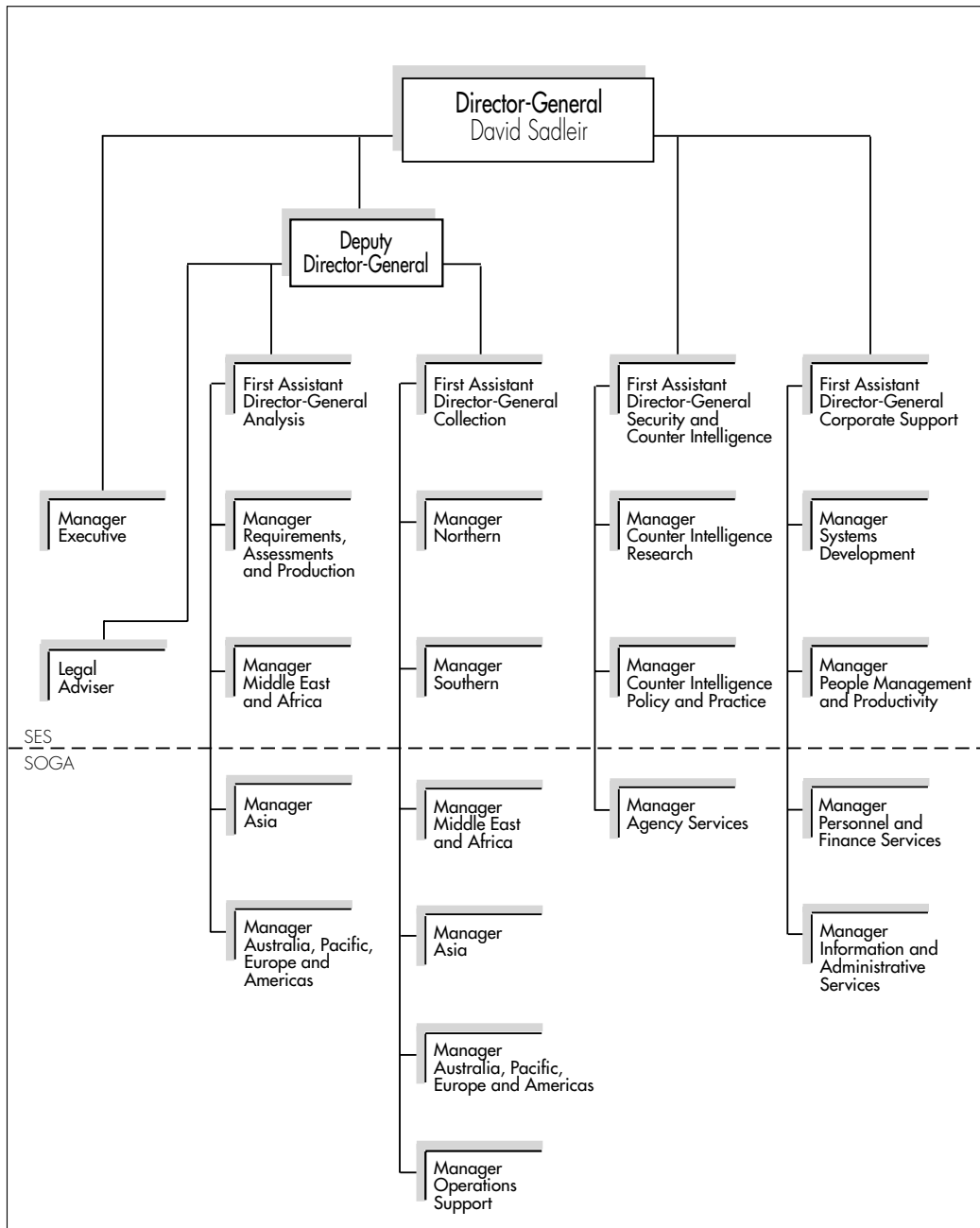
## **Security management plan**

The second imperative was to develop and deploy strategies in response to recommendations of a government inquiry into various aspects of national security, conducted in 1995 by Mr Michael Cook, AO. (Our last classified *Annual Report* dealt with the outcomes in some detail.)

Underpinning the whole strategic approach was the creation and staffing of a new Security and Counter Intelligence (SCI) Division (see Figure 1), headed by a Senior Executive Service Band 2 equivalent officer. The new division comprises three branches, each with distinct counter intelligence and security responsibilities:

- *Counter Intelligence Policy and Practice (CIPP) Branch*—responsible for implementing and overseeing policies and procedures relating to

Figure 1: Management structure at 30 June 1996





- ASIO's internal security and ensuring the continued integrity of our security practices, notably in respect of computer auditing, security revalidation of staff, and effective operational review.
- *Counter Intelligence Research (CIR) Branch*—responsible for resolving outstanding issues arising from the inquiry undertaken by Mr Cook.
  - *Agency Services (AS) Branch*—previously part of Corporate Support Division, continues to provide security assessments and other protective security advice to government agencies.

The establishment and staffing of the new division took much effort in 1995–96. Following its establishment, a new committee was formed to

coordinate cross-program security and counter intelligence approaches.

The new security committee is chaired by the head of SCI Division. The committee reports to senior management on security. It directs five working groups with the task of identifying security principles and practices applying to five key areas identified as central to ASIO's internal security. These are:

- security culture and awareness, and personnel security
- physical security
- operational security
- administrative security
- information technology security.

As a basis for strengthening ASIO's security culture, five 'precepts of security' have been identified (see Figure 2).

Figure 2: ASIO's precepts of security



### **Continuous improvement commitment**

A third imperative in our work during 1995–96 was corporate commitment to continuous improvement. A major staff attitudes survey (see page 23) was conducted in March 1996 to find out how well staff rated ASIO's management and performance, what they valued most about working in ASIO, and what they wanted to see improved. The results of the survey provided direction for further change during the next year, focusing particularly on leadership, management and communication issues.

---

### **Meeting corporate goals**

A matrix on pages 10 and 11 offers an at-a-glance view of ASIO's main issues and outcomes in 1995–96, set in the context of corporate goals and strategic directions. A small amount of material contained in the matrix is excluded from the unclassified *Report to Parliament*.

Subsequent chapters examine each goal area in more detail under the headings of clients, partners, technology, workforce, efficiency, and reputation. The Program Reports section (see page 35) covers the objectives, activities and outcomes of ASIO's five programs.

# Our focus at a glance

	Our clients	Our partners	Our technology
<b>GOALS</b>	<ul style="list-style-type: none"> <li>Anticipate and satisfy clients' needs for reliable and timely security intelligence and security advice</li> </ul>	<ul style="list-style-type: none"> <li>Have relationships with other agencies that maximise security intelligence benefits</li> </ul>	<ul style="list-style-type: none"> <li>Have the infrastructure and expertise that meet our needs and support those of our partners and clients</li> </ul>
<b>STRATEGIC DIRECTION</b>	<ul style="list-style-type: none"> <li>Identify and respond to clients and their needs</li> <li>Develop new and improved products</li> <li>Adopt a risk management approach in our activities</li> </ul>	<ul style="list-style-type: none"> <li>Establish consultative mechanisms</li> <li>Explore cooperation</li> <li>Pursue resource sharing</li> </ul>	<ul style="list-style-type: none"> <li>Continuously improve our technical collection capability</li> <li>Develop technology-based systems</li> <li>Establish effective counter intelligence and security practices</li> </ul>
<b>HIGHLIGHTS</b>	<ul style="list-style-type: none"> <li>Security intelligence clients surveyed</li> <li>Client list for reports extended</li> <li>Position dedicated to client liaison</li> <li>Improved coordination of threat assessment arrangements</li> <li>Study begun of economic espionage against Australian interests</li> <li>Growing external use of ASIO risk management model</li> </ul>	<ul style="list-style-type: none"> <li>ASIO officer seconded to US Olympics security planning team</li> <li>Participation in a range of international meetings</li> <li>Interagency language database progressed</li> <li>Improved communications capability in counter terrorism response situations</li> </ul>	<ul style="list-style-type: none"> <li>Participation in encryption policy discussions</li> <li>Computer workstations upgraded throughout ASIO</li> <li>Systems architecture being redeveloped; Windows NT pilot project begun</li> <li>Groundwork laid for improved information management system</li> </ul>



<b>Our workforce</b>	<b>Our efficiency</b>	<b>Our reputation</b>
<ul style="list-style-type: none"> <li>• Bring out the best in our people within a security intelligence culture through leadership and best management practices</li> </ul>	<ul style="list-style-type: none"> <li>• Continually achieve greater efficiencies in managing our resources</li> </ul>	<ul style="list-style-type: none"> <li>• Be recognised as responsible and effective</li> </ul>
<ul style="list-style-type: none"> <li>• Develop good workforce planning and employment practices</li> <li>• Foster a stimulating and satisfying work environment</li> <li>• Encourage a continuous improvement culture</li> <li>• Develop high levels of professionalism</li> </ul>	<ul style="list-style-type: none"> <li>• Establish an integrated evaluation framework</li> <li>• Provide appropriate computing and technical support</li> <li>• Provide incentives for workplace reforms that contribute to our productivity, efficiency and flexibility</li> </ul>	<ul style="list-style-type: none"> <li>• Explain our goals and capabilities</li> <li>• Satisfy all external accountability and reporting requirements</li> <li>• Develop and promote communication to help achieve positive outcomes</li> </ul>
<ul style="list-style-type: none"> <li>• 'Continuous improvement in ASIO' workplace bargaining agreement in place</li> <li>• Competency-based staffing systems introduced</li> <li>• Traineeship system for Generalist Intelligence Officer recruits showing good results</li> <li>• OH&amp;S case officer support strengthened</li> <li>• New EEO program ratified by Public Service Commissioner and published</li> <li>• Performance pay arrangements made more efficient</li> <li>• Staff attitudes survey conducted, and benchmarking relationships with other agencies developed</li> </ul>	<ul style="list-style-type: none"> <li>• Fraud control plan under development</li> <li>• Completed installation of secure overseas communications link resulting in productivity gains</li> <li>• 50 staff-initiated continuous improvement projects underway</li> <li>• Considerable efficiencies in recruitment processes from using Recruitment Services Australia to conduct initial screening and provide a pool of high-calibre applicants</li> <li>• A major sub-program evaluation completed</li> </ul>	<ul style="list-style-type: none"> <li>• Comment by IGIS on high standard of ASIO's warrant procedures</li> <li>• An appeal against a qualified security assessment from ASIO disallowed by AAT</li> <li>• 64 appealable staff promotions or transfers confirmed without call on internal or external appeal mechanisms</li> <li>• Explanatory brochure about ASIO published, and ASIO 1994–95 annual report judged best in its category by Institute of Public Administration Australia</li> </ul>



# Our clients

## Goal

**Anticipate and satisfy clients' needs for reliable and timely security intelligence and security advice**

ASIO's clients are mainly commonwealth agencies, statutory authorities, government business enterprises and state and local government authorities.

Broadly ASIO supplies these clients with:

- security intelligence reporting—on immediate and longer term risks to security
- threat assessments—estimates of the level of risk in specific situations to the safety of people and property (including overseas dignitaries, officials and premises) and other Australian interests
- security checking services—assessments of the security background of people applying to enter or remain in Australia or to be given access to classified material or secure premises
- protective security reviews and recommendations—on how agencies can best monitor their security risks and protect their assets, including people, premises and information
- intelligence-gathering support—using our technical expertise and special powers to gather intelligence in support of other agencies as part of Australia's strategic positioning and counter terrorism defences
- foreign intelligence gathered incidentally in the course of security intelligence investigations.

This chapter describes particular developments in improving services to clients in 1995–96. A small amount of material is excluded from the unclassified *Report to Parliament*.

## Seeking client input

Mechanisms for client input and comment on security intelligence reporting include:

- a consultative committee on security intelligence—created during the last reporting period to provide ASIO's clients with a forum to discuss their views on security intelligence reporting and priorities, and to coordinate their activities
- formal surveys of client needs
- client evaluation reports on individual assessments
- formal interviews with clients
- informal feedback arising from working relationships between our officers and their counterparts and contacts in client agencies.

Towards the end of 1995 ASIO commissioned a small survey designed to compare our view of client focus with that of the clients to whom we provide security intelligence reports. One aim was to find out how major clients rate our services and, in particular, our reports. The results showed there was room for improvement, particularly on a range of communication issues. Addressing these concerns is one of our continuous improvement objectives.

## Extending security intelligence reporting

During the past 12 months, we sought to strengthen the relevance of our reporting to clients.

Copies of security intelligence reports are now distributed to the regional offices of a range of commonwealth agencies. In addition, specialist security advisers in 45 client agencies have been added to the distribution list for our reports.

The program to develop a client database mentioned in last year's report was postponed because of competing priorities in the information technology area. However, we began a program of interviews with major clients aimed at eliciting their views on the harm that could be done to Australia's security by groups and foreign intelligence bodies of concern to ASIO. Clients were also asked to identify their information requirements, so as to help ASIO's analysts improve the content and presentation of product.

### **Improving security for commonwealth holders of high public office**

Security arrangements can only be based on an accurate and realistic picture of both the general threat environment and any specific threats to individuals or events. ASIO advises agencies involved in protective security on the likelihood of violence in specific situations. Our threat assessment advice helps agencies effectively allocate their preventive and protective resources.

During 1995 a team led by Mr Greg Wood, Deputy Secretary to the Department of the Prime Minister and Cabinet (PM&C), reviewed security arrangements for commonwealth holders of high office, including current and former governors-general and prime ministers, senior commonwealth ministers and senior opposition officeholders.

The review team examined ASIO's threat assessment function and also looked at

our work in providing physical security advice for commonwealth official establishments and ministerial residences. It recognised our central role in the threat assessment process and emphasised the need for us to give high priority to developments in officeholder security. Among the review team's recommended measures were:

- the establishment by ASIO and the Protective Services Co-ordination Centre of a system for checking ASIO assessments against incidents which actually occur—to help improve our predictive capability and evaluate our threat assessment product
- reaffirmation by the government of the requirement for commonwealth agencies to pass to ASIO all security-related intelligence.

The review has been endorsed by the government. Its recommendations underline ASIO's requirement to provide physical security advice relating to the commonwealth's official establishments and to the offices and residences of holders of high office.

### **Improving protection for foreign interests in Australia**

During the year ASIO took up representation on two new committees specifically concerned with ensuring protective security for local and foreign dignitaries and foreign interests in Australia (the Diplomat and Dignitary Security Subcommittee of SIDC–PAV, and the Visits Assessment Group).

ASIO's strategic planning approach, as endorsed by government in 1995, recommended that Australia's law enforcement agencies and ASIO should examine how they might better respond to potential security risks facing foreign



interests in Australia. In early 1995 the government examined arrangements for protecting visiting foreign dignitaries. As a result, improvements to protective security procedures and arrangements were implemented during the year. ASIO also worked with federal and state police agencies to improve the quality and timeliness of the threat assessment advice we give on visits by foreign dignitaries.

### **Passing on incidental foreign intelligence**

During the course of security investigations, ASIO may acquire information relating to foreign rather than security intelligence. In such cases our legislation allows us to pass intelligence to the relevant minister or department, or to another Australian intelligence agency. In 1995–96 ASIO issued 35 such foreign intelligence reports.

### **Identifying economic espionage**

At government's request, ASIO began a study in early 1996 to assess to what extent Australian scientific information and technology is being pursued through economic espionage by foreign governments. We know that some countries post agents to Australia with shopping lists of industrial, scientific and technical knowledge or hardware to assist their own industries. While a considerable amount of public material is available to them, their activities become of security concern if they engage in deception or cause Australia to be disadvantaged economically or in other ways.

ASIO has therefore been contacting industry groups, research centres and manufacturing firms, asking whether they know of or suspect attempts at espionage

aimed at their research or business interests. Their responses will help us assess the extent to which economic espionage by foreign governments is happening in Australia, which countries may be involved, and what sort of material and information they are seeking. A confidential report will be provided to government on the outcomes.

### **Helping clients with protective security advice**

ASIO prepares protective security plans for government agencies seeking advice on how to monitor their risks and protect their assets—including people, property and information. A security plan identifies assets, assesses risks and recommends cost-effective methods of protection. Our protective security advice to clients is underpinned by a risk management approach which recognises the role of clients in determining their own needs and influencing the service provided to them. In 1995–96 we supplied plans to 61 client agencies on a cost recovery basis.

### **Fostering the risk management approach**

Client feedback during the period confirmed that many agencies are now using a logic model developed by ASIO for assessing organisation security and other risk levels. We continue to work with the Commonwealth Management Advisory Board (MAB), and our 'Protective security risk management' was included as a case study in the publication *Guidelines for Managing Risk in the Australian Public Service* which was issued by MAB and the Management Improvement Advisory Committee (MIAC) in July 1995.

# Our partners

ASIO is one of a group of federal intelligence and security agencies, each with its own responsibilities yet with interests in common. It makes sense for us to pool resources and work together to avoid duplicating inputs and effort. We also work extensively with other government agencies, federal and state, including the various law enforcement agencies. We seek similarly cooperative relationships with all these partners, so as to give effective and timely advice on security matters.

ASIO is also part of a worldwide network of intelligence and security services with which we share knowledge so as to counter terrorism and efforts to proliferate nuclear, chemical and biological weapons.

Although the distinction between clients and partners is often blurred, this chapter deals with areas of specific cooperation, joint effort and liaison where partnership is the best description. Because of security sensitivity, about half the chapter is excluded from the unclassified *Report to Parliament*.

## Working with other Australian authorities

As well as building strong cooperative relationships with our partners in the Australian intelligence community, ASIO seeks to strengthen its links with other authorities. The keystone for these links with commonwealth agencies is the Consultative Committee on Security Intelligence. Formed only in May 1995,

this is its first full year of operation. During the review period the committee worked to improve the flow and focus of security intelligence advice, and to address strategic policy issues impacting on the security intelligence community.

Through its involvement in Australia's counter terrorist mechanisms, ASIO continued to engage with both federal and state authorities. Cooperation with the Protective Services Co-ordination Centre, the Australian Protective Service, Australian Federal Police and state police agencies allowed accurate and timely threat assessments to be communicated. This enabled appropriate responses to be arranged.

ASIO officers provided technical training to police units and contributed to other training courses conducted by police agencies and other organisations. Officers from some of our state collection offices regularly gave presentations to police groups on changes in the threat environment and counter terrorist readiness. Similar presentations were given to other courses, notably those for federal agency security advisers and the Defence Force.

Cooperation with Defence continued on a broad range of activities, notably with Defence Security Branch. The Department of Immigration and Multicultural Affairs remained a significant partner in relation to security regimes protecting Australia from the entry of potential terrorists, officers of hostile intelligence services and other

## Goal

**Have relationships with other agencies that maximise security intelligence benefits**



individuals of security significance. ASIO was also extensively involved in the continuing refinement of protective security arrangements for aviation interests in Australia, coordinated by the Department of Transport.

### **Liaison with overseas services**

ASIO is seeking to increase its understanding of potential sources of security harm in the South East Asia and Pacific region. Regional conferences examining common security problems enhance both ASIO's knowledge base and the wider Australian initiative for involvement in the region.

In February this year the Philippine government convened an international conference on counter terrorism with the aim of discussing ways in which international cooperation could be strengthened, notably against international terrorists who directly target countries or use host countries as springboards for staging terrorism elsewhere. Representatives of ASIO took part in proceedings.

Some of the more significant contributions from liaison with overseas services are reflected in the reported outcomes of the geographic subprograms of the Security Intelligence Program (excluded, along with much of this section, from the unclassified *Report to Parliament*).

A substantial amount of ASIO's information continued to come from liaison with approved foreign intelligence services. This liaison was conducted mainly through ASIO officers posted to a number of Australian missions overseas. During the year we completed the installation of a fast, secure computer

link between our offices in Australia and all the overseas posts, using the Department of Foreign Affairs and Trade (DFAT) Australian diplomatic communications network. This has greatly enhanced liaison effectiveness. We also had regular contact with representatives of liaising foreign services posted to Australia.

During 1995–96 the Attorney-General approved ASIO's liaison with a further 15 foreign authorities judged necessary or helpful to our work. This brought the total number of approved liaison authorities to 156 at 30 June 1996. These authorities belong to 76 countries, listed in Appendix A (excluded from the unclassified *Report to Parliament*).

We continued to explore new avenues for liaison through visits by ASIO officers to approved agencies and reciprocal visits to ASIO, with particular focus on specific security intelligence objectives and strategies. The policy of encouraging subject specialists to engage in face-to-face dialogue with their overseas counterparts has been particularly effective.

### **National language database**

An element of the national security intelligence strategy was the creation of a national language database to help federal agencies with an urgent need for translators and interpreters. During the year ASIO asked several agencies known to employ large numbers of linguists to prepare lists of their language resources. We will combine these with a list of our own resources and compile a central database to which other agencies can have access.

# Our technology

ASIO's capability rests in many elements, none more than its technological resources and expertise. Technology is important in the collection and processing of intelligence, and powerful technology-based information systems are needed to underpin analytical activity as well as the day-to-day management and communications of a modern organisation.

This chapter looks at recent developments in our technology environment, external and internal, during 1995–96. Because of security sensitivity, about half of this chapter is excluded from the unclassified *Report to Parliament*.

## Telecommunications technology

Rapid changes in telecommunications—technical and regulatory—bring benefits and drawbacks to national security. On the one hand, cheaper and more effective and secure communications speed up our responses to client demands and help our work. But those working against the national security interest enjoy the same advantages, improving the efficiency of their planning and activities and making investigation harder—a challenge to our work which we share with other authorities.

## Encryption

The need to protect complex electronic information systems worldwide has spurred the development of sophisticated

encryption technology. In common with the law enforcement agencies, ASIO expects encryption to become an essential feature of electronic commerce in the emerging global information infrastructure. ASIO is a member of an interdepartmental committee chaired by the Attorney-General's Department, which is preparing Australia's response to OECD draft cryptography policy guidelines and related requirements for an international policy on cryptography.

## Technology exchange liaison

Law enforcement and national security agencies all over the world are facing the common problem of declining resources in their intelligence collection activities. They are responding by accelerating a trend towards international cooperation, particularly in technical areas.

## Enhancing information technology systems

As foreshadowed last year, ASIO is nearing completion of an exercise to replace all lower level machines with 486 DX-2/66 or Pentium 100 personal computers and introduce a new internal electronic mail (e-mail) system. This constitutes most of the first phase of the OASYS (office automation systems) replacement project, funded by a resource agreement.

The ultimate goal of OASYS is to give ASIO's staff robust and flexible applications and seamless access to the data resources they need. We are

## Goal

***Have the infrastructure and technical expertise that meet our own needs and support those of our partners and clients***



adopting 'object oriented' technology to ensure system stability and to incorporate a range of security options within the systems architecture.

To build a suitable platform to support the new technology and associated applications, a Windows NT pilot project has begun. By mid-1997 all ASIO's workstations are expected to be running Windows NT, providing an industrial strength operating system.

Our information technology (IT) specialists also began working on the first two major application redevelopments using object oriented technology. A third is scheduled to begin mid-way through the next review period. The first significant benefits from the new technology are expected in 1996–97.

The upgrading of communications between our Australian offices and overseas liaison posts has been completed. All posts now have access to a fast, secure e-mail system, as well as desktop terminals providing the same standard of PC applications as they would have in Australia.

### **Managing and enhancing information access**

All agencies need regularly to review their information management strategies. The imperative is even greater for ASIO since our business is information—its collection, collation, storage, analysis and dissemination as intelligence to a variety of clients. To be of value, ASIO's information must be relevant, timely and presented well.

During the year work began to develop a modern, formal information management strategy. Its aim is to respond to the information revolution

and establish an approach that encompasses all aspects of ASIO's information, whether electronic or hard copy, produced in-house or externally, overt or covert in nature. By 30 June, a set of draft information security principles had been produced, and the development of an information model was in progress.

The strategy will be used by the major information provider areas to identify priorities and determine resource requirements over the next five years. It will constitute a framework for future decisions on information management. We want it to support a flexible and adaptive way of doing business and help us move our information systems into the future in a consistent and logical way.

ASIO's information holdings include a library containing material on intelligence, security and related issues in Australia and overseas, much of which can be made available through the Australian Bibliographic Network. During the year new library management software was introduced which will allow for integration of serials, invoicing and a range of other functions. The library also utilises the expanding range of available electronic sources of information.

A review began in 1995–96 of our system of monitoring and accessing policy and procedures documents. The existing system—the ASIO Procedures Manual—is unwieldy to produce and access, and difficult to maintain. One of the terms of reference of the review was to explore the feasibility of placing essential corporate documentation on-line as soon as is consistent with overall IT planning and other information management priorities.



# Our workforce

ASIO's workforce comprises two main streams:

- Generalist Intelligence Officers (GIOs) with training and experience in collecting and analysing intelligence and preparing assessments and security advice. They are employed in program areas where their professional intelligence skills are necessary to achieve the Organization's central objectives.
- Specialist Intelligence Officers (SIOs) with qualifications or experience in a wide range of professional, technical, managerial and administrative fields. SIOs provide support across all program areas, underpinning ASIO's main security intelligence business.

Our staff are employed under the ASIO Act rather than the Public Service Act, through contract arrangements between the Director-General and each officer. However, in general, the terms and conditions of employment in ASIO are similar to those applying in the Australian Public Service (APS).

This chapter describes progress towards the important goal of bringing out the best in ASIO's people through a range of strategies, including the strengthening of workforce planning and employment practices, embedding a competency-linked staffing system, and giving all staff professional development opportunities. No material in this chapter is excluded from the unclassified *Report to Parliament*. Staffing statistics and other details of staff management practices are contained in Appendix B.

## Shaping the workforce

ASIO's Computerised Human Resource Information System (CHRIS) was enhanced during the review period to provide a greater range of staffing information and to aid recruitment planning.

During 1995–96 ASIO recruited more than 60 new officers. Twenty-six of these were GIOs, 11 were base grade clerical staff, and the rest were specialist officers mainly in the technical and information technology areas. Recruiting skilled specialist officers continues to be a challenge, since they are highly sought-after by other employers who generally do not require applicants to go through the lengthy security checking procedures that are mandatory for ASIO staff. We now plan to recruit one intake of up to ten GIO trainees annually, aligning this with the APS graduate entry program.

The amount spent on press recruitment advertising in 1995–96 was \$44 324, compared with \$125 083 last year. The advertising was placed through Neville Jeffress Sydney Pty Ltd.

## Using competencies

The ASIO competency project, an essential strand of our workforce planning strategy, was set up two years ago as a major initiative to help develop a multi-skilled, more flexible workforce with clear job objectives. A small project team and steering committee worked on developing competencies, work level

## Goal

***Bring out the best in our people within a security intelligence culture through leadership and best management practices***



standards and a job evaluation method to produce a coherent, comprehensive package of human resource management tools and data for use in organisational planning and decision making.

The competency-based approach is now embedded in:

- intelligence and operations training courses—including GIO traineeships
- leadership and management development courses
- profiles used to fine-tune and streamline staff selection processes and outcomes
- instruments, methods and profiles used in psychological assessment for various purposes
- selection criteria used for internal promotion and transfer purposes.

The job evaluation methodology was developed using an external consultant working with an advisory group which had representatives drawn from ASIO's Staff Association and all divisions. In the course of its development, several issues to do with staffing structure and job classification were identified as needing resolution during the next review period.

### **Providing development opportunities**

During the year two senior officers returned from successful participation in the Executive Development Scheme and the Senior Women in Management program conducted by the Public Service and Merit Protection Commission. No officers were nominated for these programs in 1995–96 because of redistribution of the development budget, but one officer will be nominated in 1996–97.

ASIO's leadership strategy continued in 1995–96 with a range of activities for all levels of management, including team leaders. Senior managers participated in a Leadership and Business Planning workshop to set directions for the year and improve cross-program working relationships. They later attended a seminar on the leadership findings of the Karpin Report led by Mr Peter Ivanoff, a member of the Karpin Task Force.

Team development initiatives continued to reassess and improve the ways ASIO does business. To complement this a Line Management program was provided for team leaders. This was a successful four month action learning program conducted on a part-time basis with all participants undertaking significant organisational improvement projects.

To provide an opportunity for officers to experience networks and learning programs external to the Organization, a significant investment was made in the Public Sector Management Course. Ten officers continued their studies towards a graduate certificate and a further nine have enrolled for the 1996–97 programs. This initiative is also available to line managers in ASIO's state-based collection offices.

Many of ASIO's officers, both generalists and specialists, seek professional development by taking part in external courses. Through a scholarship scheme, some officers are engaged in undergraduate and postgraduate studies bearing on their professional interests. Technical specialists similarly upgrade their knowledge of new technologies and techniques through external training courses. During the review period officers also attended courses conducted by bodies such as the Department of Defence, the National Crime Authority

and state police agencies. The courses are particularly valuable not only in enabling our officers to develop contact networks but also in conveying a better understanding of our role in the wider intelligence and security network.

Developing professionalism in our GIOs continued to be a high priority. Twenty-six new recruits entered into traineeships during 1995–96. The traineeship program lasts 12 months and includes modules on analytical and intelligence collection techniques. Supervised work experience is another key element. Evidence of the success of the program (introduced in the previous year) came this year when the first group of 17 trainee graduates took up postings in various analysis and collection areas and demonstrated a well-rounded understanding of work requirements.

Reflecting their importance to the Organization, ethics and accountability are treated in depth in a course offered to officers at all levels. The program makes use of external presenters (from review bodies such as the Public Service and Merit Protection Commission, and the offices of the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security) to complement the internal view of ASIO's obligations to government, parliament and the community. Three such courses were conducted during 1995–96, with about 15 participants on each.

A new program developed this year will provide support for non-managerial staff in the front line of client service. The 'FrontLine Network' will be supported by a series of short modular learning programs, with the first due to be delivered at the outset of 1996–97.

## **Fostering industrial democracy**

Consultation and negotiation between ASIO's staff and management on employment matters are conducted through the ASIO Consultative Council (ACC). The ACC provides a forum in which management and representatives of ASIO's Staff Association can discuss terms and conditions of service and recommend changes, if required, to the Director-General. To give effect to such a change the Director-General issues a determination in accordance with sections 85 and 86 of the ASIO Act.

Issues coming before the ACC may be explored through several subcommittees dealing with matters such as productivity, occupational health and safety and equal employment opportunity.

During the year issues brought to the ACC included:

- negotiations on ASIO's second and third productivity agreements signed in September 1995 and January 1996 respectively (see page 26)
- selection criteria for sensitive security-related positions
- requirements for disclosure of employment details by ASIO staff applying for personal insurance cover.

## **Managing health and safety**

Changes were made to occupational health and safety (OH&S) management arrangements so as to align preventive and educational aspects more closely with the handling of rehabilitation and compensation cases. Communication networks are well established. OH&S newsletters, magazines, articles in the staff bulletin and a dedicated Health



Week have increased general health and safety awareness, as have periodic safety 'walk-arounds' by OH&S workplace representatives.

Twelve case managers were trained during the year, bringing the total number to 20. Case managers support officers suffering from injury or stress-related disorders and assist their eventual return to work. Early intervention in stress cases is also an aim, to prevent distress becoming incapacitating. Following a review, the team of volunteer OH&S representatives now better reflects ASIO's various designated workgroups.

Work proceeded on revising ASIO's OH&S Agreement with a view to completion in November 1996. In this context, the relevant subcommittee of the ACC began examining the implications and effects of section 6 of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*—which states that the Director-General of Security can declare that certain provisions of the Act do not apply to ASIO (or apply subject to modification). This examination is in recognition of the need to promote occupational health and safety to the greatest extent consistent with the exigencies of necessary security operations.

A table showing the incidence of reportable accidents in ASIO in this and previous years is included in Appendix B.

### **Providing equal employment opportunity**

The manager of ASIO's Corporate Support Division is responsible for

ensuring that equal employment opportunity (EEO) is firmly woven into the fabric of the ASIO workplace. She is supported in this by a subcommittee of the ASIO Consultative Committee.

During the year a new EEO program for ASIO was published. *Equal Employment Opportunity in ASIO, a Strategic Plan for 1996 to 2000* is based on the new model approach developed by the Public Service and Merit Protection Commission, incorporates ideas from staff at all levels, and identifies key change areas for attention. The new program was ratified by the Public Service Commissioner in May 1996.

No EEO-related grievances were reported during 1995–96. Tables in Appendix C show the representation of designated groups within ASIO's occupational groups and the overall percentage against total staff numbers.

### **Managing performance**

During the year changes were introduced to efficiency bonus and performance pay arrangements for ASIO's senior and SES-equivalent officers. As part of ASIO's third productivity agreement, senior officers' efficiency bonus payments were rolled into base salary. This change took effect from 11 January 1996 and a total of \$244 677 was paid under the old arrangements for the period 1 May 1995 to 11 January 1996. For SES-equivalent officers, performance pay will now be payable only to officers whose performance is assessed as 'superior' or 'outstanding'. The SES performance pay period (1 July 1995–11 January 1996) was finalised during the reporting period with payments totalling \$39 100. Further details of payments are contained in Appendix B.

At the end of the period, new performance appraisal arrangements linked to competencies and personal development plans were being developed for officers at all levels.

### **Benchmarking for continuous improvement**

In March 1996 ASIO staff were invited to take part in a survey of staff attitudes designed to quantify their views on ASIO's performance against such factors as leadership, client focus, products and services, communication and people management. The survey was conducted by a consultancy firm under the auspices of the Australian Quality Council (AQC) Survey and Benchmarking Program. The ASIO Continuous Improvement Survey (ACIS) is a continuing initiative which

allows us to measure our management skills and performance against other public and private sector organisations and share approaches to improvement with other participating firms and agencies.

The results of the survey were released to management and staff in May 1996 and were followed by feedback sessions at which staff were encouraged to articulate problems more specifically and—more importantly—suggest ways of improving performance in areas that concerned them. The steering committee and working group formed to manage the initial survey will be involved in follow-up activity and in continuing our participation in the AQC program. The survey will be repeated at regular intervals to measure progress.



# Our efficiency

## **Goal**

**Continually  
achieve  
greater  
efficiencies  
in managing  
our  
resources**

Efficiencies are sought in all program areas through an integrated evaluation framework aimed at achieving better resource allocation. Developments in our computing systems also underpin efficiency as do technical advances relating to the collection of intelligence. As described on page 26, ASIO's Continuous Improvement Program, which is the basis of our third enterprise agreement with government, gave rise to a wide range of initiatives, many aimed at producing workplace dividends. This chapter deals with progress across these and other fronts where efficiency outcomes are the focus. A small amount of material is excluded from the unclassified *Report to Parliament*.

## **Evaluating programs**

ASIO continued to maintain close liaison with the Evaluation and Supply areas of the Department of Finance (DoF). The department provides continuing guidance on how evaluation can best contribute to reshaping ASIO's activities to meet the needs of government and other clients in a changing security and policy environment.

Early in the year, DoF officers gave an in-house presentation to ASIO's managers on the place of evaluation in the broader financial management improvement framework. Other topics included evaluation methodologies and the work being done on a way to evaluate policy advice. More than 40 ASIO officers have now attended DoF's

evaluation workshops, including all those involved in current or planned evaluations.

ASIO's four-year evaluation schedule examines components of the five reporting programs and associated subprograms, as well as corporate support functions which are attributed across programs. Evaluation results are built into ASIO's broader resource planning.

ASIO's Audit and Evaluation Committee, in introducing improvements flowing from the evaluations, continued to stress recommendations seen as contributing to collection, analytical and technical improvements across the broadest range of ASIO's programs.

By including external participants on evaluation steering committees and teams we continue to promote benchmarking and continuous improvement.

Greater detail on evaluation is contained in Appendix D (with some material excluded from the unclassified *Report to Parliament*).

## **Managing fraud control**

Government has identified fraud against the Commonwealth of Australia as a priority issue that departments and agencies must combat by an active role in fraud control management as well as in prevention and detection. In response, ASIO's Audit and Evaluation Committee last year established a working group to develop a fraud control policy for the

Organization. The policy will be embodied in a plan setting out corporate responsibilities, the nature of fraud risk assessments, measures for education and training, and procedures for fraud reporting and investigation.

The group worked with the Commonwealth Law Enforcement Board, the Australian Federal Police and the Department of Defence to develop a fraud risk assessment strategy suitable for a small agency. Much of the group's attention centred on the relationships between fraud control and ASIO's security and counter intelligence arrangements. Key issues included determining the non-legislative definition of fraud to be used in framing the policy (being careful to distinguish fraud from espionage and other acts with significant security consequences).

In developing the plan the group took account of fraud controls already built into ASIO's administrative practices and training programs. Our ethics and accountability training course, for instance, includes the analysis of issues directly relevant to fraud control. New graduate entrants are introduced to the responsibilities of handling public moneys in the first days of their traineeship, to emphasise the importance of the issues involved.

By the end of June the direction and key elements of the proposed fraud control framework had been endorsed. The plan will be published early in the new reporting period.

### **Efficiencies in computing**

Maintaining a large computing network is expensive. ASIO's strategy has been to minimise variety while ensuring

competition in purchasing. Through standardisation and by limiting the number of desktop packages, the cost of training for specialised IT staff and their internal clients has been kept down. During 1995–96 progress was made in reducing the variety of programming languages, with the promise of significantly better efficiency in the future. Apart from a welcome reduction in the complexity of the systems, the adoption of a single set of standard tools for IT development makes for more consistent design and interfaces which in turn provide greater flexibility in making use of applications. And as earlier systems are phased out, there will be a corresponding reduction in maintenance costs and licence fees.

### **Increasing global monitoring**

ASIO is exploring more efficient ways to access the growing volume of public information relevant to its responsibilities and to discriminate between the many sources available. We are cooperating with other Australian intelligence and law enforcement agencies so that our open source information systems are coordinated and complementary. In May 1996, ASIO participated in a seminar on this subject sponsored by the Office of Strategic Crime Assessments.

The monitoring of public information has two elements. We need to be aware of breaking news in case it could lead to incidents, events and developments likely to affect Australia's security. We also need to stay abreast of subjects judged to pose low-level threat, in case there are signs that judgment should be reviewed. Together, these two elements affect the allocation of resources to subjects of investigation. Open source



information can be used to identify and monitor patterns and trends suggesting an escalation of activity prejudicial to security, and so assist the more appropriate use of intrusive investigative methods. Moreover, wide access to publicly available material is essential to longer-term security forecasting and forward planning, by helping identify trends in the broader security environment that bear on Australia.

### **Efficiencies from workplace bargaining**

Two productivity agreements were signed during the review period. The 'Second ASIO Productivity Agreement', ratified in September 1995, was an interim document mainly addressing priority issues arising from the first agreement and introducing a change in senior officer performance appraisal and management procedures.

Our third productivity agreement was signed by the Director-General and the President of ASIO's Staff Association in January 1996. It will remain in force until March 1997. The agreement, 'Continuous Improvement in ASIO', sets out to embed the continuous improvement process and align ASIO's products more closely with client needs. Its overall objectives are 'making ASIO work better' (that is, finding ways to improve the relevance, productivity and efficiency of what we do for clients) and 'making ASIO a better place to work' (that is, improving the work environment for staff). In exchange for a commitment by staff to negotiate initiatives to improve ASIO's productivity and efficiency, the

third agreement delivered a salary increase of 3.7% in January 1996, with a further increase of 1.7% to follow in July 1996.



Underpinning the agreement is a continuous improvement program of around 50 separate initiatives for implementation within the life of the agreement and beyond. Major projects include:

- introducing a staff attitudes survey and benchmarking process (see page 23)
- an automated job evaluation methodology to improve job design
- 'best practice' implementation in internal protective security arrangements
- a review to streamline the delivery of threat assessments to clients.

### **Efficiencies in recruitment**

A significant efficiency was achieved in 1995–96 by aligning our GIO trainee recruitment process with the APS



Graduate Administrative Assistant recruitment campaign conducted by the government agency Recruitment Services Australia (RSA). In 1994–95 ASIO advertised traineeships independently and received over 5000 applications, all of which required screening. In 1995–96, ASIO again advertised traineeships but required applicants to achieve a qualifying score from RSA before

---

submitting their applications. This resulted in 1000 applications, all of high quality. The consequent saving in screening is approximately equal to half the workload of a full-time officer. Similar savings are estimated to have flowed from using RSA to provide screened applicants for base-grade clerical positions.



# Our reputation

**Goal**  
**Be**  
**recognised**  
**as responsible and**  
**effective**

In pursuing a reputation for integrity as well as performance, ASIO looks beyond the matter of public image. As is the case with any investigative agency, the nature of our work places limits on what can be publicly said about much of our activity. So it is inevitable that where we must be reticent, myth and rumour grow to fill an apparent void.

Yet the void is illusory. ASIO is answerable to government, the parliament and the community through a raft of accountability mechanisms designed to ensure oversight while maintaining necessary levels of confidentiality and security. ASIO welcomes this scrutiny as a way of demonstrating its core values of professionalism, integrity, avoidance of bias and respect for freedom of opinion and civil liberties. These values are impressed on our officers during training and throughout their working life in ASIO.

This chapter looks at the working of the accountability mechanisms that apply to ASIO, the outcome of which is our reputation. There is also an account of recent initiatives aimed at giving the public a broad-brush sketch of our role and activities. A small amount of material is excluded from the unclassified *Report to Parliament*.

## Reporting to government and the parliament

ASIO's primary avenue of accountability to government and the parliament is through the Minister, the Attorney-General, who is briefed on matters of security concern. The Attorney-General is a member of the National Security Committee of Cabinet which is supported by the Secretaries Committee on National Security, a group of senior officials charged with policy direction and oversight of the work of the Australian intelligence and security agencies. These are the primary readers of ASIO's classified *Annual Report*, which each year reviews security issues, programs and outcomes in detail. A copy of the report is made available to the Leader of the Opposition, who also receives security briefings from the Director-General.

As a subprogram within the Attorney-General's portfolio, ASIO's programs are set out in the Portfolio Budget Statement and therefore undergo the same scrutiny as any other federal agency, in our case by the Senate's Legislation Committee on Legal and Constitutional Affairs. Like all other heads of federal agencies, the Director-General appears before the committee at its budget estimates and additional estimates hearings.

## **The Inspector-General of Intelligence and Security**

The Inspector-General of Intelligence and Security (IGIS) assists ministers in the oversight of Australia's intelligence and security agencies. The current IGIS, appointed in April 1995, is Mr Ron McLeod, AM. Some of his key tasks are to check that ASIO acts legally and with propriety, complies with ministerial guidelines and directives, and has due regard to human rights and civil liberties. He may inquire into complaints against ASIO from the public, or into matters referred to him by the Attorney-General, or into other matters at his own discretion. The IGIS reports separately to the parliament (see 'Tabled reports concerning ASIO', page 30).

### **Providing a case for warrants**

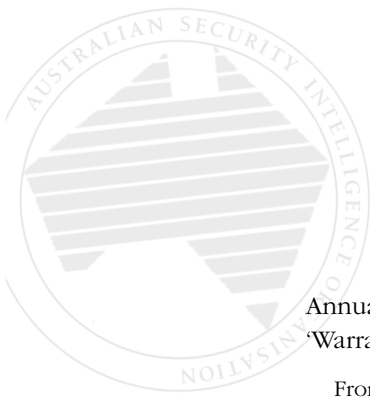
Although ASIO derives much intelligence by overt means (from interviews and publicly available material), other information can only come from using techniques which intrude on the privacy of individuals. Special powers under the ASIO Act allow the Organization to use such techniques as intercepting telecommunications, using listening devices, inspecting and copying postal articles, and entering and searching premises. These powers are given to ASIO because individuals or groups that are of concern to security generally operate in a clandestine manner or in ways deliberately designed to hide their real purpose. These powers, however, can only be used when the Attorney-General is satisfied their use is justified by the severity of harm that might be done by the person or group to be investigated.

The Attorney-General authorises the use of special powers by signing a warrant. ASIO's procedures for requesting warrants constitute in themselves an effective oversight mechanism. Only the Director-General can seek a warrant, and the request must be accompanied by a written supporting statement of facts and grounds showing that the projected intrusion on privacy is justified by serious security considerations. Warrants are issued for limited periods only, at the end of which ASIO must report on the extent to which the use of the special powers helped in collecting security intelligence.

Table 1 (excluded from the unclassified *Report to Parliament*) shows the number of people or premises against which warrants were issued in the reporting period compared with previous years. There may be multiple warrants in operation against any particular subject of investigation. During the course of a year, warrants against some subjects may be renewed.

In June 1995, minor changes were made to the wording used in warrant requests. The Solicitor-General's recommendation—that a senior official of the Attorney-General's Department should read each warrant request, to provide independent advice on whether it contained sufficient information for the Minister to be satisfied he could properly issue the warrant—was incorporated into the documentation.

During the year the IGIS continued the practice of carrying out spot check inspections of ASIO's warrant processes and operations. The following comment was published in the IGIS's 1994–95



Annual Report under the heading 'Warrant Operations' (paragraph 58):

From the monitoring done by my predecessor, and from my own observations, I can report that ASIO has maintained the high standards of past years in the care it has exercised in having proper authority for the intrusive activities it conducts.

### Tabled reports concerning ASIO

Three reports containing comments on ASIO were tabled during 1995–96:

- ASIO's own *Report to Parliament 1994–95*, tabled in the House of Representatives and in the Senate on 24 October 1995.
- *Audit Report No 13 of 1994–95 (Financial Statements Audit – Results of the 1994–95 Financial Statements Audits of Commonwealth Entities)*, was tabled by the Auditor-General on 30 November 1995. As in previous years, this recorded a qualification on the audit of ASIO financial statements for 1994–95. The qualification arises from the exemption from external audit of some items of ASIO's expenditure associated with sensitive intelligence collection activities. These outgoings are recorded in accounts exempted from audit by the Auditor-General under subsection 70D(1) of the *Audit Act 1901*. As a result, the Australian National Audit Office was 'unable to form an opinion on receipts to and expenditure from these exempt accounts and on assets and liabilities related to those exempt accounts'. The audit report on the 1994–95 financial statements was qualified accordingly.
- *Inspector-General of Intelligence and Security Annual Report 1994–95* (see page 29).

### The Parliamentary Joint Committee on ASIO

Our activities may receive further scrutiny from the Parliamentary Joint Committee (PJC) on ASIO. The PJC reviews aspects of activities referred by the Attorney-General or the parliament (but may not inquire into individual complaints or matters that are operationally sensitive, relating to foreign intelligence, or not affecting Australian citizens or permanent residents). A new PJC was formed after the March elections comprising:

Senator David MacGibbon (Qld, Lib)—Chair

Senator John Alexander (Sandy MacDonald (NSW, NP)

Senator the Hon. Robert Ray (Vic, ALP)

Mr Noel Hicks, MP (Riverina, NP)

Mr Robert (Bob) Sercombe, MP (Maribyrnong, ALP)

Mr Alexander Somlyay, MP (Fairfax, Lib)

Mr Paul Zammit, MP (Lowe, Lib).

### Public appeal mechanisms

Appeals against the issue of adverse or qualified security assessments by ASIO (see page 43) may be taken to the Security Division of the Administrative Appeals Tribunal (AAT). The tribunal can hear evidence from the appellant, from ASIO and from the commonwealth agency that requested the assessment as part of its security checking process. The decision of the tribunal either confirms or supersedes the original assessment and the requesting agency must then decide whether or not to issue the security clearance.

The AAT may also hear appeals against decisions made by Australian Archives, on the advice of ASIO, to exempt material from release under the *Archives Act 1983*. The grounds for exemption are usually that disclosure could reasonably be expected to cause damage to the security, defence or international relations of the commonwealth, or that it would disclose the existence or identity of a confidential source. During 1995–96 three appeals were lodged, one of which was withdrawn at the preliminary hearing stage. The other two had not been heard at the end of the reporting year. Further information on access to ASIO's records is contained in Appendix E.

### **ASIO's staff appeal mechanisms**

Mr Stuart Magee, a former member of the APS Merit Protection and Review Commission chairs ASIO's Promotion and Transfer Appeal Committee. During the year a total of 64 appealable promotions or transfers were made. No appeals were lodged.

Mr Norman Attwood, AO, formerly Deputy Secretary to the Department of Defence and a current member of the AAT, chairs ASIO's Grievance Review Committee (GRC). During the year no grievances were submitted to the committee for review. Five staff grievances were dealt with under internal procedures, which are the primary means of dealing with grievances. (The GRC is designed as a secondary process in cases when a grievance cannot be resolved through established internal procedures.)

Mr John Dainer, AM, RFD, Special Magistrate of the ACT Magistrates Court, chairs ASIO's Disciplinary Appeal Board. During the year no appeals were lodged with the board.

### **Internal ombudsman**

The office of ASIO Ombudsman is an internal position, filled by an SES or senior officer who accepts the role in addition to his or her substantive position. The role of the Ombudsman is to act as a first stop for staff wishing to discuss problems or difficulties they may be having in the work environment, in a way that allows matters to be raised informally rather than through the more structured grievance and external review processes. While only a few cases were dealt with during the period under review, all the problems raised were resolved. Apparently the trend among staff is to use the Ombudsman as a sounding board in trying to resolve situations themselves—for instance, by discussing with the Ombudsman whether their concerns are reasonable. A new Ombudsman was appointed towards the end of the year and will serve for the next twelve months.

### **Communicating with the community**

The mystique inevitably surrounding the work of an agency such as ASIO means the role it plays in contributing to Australia's security may be neither obvious nor meaningful to the public. Misconceptions and misunderstandings are common; but, unlike most other agencies, we are generally unable to comment or explain.



Although ASIO can never publicly discuss specific security-related matters, we have in recent years sought to explain the general value of our work so as to help dispel misconceptions. In April 1996 a new booklet entitled *ASIO Now* was published for public and client liaison purposes. The booklet sets out our role and general activities in clear and non-bureaucratic terms. It is a concise plain English document that can be given to people applying for jobs and

anyone else with an interest in ASIO. This expanded a range of brief information leaflets already available.

ASIO's efforts to communicate publicly were recognised by the Institute of Public Administration Australia in their annual report awards. The adjudicators placed ASIO's 1994–95 *Report to Parliament* first in the category of commonwealth statutory authorities reporting on similar lines to departments of state. The judges report said 'the annual report is one of ASIO's only public documents, and as such the judges found it refreshing to observe the positive approach to public accountability which came through in this report'.

Another initiative, aimed jointly at attracting potential GIO trainees and publicising the role of ASIO to young people, was our participation for the first time in the Australian Public Service Graduate Career Fairs held in Brisbane, Adelaide and Melbourne. More than 2000 people showed interest and were given literature on careers in ASIO, which at the same time may have increased their understanding of our role in Australia's security.

Communicating about ASIO is also part of the job of several managers, particularly those working in collection offices in state capitals, where there is a particular need to build networks with counterparts and contacts in other federal and state agencies, the private sector and the community in general.

During the review period, members of ASIO's senior management team spoke to Defence-sponsored conferences and workshops, and to non-government organisations, including the Australian



Institute of International Affairs. Other officers attended conferences where talking about ASIO and listening to others speak about their agency responsibilities helps to integrate our national security agenda with other aspects of the national interest.

---



*ASIO participated for the first time this year in the APS Graduate Career Fairs.*





# Program Reports

*Nature holds no brief for the human  
experiment; it must stand or fall by its results.*

---

GEORGE BERNARD SHAW, 1921



# Our program framework

ASIO is a subprogram (6.8) of the Attorney-General's portfolio program structure. Our internal program framework is shown in Figure 3. A summary of program outcomes (excluded from the unclassified *Report to Parliament*) is included on page 38. Program expenditure in 1995–96 is shown in Appendix F (excluded from the unclassified *Report to Parliament*).

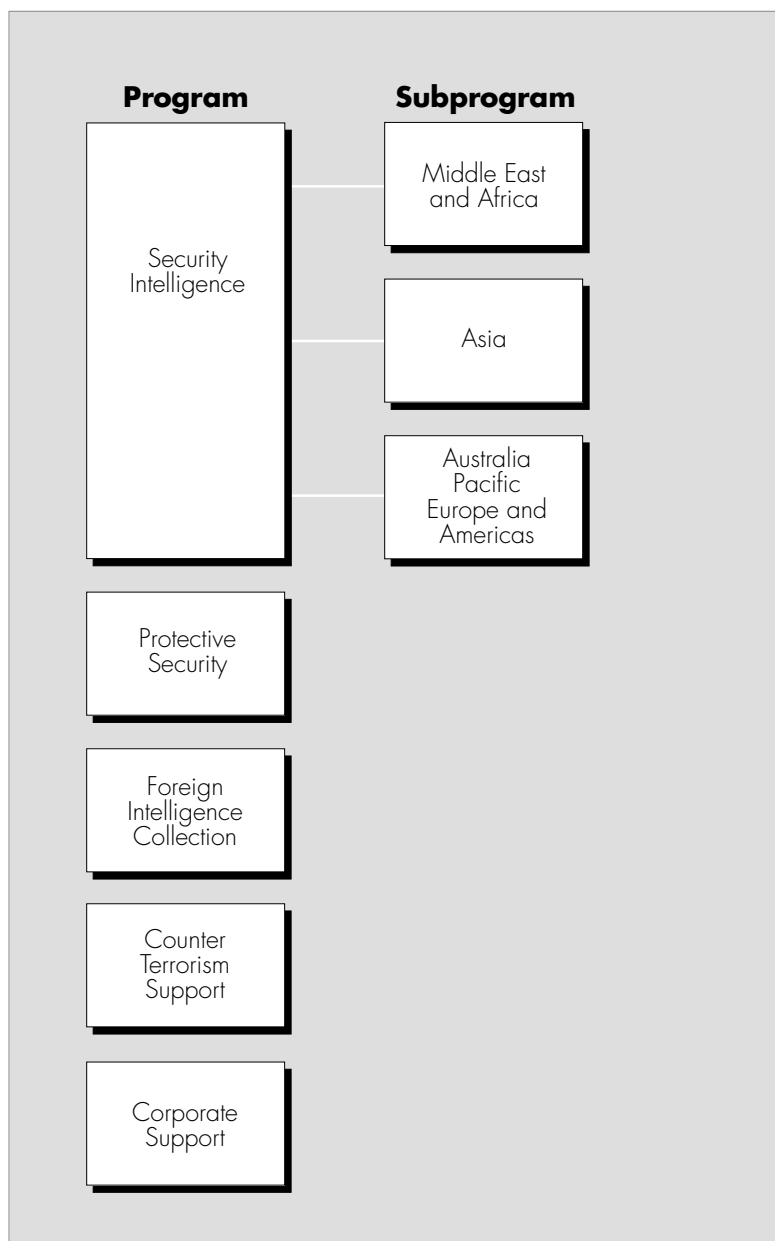
The *Security Intelligence Program* encompasses our main business of collecting and analysing security-related intelligence and advising government through three geographic subprograms:

- Middle East and Africa (MEA)
- Asia
- Australia, Pacific, Europe and Americas (APEA).

Three smaller programs (*Protective Security*, *Foreign Intelligence Collection* and *Counter Terrorism Support*) are also intelligence based, but are defined and reported on separately because they provide services in support of the programs of other departments and agencies.

The fifth program, *Corporate Support*, covers executive support, corporate planning, corporate communication and foreign liaison. The costs of other corporate activities, including the management of our internal security, are attributed across all programs and are not detailed within this program.

Figure 3: ASIO's program framework





# Summary of program outcomes

The following table summarising program outcomes is classified 'secret' and is excluded from the unclassified *Report to Parliament*.

# Security Intelligence Program

The Security Intelligence Program coordinates ASIO's contribution to the assessment and collection of security intelligence. Its role is to forewarn ministers and government agencies of activities and events which may endanger Australia, its people and its interests.

## Investigating security risks

ASIO's advice to government and its agencies derives from the analysis of security intelligence, collected from a variety of sources. Background information comes from publicly available channels such as news services and publications. Much intelligence reaches us through liaison contacts in an extensive network of overseas intelligence and security services and authorities. More specific intelligence comes from investigating people or groups (known as 'subjects') suspected of posing threats to security in Australia.

Investigation methods range from interviewing people who may know something about a subject, or talking direct to the subject about their activities, to mounting covert operations using ASIO's special powers (see page 29).

Investigations are normally conducted at one of three levels of intensity, depending on the level of assessed risk attached to the subject:

- *Level 1* relies primarily on examining existing intelligence and public information; its aim is to identify and locate higher probability sources of

harm (risk groups) using the most readily available and least intrusive sources of information.

- *Level 2* investigates the higher probability subjects by using methods likely to be more intrusive and resource intensive, with the aim of confirming or denying the 'high risk' assessment.
- *Level 3* investigates identified high risk subjects, using all necessary legal means.

## Providing advice on security

ASIO's advice to government and its agencies is generally of three kinds:

- *event reporting*—tactical intelligence to assist immediate management of imminent security risks
- *security risk reporting*—considered assessments of the risk posed by potential sources of harm, often in a specific context
- *environment appreciations*—developed from analysis of longer-term trends.

For more information on ASIO's clients, see page 12.

ASIO conveys much of its advice to government through a series of formal published reports prepared by analysts. These include:

- *ASIO's Fortnightly Digest*, which keeps government up to date on security issues.



- *ASIO's Report to SIDC-PAV*, containing detailed current intelligence on politically motivated violence and related concerns and produced every fortnight for commonwealth and state agencies concerned with protective security.
- *ASIO's Security Intelligence Report*, dealing with security risks and environment appreciations. This publication discusses security intelligence issues, assessing their implications for Australia and Australian interests. Sixty of these reports were produced in 1995–96, based on a wide range of material obtained from all sources available to ASIO.
- *ASIO's Incidental Foreign Intelligence Report*, generally containing information provided direct to ASIO by the services of other countries. Occasionally the reports are used as a reporting medium for foreign intelligence collected within Australia during the course of a security investigation. In all, 35 were published during the year.

We also occasionally publish an *ASIO Special Issues Report* as a means of passing Australian government information to cooperating overseas services, usually to fulfil a stated requirement. Three such reports were issued in 1995–96.

As well as the range of published reports ASIO provides a threat assessment service, issuing immediate advice to police forces and other agencies involved in protective security. Threat assessments advise on the likelihood of politically motivated violence occurring in specific situations.

## Managing program resources

ASIO uses risk management principles to decide which people or groups are priority subjects for investigation, and to apply scarce resources where they will count the most. Subjects are assessed according to the level of threat they pose (*how likely are they to cause harm?*) and the level of harm that might result (*how much damage could they do?*), and are ranked accordingly. Generally rankings indicate priorities, although there is a need to balance the shorter term acute risks against those posing a longer term, more chronic threat to security.

The ranking of subjects is continuously monitored and undergoes a rigorous moderation process. The security risk each subject is assessed as constituting determines the level of resources assigned to combatting it. Collection and analytical resources are managed through the three geographic subprograms.

Working within the geographic framework, analysts collate and process the intelligence that collection officers have gathered to produce reports and assessments for client agencies, many of which use a similar geographic approach.

The program encompasses two other major functions: a counter proliferation effort in support of Australia's international commitment against nuclear, chemical and biological weapons; and the threat assessment service to agencies with protective security responsibilities (see page 41). These functions cross geographic subprogram boundaries and their costs are attributed accordingly.

Security Intelligence Program expenditure in 1995–96 is shown in Table 2 (excluded from the unclassified *Report to Parliament*).

## Program focus in 1995–96

The following subprogram reports (excluded from the unclassified *Report to Parliament*), and reports on counter proliferation and threat assessment activities, give details of investigative outcomes during the year.

## Counter proliferation and technology procurement

ASIO has introduced an industry awareness program to alert researchers and manufacturers to the interests of proliferators and their agents. The program began with a small number of government and commercial organisations thought to be at high risk. The response from those approached was encouraging and the program will continue during the next reporting period.

## Threat assessments

ASIO provides government agencies with assessments of the likelihood of politically motivated violence arising from specific situations or events.

As well as advice on day-to-day events, we provided longer term assessments on:

- Australian dignitaries in this country and overseas
- foreign dignitaries visiting Australia
- threats to foreign interests in Australia
- the overall threat from politically motivated violence (two comprehensive biannual assessments for SAC-PAV)
- threats to aviation interests (two biannual assessments, principally for the Department of Transport)
- threats to commonwealth government buildings (for example, Defence headquarters and the National Gallery of Australia), Australian interests in this country and overseas, and the private residences of commonwealth holders of high public office (national security threat assessments).

Table 3 compares the number of threat assessments issued in the last three years. Appendix G lists significant assessments during 1995–96.

*Table 3: Threat assessments issued 1993–94 to 1995–96*

Subject of assessment	1993–94	1994–95	1995–96
Visiting dignitaries	236	216	153
Australian dignitaries	223	170	315
National security threat assessments	28	21	21
Demonstration notifications	229	105	45
Diplomatic premises	90	114	109
Other threat assessments	143	86	93
Total	949	712	736



Although the number of incidents of politically motivated violence has not increased since the last reporting period, the level of potential threat has risen. The federal election campaign gave rise to many requests for assessments relating to commonwealth holders of high public office. The demand continued after the election, with threats and volatile protests against some new government policies, including the projected gun control laws.

Visiting overseas dignitaries, especially from Asia, arrived in significant numbers during the last half of 1995, generating a corresponding number of requests for threat assessments. High profile visitors from Indonesia and Vietnam in particular were the targets of highly charged demonstrations. The diplomatic missions in Australia of Cambodia, China, France, Germany, Indonesia, Lebanon, Turkey, the USA and Vietnam were afforded additional protection at various times during the year, in response to our assessments of potential threats to their security.

*Minister for Foreign Affairs Alexander Downer meeting the Prime Minister of Malaysia, Dr Mahathir, during his visit here in March 1996. ASIO provides threat assessments to help ensure the safety of foreign dignitaries visiting Australia.*

*(Photo: AAP)*



# Protective Security Program

ASIO's Protective Security Program provides government and its agencies with advice on protecting commonwealth assets—people, property and information—against security risks.

Each of the program's components—security assessments and protective security advice—is covered in more detail below. Very little information is excluded from the unclassified *Report to Parliament*.

Program expenditure in 1995–96 is shown in Table 4 (excluded from the unclassified *Report to Parliament*).

## Security assessments

A 'security assessment' is a formal means by which ASIO tells a government agency whether a particular person may be of security concern to Australia. Assessments are provided for two distinct client purposes. One client group requests the screening of non-Australians seeking entry visas, permanent residence or change of status from temporary to permanent residence. Assessments of this nature are generally requested by the Department of Immigration and Multicultural Affairs (DIMA) or the Department of Foreign Affairs and Trade (DFAT). The other client group requests background checking of people seeking a security clearance that will give them access to classified material or secured premises. Any commonwealth government agency may request such a security assessment.

In most cases—if the checking procedures do not indicate anything of security concern—the assessment takes the form of a statement that ASIO does not wish to recommend against the application. However, if something in the person's background or activities arouses security concern, an assessment will be issued which is either 'adverse' or 'qualified'. An adverse assessment is a recommendation from ASIO, supported by a statement of grounds, that the person should not be granted the entry or access sought. A qualified assessment does not recommend against the access but passes on to the requesting agency some information that ASIO considers should be taken into account in decision-making. In each case, a final decision rests with the requesting agency.

## Screening for entry or permanent residence

One countermeasure against people constituting a security risk is to deny them access to this country. In deciding whether to grant the applications of people wishing to enter Australia or to become permanent residents, DIMA and DFAT take into account assessments by ASIO of the security threat potential of applicants.

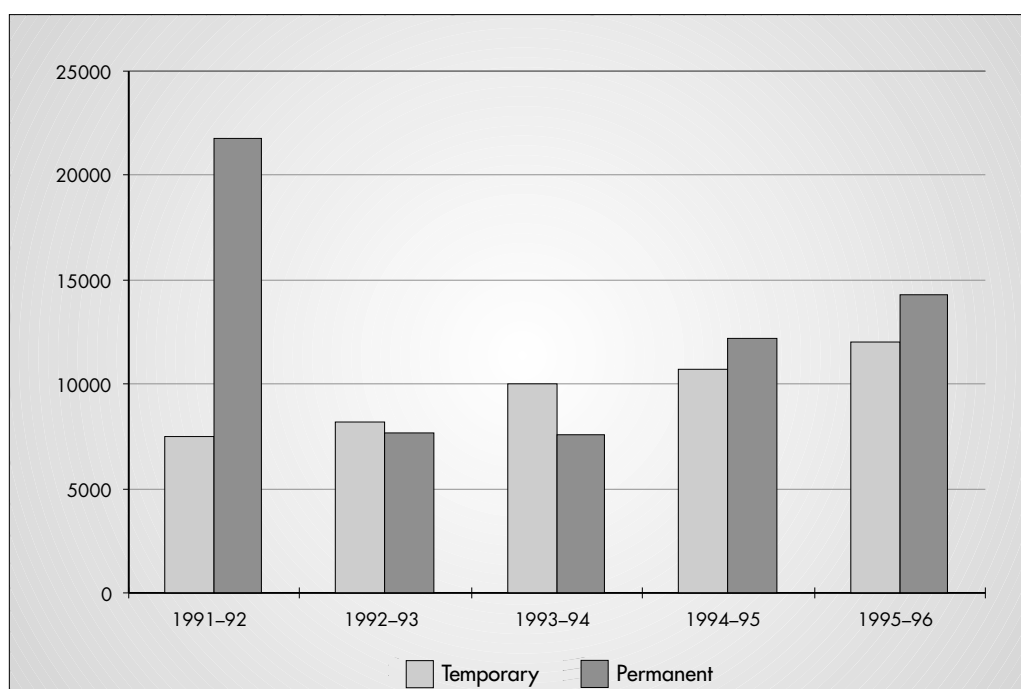
During the last year, ASIO processed over 26 000 applications for temporary and permanent entry or residence (see Table 5 and Figure 4 for five-year trends). There is a time frame within which security checking must be completed. We processed 96.4% of applications within the agreed time.



**Table 5: Visa security assessments requested 1991–92 to 1995–96**

Type of entry	1991–92	1992–93	1993–94	1994–95	1995–96
Temporary	7 517	8 203	10 044	10 695	12 037
Permanent	21 772	7 705	7 588	12 228	14 322
Total	29 289	15 908	17 632	22 923	26 359

**Figure 4: Trend in visa security assessments, 1991–92 to 1995–96**



The trend in adverse and qualified security assessments issued during the last five years to people seeking temporary or permanent entry to or residence in Australia is shown in Table 6 and Figure 5. In 1995–96 adverse assessments fell from 19 to 16, and qualified assessments increased from 16 to 17. All but one of the 16 adverse assessments were accepted by the requesting departments, resulting in

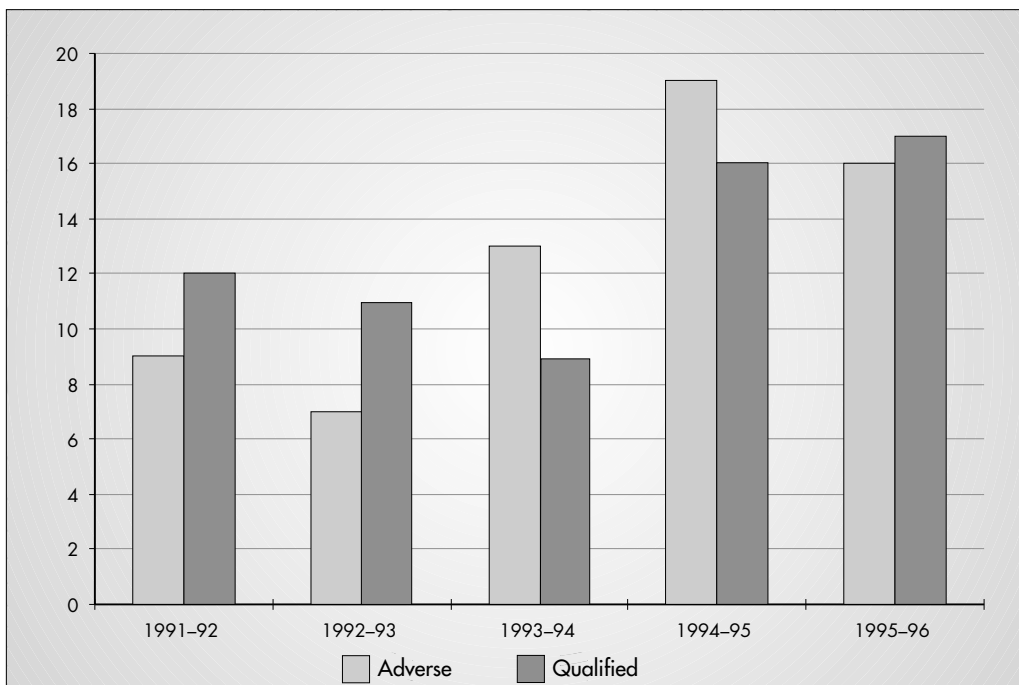
denial of the applications. The exception was granted entry on national interest grounds, following representations by DFAT. In the case of two qualified assessments issued by ASIO, DIMA subsequently declined to grant a visa.

More detail on the recommendations against entry or residence are contained in Appendix H (with some detail excluded from the unclassified *Report to Parliament*).

*Table 6: Adverse and qualified assessments for visa applicants 1991–92 to 1995–96*

Type of assessment	1991–92	1992–93	1993–94	1994–95	1995–96
Adverse	9	7	13	19	16
Qualified	12	11	9	16	17
Total	21	18	22	35	33

*Figure 5: Adverse and qualified assessments for visa applicants, 1991–92 to 1995–96*



### *Checking for agency security clearances*

Since ASIO was established in 1949, it has had a role in checking the background of government employees whose work requires access to information of national security

significance. Before granting a security clearance to a candidate for a 'designated security access position', commonwealth agencies are required carefully to assess the suitability of the candidate. This process of assessment includes seeking advice from ASIO (in the form of a



security assessment) on whether anything in the candidate's background or activities is a cause for security concern.

In delivering this service to client agencies in 1995–96, ASIO continued to aim at completing 80% of the assessments within ten working days, with no more than 1% remaining incomplete after twelve weeks. Altogether 87.7% of access cases were completed in ten days or less (compared with 93.3% last year), but 1.3% took longer than twelve weeks to resolve (compared with less than 1% last year). The slight drop in performance resulted

mainly from external delays in completing international inquiries and the complexity of some of the cases.

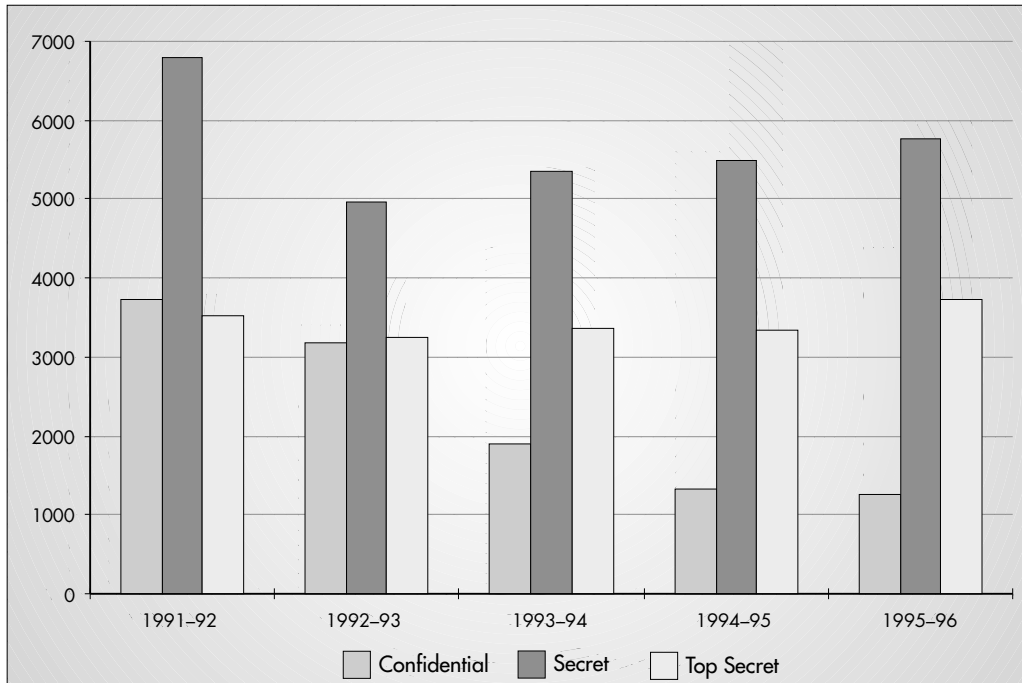
No adverse assessments, but three qualified assessments were issued in 1995–96 in response to requests from agencies for security clearances. One appeal against a qualified assessment in 1994–95 was heard by the Security Appeals Tribunal in 1995–96. The appeal was dismissed.

Table 7 and Figure 6 show the number of requests for security clearance assessments during the last five years.

*Table 7: Requests for security clearance assessments 1991–92 to 1995–96*

Level of access sought	1991–92	1992–93	1993–94	1994–95	1995–96
Confidential	3 734	3 180	1 905	1 325	1 259
Secret	6 803	4 955	5 363	5 485	5 757
Top Secret	3 528	3 237	3 361	3 346	3 725
Total	14 065	11 372	10 629	10 156	10 741

Figure 6: Requests for security clearance assessments 1991–92 to 1995–96



### Protective security advice

ASIO's role as the government's adviser on security encompasses the need to advise agencies on protective security measures to safeguard national security classified material and government assets. This advisory work falls into three categories:

- *Consultancy security advice* to clients on how best to protect their people, classified information, premises and assets.
- *Equipment testing and reporting* to help clients select the right security equipment.
- *Security awareness raising* to pass on expertise and information and raise general awareness of protective security issues.

### Consultancy security advice

In response to requests from government agencies, ASIO prepared 61 risk assessment and protective security advice reports in 1995–96 (compared with 59 last year). In each case the emphasis was on identifying cost-effective ways to secure assets and reduce outlays on security expenditure. The process involves close liaison with clients, who work with ASIO to identify their assets and threshold of risk tolerance as a basis for managing the risks.

As well as providing these formal reports on a cost recovery basis, our protective security specialists continued to respond to ad hoc requests for advice, usually by telephone, from experienced agency security advisers and officers who were able to do most of the risk assessment



and security planning work for their own agencies. There were more than 2000 calls for this fast and economical form of advice during the review period, making it a significant part of our protective security commitment. Informal feedback from clients indicated they found it effective.

We are seeing an increasing trend for agencies to address the safety of personnel, in conjunction with the security of information, assets and property.

As in past years, there was a strong demand from agencies for audio counter-measure testing of areas used for sensitive meetings. The audio counter-measure testing program was rated effective since we received no reports of compromised meetings where tests were conducted before the meeting.

### *Equipment testing and reporting*

Many manufacturers seek to sell equipment to commonwealth agencies with the claim that it improves physical security. ASIO carries out equipment testing to validate these claims. The testing program sets minimum standards for the quality of security products. Test results are reported in ASIO's *Security Equipment Catalogue* or are passed to manufacturers and clients via training sessions and on-site briefings and advice. The catalogue is sold to government agencies to help them choose equipment that best suits their agency's needs. As well as this role in quality control, our test and evaluation resources help manufacturers and suppliers to develop and market Australian-made security products and services, nationally and internationally.

During the year we also trained security specialists from the private sector in the design philosophy of government high security alarm systems to reduce dependence on public sector protective security resources.

Our capacity to advise government on cost-effective protective security depends on keeping abreast of technological developments in the security industry. We therefore seek representation in international bodies and remain alert to developments which could strengthen commonwealth security.

As in previous periods, two engineering undergraduates joined ASIO during 1995–96 for work experience training in security engineering.

### *Raising security awareness*

ASIO not only supports the work of security advisers in individual departments and agencies, but also aims to raise the security awareness generally of government officials. In addition, we pass on our security experience and standards to the broader community through membership of six working committees of Standards Australia and by helping educational institutions design training courses in security work.

In response to the demands of a small group of government clients we continued to provide special training on such topics as using and operating security equipment, and contributed several lectures at security training courses for government security officers (mostly run by the Attorney-General's Department). As in previous years, we conducted a risk assessment course for government agencies.

During the review period we gave three security awareness presentations to groups of up to one hundred government officials and delivered 15 personal briefings to people travelling overseas on government business. The briefings are designed to help Australians protect themselves from security problems and alert them to circumstances which could compromise or harm them and Australia's interests.

We also continued a program to explain our protective security responsibilities to commonwealth agencies and to the security industry, which has obligations to the commonwealth. A number of officers represented ASIO at the South Pacific regional conference of the American Society for Industrial Security and at the annual 'Security in Government' conference, where they gave presentations on ASIO's role in protective security.

---



# Foreign Intelligence Collection Program

As well as stipulating our principal role of collecting and analysing security intelligence, the ASIO Act authorises us to collect foreign intelligence under warrant inside Australia on behalf of partner agencies within the Australian intelligence community. This function is discharged through the Foreign Intelligence Collection Program. Foreign intelligence is collected only in response to specific requests from the Minister for Defence or the Minister for Foreign Affairs. (The handling of foreign intelligence gathered incidentally in the

course of security intelligence investigations is described on page 14.)

Table 8 (excluded from the unclassified *Report to Parliament*) shows recent program expenditure.

The program's main objective is to satisfy the needs of client agencies by delivering the requested intelligence product within the required timeframe.

The remainder of this program report is excluded from the unclassified *Report to Parliament*.

---



# Counter Terrorism Support Program

ASIO is one of several agencies contributing to Australia's defences against terrorism under the coordination of two major committees:

- SIDC-PAV, the Special Interdepartmental Committee for Protection Against Violence, which coordinates federal agencies with responsibilities for countering politically motivated violence
- SAC-PAV, the Standing Advisory Committee on Commonwealth-State Cooperation for Protection against Violence, which coordinates the work of federal agencies with that of their state counterparts.

During 1995–96, with a view to the 2000 Olympics, the security committee of the Sydney Organising Committee for the Olympic Games (SOCOG)—on which ASIO is represented—also played a significant part in coordinating the activities of those state and federal agencies with a role in countering terrorism and violence.

ASIO's counter terrorism work comprises prevention as well as a crisis management and response capability. Prevention functions include collecting information and providing reports and advice to government and clients under ASIO's security intelligence and protective security programs. We provide threat assessments, security intelligence and protective security advice to agencies through SIDC-PAV and SAC-PAV.

The crisis response function is delivered by the Counter Terrorism Support Program. Its main purpose is to strengthen Australia's counter terrorism response capability and meet the needs of partner agencies for cooperation and support.

Table 10 (excluded from the unclassified *Report to Parliament*) shows recent program expenditure.

Arrangements for liaison between federal and state departments and agencies, national crisis response management and post-incident cooperation are set out in the National Anti-Terrorist Plan (NATP). Under the NATP, ASIO contributes to policy development, preventive arrangements and crisis contingency planning. We also maintain an intelligence collection and communications structure—the National Intelligence Group (NIG)—which operates during counter terrorism exercises and in times of national crisis when the government orders activation of the NATP. During the review period a new operations centre within ASIO's central office was fitted out for use by the NIG.

The NIG, when convened, is staffed by a mix of ASIO officers and officers from other agencies. The JIG (Joint Intelligence Group), which is a unit established by the local police agency at or near the scene of a terrorist incident, also includes staff from ASIO.



In 1995–96 ASIO took part in four NATP counter terrorism exercises conducted under the auspices of SAC–PAV:

- Operational Response Exercise (OPREX) TASMANIAN TIGER in Tasmania in August 1995.
- National Exercise (NATEX) RUSSET MIST in South Australia in October 1995.
- OPREX RED RATTLER in Sydney in November 1995.
- NATEX TOP SHELF in Karratha, Western Australia in April 1996.

ASIO also helped to plan, write and control the exercises.

The exercise series gave us opportunities to test how our procedures, resources and methods fit in with those of state and territory police agencies. It confirmed the effectiveness of our crisis response capability.

In two of the exercises ASIO provided technical intelligence gathering facilities in support of the police incident commander, supplementing police technical unit capabilities.

An evaluation of the appropriateness, efficiency and effectiveness of the counter terrorism technical support capability began in November 1995. A report is to be completed by December 1996.

Aviation security exercise REACT 6 was held in Sydney on 29 February 1996. ASIO helped to write the scenario as well as taking part.



*During 1995–96, new NIG accommodation and facilities were established within ASIO's central office in Canberra.*

# Corporate Support Program

ASIO's Corporate Support Program covers a range of executive and corporate management support functions, liaison with government and corporate communication. In budget terms the program allocation is small, because the cost of most of the day-to-day support functions—including the technical development infrastructure, human resource management and budget and financial services—is dispersed among the business programs making use of them. Table 11 (excluded from the unclassified *Report to Parliament*) shows expenditure.

---

Information on outcomes within various support function areas is included under the four other program headings. However, a range of important activities and outcomes that are part of the general concept of corporate support still require to be reported on separately (even though for working purposes they are funded diversely under the other programs). These include various people management and infrastructure issues and corporate executive functions, and have been dealt with in the corporate overview section of this report.



## Information available on request

In line with government guidelines this year's report is again, as an efficiency, omitting a proportion of administrative detail. Instead, unclassified information will be made available to senators, members of parliament and members of the public within five days of the request. Requests can be made in writing to the Director-General of Security, GPO Box 2176, Canberra City, ACT 2601; or by telephoning the public liaison number: (06) 249 8381.

Material is available on request on the following topics:

- ASIO's employment of people from equal employment opportunity (EEO) target groups (see also Appendix C).
- Training, including expenditure in relation to the *Training Guarantee Act 1990* and on the number of people and person days involved (see also Appendix B).
- Insurable or manageable claims and losses which individually resulted in net costs to the commonwealth of \$50 000 or more, as well as aggregate claims of more than \$10 000.
- Compliance with government information technology purchasing arrangements.
- Payment of accounts.
- Consultancy services used (with the exception of some details excluded for security reasons).
- Environmental matters (including details of energy usage, energy savings targets, use of energy efficient features in buildings; consumption of energy by ASIO's administrative vehicle fleet and reviews of vehicle usage; purchase of appliances with not less than a four-star energy rating; and the use of opportunities to improve energy efficiency in regard to equipment which consumes a significant amount of energy).
- Property usage (showing overall usage in terms of both rental charges and square metres of office space, non-office space and dead rent attributed to each program, and valuations for properties which are exempt from a rent or capital use charge).

A full list of annual reporting requirements can be found in the compliance index on page 96 of this report.

# Financial Statements

*Money is like a sixth sense without which you  
cannot make use of the other five.*

---

W. SOMERSET MAUGHAM, 1915



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



## AUSTRALIAN SECURITY INTELLIGENCE ORGANIZATION INDEPENDENT AUDIT REPORT

### Scope

I have audited the financial statements of the Australian Security Intelligence Organization for the year ended 30 June 1996.

The statements comprise:

- Statement by the Director-General of Security;
- Operating Statement;
- Statement of Assets and Liabilities;
- Statement of Cash Flows;
- Statement of Transactions by Fund; and
- Notes to the Financial Statements.

The Director-General of Security is responsible for the preparation and presentation of the financial statements and the information contained therein. I have conducted an independent audit of the financial statements in order to express an opinion on them.

The audit has been conducted in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards, to provide reasonable assurance as to whether the financial statements are free of material mis-statement. Audit procedures included examination, on a test basis, of evidence supporting the amounts and other disclosures in the financial report, and the evaluation of accounting policies and significant accounting estimates. These procedures have been undertaken to form an opinion whether, in all material respects, the financial statements are presented fairly in accordance with Australian Statements of Accounting Concepts, applicable Accounting Standards, other mandatory professional reporting requirements and statutory requirements so as to present a view of the Organization which is consistent with my understanding of its financial position, its operations and its cash flows.

The audit opinion expressed in this report has been formed on the above basis.

### Qualification

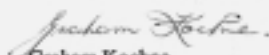
The Attorney-General has issued a declaration under subsection 70D(1) of the *Audit Act 1901* that particular parts of the accounts are to be treated as exempt accounts. These accounts are not subject to audit by the Auditor-General. I am therefore unable to form an opinion on the receipts to and expenditure from the exempt accounts, and on the assets and liabilities related to those exempt accounts. The audit opinion on the financial statements for the year ended 30 June 1995 was qualified on the same basis. A certificate will be sought from the Attorney-General under subsection 70D(5) of the *Audit Act 1901* that moneys allocated to those exempt accounts were properly expended.

### Qualified Audit Opinion

In accordance with subsection 51(1) of the *Audit Act 1901* I now report that, except for the limitation of scope on my work as described in the qualification section, and the effects of such adjustments, if any, as might have been determined as necessary had the limitation not existed, the financial statements, in my opinion:

- are in agreement with the accounts and records kept in accordance with section 40 of the Act;
- are in accordance with the Guidelines for Financial Statements of Departments; and
- present fairly in accordance with Statements of Accounting Concepts, applicable Accounting Standards and other mandatory reporting requirements the information required by the Guidelines including the Organization's departmental and administered operations and its cash flows for the year ended 30 June 1996 and departmental and administered assets and liabilities as at that date.

Australian National Audit Office

  
Graham Koehne  
Executive Director

For the Auditor-General

Canberra ACT  
13 September 1996



COMMONWEALTH OF AUSTRALIA

AUDIT ACT 1901

CERTIFICATE UNDER SUB-SECTION 70D(5)

I, Daryl Williams, the Attorney-General of the Commonwealth, being, for the purpose of sub-section 70D(5) of the *Audit Act 1901*, the responsible Minister in respect of the Australian Security Intelligence Organization and having received from the Auditor-General a notification, under that sub-section, of the total of the amounts that, according to the accounts of, or relating to, that Organization audited by him, were, during the financial year that commenced on 1 July 1995, allocated for crediting to exempt accounts of that Organization, hereby certify:

- (a) that the moneys shown in those exempt accounts as having been expended for a purpose or service specified in those exempt accounts during that financial year were properly expended in respect of that service or purpose and in the public interest;
- (b) that the amount standing to the credit of those exempt accounts at the end of the financial year:
  - (i) was held partly in cash and partly on deposit with a bank;
  - (ii) did not equal the amount ascertained by aggregating the amount standing to the credit of those exempt accounts at the commencement of that financial year and the total specified in the above-mentioned notification and subtracting from that aggregate the total of the moneys referred to in paragraph (a); and
  - (iii) differed from the amount ascertained by the aggregation referred to in paragraph (b)(ii) above by reason of miscellaneous receipts credited to the exempt accounts, in addition to the amounts allocated for crediting to the exempt accounts referred to above;
- (c) that the exempt accounts were inspected and audited; and
- (d) that no irregularities or deficiencies in the exempt accounts were disclosed during the financial year.

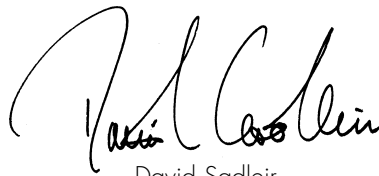
Dated this      *2nd day of December*      1996

*Daryl Williams*  
ATTORNEY-GENERAL

## Statement by the Director-General of Security

### CERTIFICATION

I certify that the attached financial statements for the year ended 30 June 1996 are in agreement with the Organization's accounts and records and, in my opinion, the statements have been prepared in accordance with the Guidelines for *Financial Statements of Departments* issued by the Minister for Finance for reporting periods on and after 30 June 1995.

A handwritten signature in black ink, appearing to read 'David Sadleir', with a stylized flourish at the end.

David Sadleir  
Director-General of Security

11 September 1996

## Operating Statement for the year ended 30 June 1996

	Notes	1995-96 \$ '000	1994-95 \$ '000
<b>NET COST OF SERVICES</b>			
<b>Expenses</b>			
Employee expenses	3	32 924	31 537
Other administrative expenses	4	27 738	25 267
Total expenses		60 662	56 804
<b>Revenues from independent sources</b>			
User charges	5	264	727
Other revenues from independent sources	5	2 261	436
Total revenues from independent sources		2 525	1 163
Net cost of services		58 137	55 641
<b>REVENUES FROM GOVERNMENT</b>			
Appropriations used for:			
Ordinary annual services		51 502	54 083
Liabilities assumed by Government	1(l)	1 438	3 761
Resources received free of charge	5	2 067	1 697
Total revenues from government		55 007	59 541
<b>Excess of revenues from government over net cost of services</b>		(3 130)	3 900
Accumulated revenues less expenses at beginning of reporting period		16 868	12 968
<b>Accumulated revenues less expenses at end of reporting period</b>		13 738	16 868

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

## Statement of Assets and Liabilities as at 30 June 1996

	Notes	1995-96 \$ '000	1994-95 \$ '000
<b>CURRENT ASSETS</b>			
Cash	7	2 949	2 939
Receivables	8	312	211
Other	9	527	317
Total current assets		3 788	3 467
<b>NON-CURRENT ASSETS</b>			
Property, plant and equipment	10	21 416	24 935
Total non-current assets		21 416	24 935
Total assets		25 204	28 402
<b>CURRENT LIABILITIES</b>			
Creditors	11	888	1 916
Provisions	12	2 875	2 916
Total current liabilities		3 763	4 832
<b>NON-CURRENT LIABILITIES</b>			
Provisions	12	7 703	6 702
Total non-current liabilities		7 703	6 702
Total liabilities		11 466	11 534
<b>NET ASSETS</b>		13 738	16 868

The above Statement of Assets and Liabilities should be read in conjunction with the accompanying notes.

## Statement of Cash Flows for the year ended 30 June 1996

	Notes	1995-96 \$ '000	1994-95 \$ '000
<b>CASH FLOWS FROM OPERATING ACTIVITIES</b>			
<b>Inflows:</b>			
Appropriation receipts		51 502	54 083
Section 35 receipts		416	1 373
Total		51 918	55 456
<b>Outflows:</b>			
Employee expenses		(30 663)	(27 234)
Other administrative expenses		(18 680)	(18 956)
Total		(49 343)	(46 190)
Net cash provided/(used) by operating activities	18	2 575	9 266
<b>CASH FLOWS FROM INVESTING ACTIVITIES</b>			
<b>Inflows:</b>			
Proceeds from sale of non-current assets		947	161
<b>Outflows:</b>			
Payments on non-current assets		(3 512)	(9 643)
Net cash provided/(used) in investing activities		(2 565)	(9 482)
<b>CASH FLOW FROM FINANCING ACTIVITIES</b>			
		–	–
Net increase/(decrease) in cash held		10	(216)
Cash at beginning of the reporting period		2 939	3 155
Cash at end of the reporting period		2 949	2 939

The above Statement of Cash Flows should be read in conjunction with the accompanying notes.

## Statement of Transactions by Fund for the year ended 30 June 1996

	<b>Notes</b>	1995-96 Budget \$	<b>1995-96 Actual \$</b>	1994-95 Actual \$
<b>Consolidated Revenue Fund</b>				
<b>RECEIPTS</b>				
Division 125		373 000	1 370 693	1 534 141
<b>EXPENDITURE</b>				
Annual Appropriations:				
Appropriation Act No. 1		56 809 000	51 501 670	54 083 257
S35 of the Audit Act 1901		373 000	1 370 693	1 534 141
Total expenditure	19	57 182 000	52 872 363	55 617 398
<b>Loan Fund</b>				
		Nil	Nil	Nil
<b>Trust Fund</b>				
		Nil	Nil	Nil

The above Statement of Transactions by Fund should be read in conjunction with the accompanying notes.

## Notes to the Financial Statements for the year ended 30 June 1996

### NOTE 1: Objective

ASIO's objective is to collect security intelligence, assess the security situation and advise government.

### NOTE 2: Summary of significant accounting policies

#### a. Basis of accounting

The financial statements are required by section 50 of the *Audit Act 1901* and are a general purpose financial report. The financial statements have been prepared in accordance with Guidelines on *Financial Statements of Departments* issued by the Minister for Finance for reporting periods ending on and after 30 June 1995 (the Guidelines). The Guidelines require compliance with Statements of Accounting Concepts, Australian Accounting Standards, Accounting Guidance Releases issued by the Australian Accounting Research Foundation and other relevant mandatory professional reporting requirements.

The financial statements have been prepared on an accrual basis, are in accordance with the historical cost convention and do not take account of changing money values, except where stated.

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

#### b. Rounding

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

- Statement of Transactions by Fund
- amounts written off
- remuneration of executives.

#### c. Taxation

ASIO's activities for 1995-96 and prior years are exempt from all forms of taxation except Fringe Benefits Tax.

**d. 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.

Currency gains and losses are not recognised in the financial statements as the Department of Finance assumes responsibility for ASIO's foreign currency exposure. The net amount of such gains and losses is not considered material to the Organization's operations.

**e. Insurance**

In accordance with government policy, assets are not insured and losses are expensed as they are incurred.

**f. Bad and doubtful debts**

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

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

**g. Asset capitalisation threshold**

All depreciable non-current assets with a historical cost equal to or in excess of \$500 are capitalised in the year of acquisition and included on ASIO's asset register. The value of all such assets is included in the financial statements. Assets with a historical cost under \$500 are expensed in the year of acquisition. In prior years only those assets with a historical cost equal to or greater than \$2 000 were disclosed. For the financial effect of this change in policy see Note 10.

**h. Valuation of non-current assets**

The cost method of accounting is used for the initial recording of all acquisitions of assets controlled by ASIO. Cost is determined as the cash amount paid or the fair value of assets transferred or acquired.

Land and buildings are revalued every three years. Land and buildings were independently valued during the year on the basis of market price.

**i. Depreciation of non-current assets**

All depreciable non-current assets are written off over their estimated useful lives. Depreciation is calculated using the straightline method which correctly reflects the pattern of usage and rate of loss of value of ASIO's depreciable non-current assets.

Leasehold improvements are amortised on a straightline basis over the estimated useful life of the improvements or the unexpired period of the lease.



**j. Employee entitlements**

All vesting employee entitlements, including annual leave and long service leave, have been recognised as liabilities in the financial statements. No provision for sick leave is included as sick leave is non-vesting.

The long service leave provision has been calculated having regard to the probability that long service leave will in the future either be taken or have to be paid even though an employee may not yet have met the qualifying period of ten years.

Provision has been made for annual leave and this item has been split between current and non-current on the basis of past history.

**k. Comparative figures**

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

**l. Superannuation**

Staff of ASIO contribute to the Commonwealth Superannuation Scheme and the Public Sector Superannuation Scheme. Employer contributions amounting to \$3 927 000 in relation to these schemes have been expensed in these financial statements. Of this amount \$1 438 000 is disclosed in the Operating Statement as a liability assumed by Government and represents the estimated cost for the period July to November 1995. Funding for this expenditure commenced in November 1995. The total cost of superannuation in 1994–95 (\$3 761 000) was a liability assumed by Government.

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

Employer Superannuation Productivity Benefit contributions totalled \$630 300. (1994–95: \$602 500)

**m. Resources received free of charge**

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

**n. Administered items**

ASIO does not have any administered items.

**o. Program statement**

ASIO is funded by Parliament as Sub-program 6.8 of the Attorney-General's portfolio and no program statement is required with these financial statements.

**NOTE 3: Employee expenses**

	<b>1995-96</b> <b>\$ '000</b>	1994-95 \$ '000
Salaries and wages	24 878	24 115
Superannuation	4 557	4 366
Employee entitlements	3 489	3 056
Total	<u>32 924</u>	<u>31 537</u>

**NOTE 4: Other administrative expenses**

Provision for doubtful debts — trade debtors	8	2
Depreciation expense — property, plant and equipment	6 617	4 304
Amounts written off — property, plant and equipment (Note 16)	1 280	—
Rental expenses	4 206	4 114
Office supplies/other operating costs	12 060	13 464
Consultants and contractors	645	518
Travel	2 251	2 318
Training	552	528
Other	119	19
Total	<u>27 738</u>	<u>25 267</u>

	1995-96 \$ '000	1994-95 \$ '000
<b>NOTE 5: Items credited as revenue</b>		
<b>Revenues from Independent sources:</b>		
User charges	264	727
Other revenues from independent sources —		
Profits arising from the sale of non-current assets	155	43
Change in asset capitalisation threshold (Note 10)	1 777	—
Other	329	393
Total	2 525	1 163
<b>Resources received free of charge:</b>		
<b>Australian Archives</b>		
Provision of ongoing archival services	28	34
<b>Australian National Audit Office</b>		
The estimated cost of services provided by the Auditor-General in auditing the Organization's financial statements	57	53
<b>Department of Defence</b>		
Provision of air transport services and training	212	110
<b>Department of Foreign Affairs and Trade</b>		
Provision of a diplomatic communications network facility and the payment of salary and support costs for ASIO staff stationed at overseas liaison posts	1 770	1 500
Total	2 067	1 697

**NOTE 6: Services received free of charge but not recognised are:**

Reliable estimates of costs for 1995-96 are not available

**Attorney-General's Department**

Provision of accounting services not able to be provided within the Organization

**Department of Industrial Relations**

Provision of advice in respect of conditions of service for ASIO staff

**NOTE 7: Cash**

	<b>1995-96 \$ '000</b>	1994-95 \$ '000
Cash at bank	2 824	2 824
Cash on hand	125	115
Total	<u>2 949</u>	<u>2 939</u>

**NOTE 8: Receivables**

	1995-96 \$ '000	1994-95 \$ '000
<b>Trade debtors:</b>		
Government departments and agencies	184	133
Other	69	10
Total	<u>253</u>	<u>143</u>
Less provision for doubtful debts	8	2
Total	<u>245</u>	<u>141</u>
<b>Other debtors:</b>		
Government departments and agencies	64	70
Other	3	—
Total	<u>67</u>	<u>70</u>
Total	<u>312</u>	<u>211</u>
Receivables are aged as follows:		
Not overdue	251	203
Overdue:		
less than 30 days	1	7
30 to 60 days	1	—
60 to 90 days	26	—
over 90 days	41	3
Total	<u>320</u>	<u>213</u>

**NOTE 9: Other current assets****Prepayments:**

Rent on properties	262	168
Computer hardware and software maintenance fees	83	93
Training fees	95	—
Other	87	56
Total	<u>527</u>	<u>317</u>

**1995-96**  
**\$ '000**

1994-95  
\$ '000

### NOTE 10: Property, plant and equipment

Computing and communication equipment less: accumulated depreciation	21 733 (13 306)	22 641 (12 199)
Technical and electronic equipment less: accumulated depreciation	7 098 (5 523)	5 920 (4 215)
Office furniture less: accumulated depreciation	371 (228)	330 (194)
Office equipment less: accumulated depreciation	2 476 (943)	2 558 (833)
Motor vehicles less: accumulated depreciation	3 090 (96)	3 058 (141)
Computing software less: accumulated depreciation	7 016 (3 742)	6 306 (2 150)
Land	497	497
Buildings less: accumulated amortisation	496 (66)	658 (121)
Building and leasehold improvements less: accumulated amortisation	4 556 (2 013)	4 384 (1 564)
Total	<u>21 416</u>	<u>24 935</u>

The value of property, plant and equipment disclosed in the 1994-95 financial statements included only those assets with a historical cost equal to or greater than \$2 000. During 1995-96 this policy was revised to include assets with a value equal to or greater than \$500. The net financial effect (after allowing for accumulated depreciation) of this change in policy is \$ 1 777 000 and it has been reflected in the Operating Statement.

### NOTE 11: Creditors

#### Trade creditors:

Government departments and agencies	333	684
Other	326	954
Total	<u>659</u>	<u>1 638</u>

#### Other creditors:

Government departments and agencies	-	-
Other	229	278
Total	<u>229</u>	<u>278</u>
Total	<u>888</u>	<u>1 916</u>

**1995-96**  
**\$ '000**

1994-95  
\$ '000

## NOTE 12: Provisions

### Current:

#### *Employee entitlements*

Long service leave	760	285
Recreation leave (including bonus)	2 100	2 508
Performance pay	15	123
Total	<u>2 875</u>	<u>2 916</u>

### Non-current:

#### *Employee entitlements*

Long service leave	6 275	5 734
Recreation leave (including bonus)	1 428	968
Total	<u>7 703</u>	<u>6 702</u>

## NOTE 13: Act of Grace payments

No payments were made during the financial year 1995-96 (1994-95: Nil) pursuant to authorisations given under section 34A of the *Audit Act 1901*.

## NOTE 14: Waiver of rights to payment of moneys

No payments were waived during the financial year 1995-96 (1994-95: Nil) under subsection 70C(2) of the *Audit Act 1901*.

**1995-96**  
**\$ '000**

1994-95  
\$ '000

**NOTE 15: Agreements equally proportionately unperformed**

Amounts payable not recognised in the financial statements from agreements equally proportionately unperformed are:

Not later than one year		
Operating leases	1 883	1 668
Other	430	1 346
Later than one year but not later than two years		
Operating leases	1 774	1 779
Other	—	—
Later than two years but not later than five years		
Operating leases	4 930	5 303
Other	—	—
Later than five years		
Operating leases	2 981	2 508
Other	—	—
Total	<u>11 568</u>	<u>11 258</u>

There is no formal lease in place in respect of ASIO's Central Office. Annual rental payments amount to \$1 800 000 (1994-95: \$1 800 000)

**NOTE 16: Amounts written off**

**1995-96**  
**\$**

1994-95  
\$

Losses or deficiencies of public moneys	—	—
Irrecoverable amounts of revenue	—	—
Irrecoverable debts and overpayments	—	—
Amounts of revenue, or debts or overpayments, the recovery of which would, in the opinion of the Minister, be uneconomical	—	—
Lost, deficient, condemned, unserviceable or obsolete stores	1 279 824	39 819

These details are furnished in relation to amounts written off during the financial year 1995-96 under subsection 70C(1) of the *Audit Act 1901*. In 1995-96, a major segment of ASIO's telecommunications network was replaced. The write-off of this obsolete equipment (depreciated value) amounted to \$1 200 000.



## NOTE 17: Losses and deficiencies etc in public moneys and other property

No action was taken during the financial year 1995–96 (1994–5: Nil) under Part XIII A of the *Audit Act 1901*.

**1995–96**  
**\$ '000**

1994–95  
\$ '000

## NOTE 18: Cash reconciliation–cash flow statement

Reconciliation of net cash provided by operating activities to operating result.

Net cost of services — gain/(loss)	(58 137)	(55 641)
Revenues from government	55 007	59 541
Depreciation	6 617	4 304
(Profit)/Loss on sale of non-current assets	(155)	(43)
Asset write-off (Note 16)	1 280	—
(Increase)/Decrease in receivables	(101)	33
Increase in prepayments	(210)	(79)
Increase/(Decrease) in creditors	(1 028)	908
Increase in provisions	960	243
Items previously capitalised written off	119	—
Asset capitalisation adjustment (Note 10)	(1 777)	—
Net cash provided by operating activities	<u>2 575</u>	<u>9 266</u>

## NOTE 19: Total appropriations

1995–96  
Appropriation  
\$

**1995–96**  
**Actual**  
**\$**

1994–95  
Actual  
\$

The budgeted appropriation was amended by Appropriation Act No 3 as follows:

Appropriation Act No 1	56 809 000	} 52 872 363	55 617 398
Appropriation Act No 3	789 000		
Amounts deemed to be appropriated	1 370 693		
Total	<u>58 968 693</u>	<u>52 872 363</u>	<u>55 617 398</u>

**1995-96**  
**\$ '000**

1994-95  
\$ '000

### **NOTE 20: 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:

57

53

### **NOTE 21: Executive remuneration**

The number of executive officers who received or were due to receive fixed remuneration of \$100 000 or more:

	<b>Number</b>	<b>Number</b>
\$100 000 to \$110 000	9	—
\$110 000 to \$120 000	—	3
\$120 000 to \$130 000	3	—
\$140 000 to \$150 000	—	1
\$150 000 to \$160 000	1	—
\$170 000 to \$180 000	—	1
\$180 000 to \$190 000	1	—

The aggregate amount of fixed remuneration of executive officers shown above. The figures for 1994-95 have been amended.

\$1 703 680

\$791 120

The aggregate amount of performance pay paid during the year to executive officers shown above

\$29 716

—

### **NOTE 22: Appropriations made for future reporting periods**

As at 30 June 1996 appropriations relating to future reporting periods totalled \$25 876 000. This was under the Supply Act (No 1) 1996-97 and are to cover operating expenses for the first five months of 1996-97.

### **NOTE 23: Post balance date event**

In August 1996, an announcement was made of an intention to reduce the number of employees in ASIO by approximately 50. At balance date, neither individual positions nor officers who may be affected by this decision had been identified.

# Appendixes

*Men trip not on mountains,  
they stumble on stones.*

---

HINDUSTANI PROVERB



# List of appendixes

- A: Authorities approved for liaison purposes at 30 June 1996
- B: Staff management statistics
- C: Equal employment opportunity statistics
- D: Evaluations
- E: Public access to ASIO's records
- F: Program and notional breakdown of expenditure
- G: Significant threat assessments
- H: Recommendations against entry or residence

Note: All figures disclosed in the audited financial statements were prepared on an accrual basis as required by the relevant guidelines. Other figures shown throughout the report and particularly in these appendixes have been prepared on a cash expenditure basis in line with ASIO's appropriation. Consequently comparisons, particularly of detailed breakdowns of specific items, may not be possible.

## **A: Countries having authorities approved for liaison purposes at 30 June 1996**

Paragraph 19.1 (c) of the ASIO Act states that ASIO may cooperate with 'authorities of other countries approved by the Minister as being capable of assisting the Organization in the performance of its functions'.

This list is excluded from the unclassified *Report to Parliament*.

## B: Staff management statistics

### Staffing information

*Table 12: Total average staff level (ASL) and staff level and number at 30 June each year*

	1993-94	1994-95	1995-96
Average staff level for each financial year (FY)	562	530	551
Full time staff equivalent (FSE) at the end of each FY (30 June)	544	529	577
Number of staff at the end of each FY (30 June)	596	585	625

*Table 13: Composition of the workforce (number at 30 June each year)*

	1993-94	1994-95	1995-96
Permanent full-time	545	525	550
Temporary full-time	8	15	26
Permanent part-time	9	14	18
Temporary part-time	4	3	–
Casual	6	17	15
Non-operational (including unattached and on compensation)	24	11	16
Total	596	585	625

*Table 14: Location and structure of the workforce (FSE at 30 June each year)*

	<b>1993-94</b>	<b>1994-95</b>	<b>1995-96</b>
Central Office			
Director-General	1	1	1
SES	10	10	13
Senior Officers	66	68	87
Other	260	231	288
	337	310	389
States and Territories			
SES	2	3	1
Senior Officers	24	32	23
Other	181	184	164
	207	219	188
Total			
Director-General	1	1	1
SES	12	13	14
Senior Officers	90	100	110
Other	441	415	452
Grand total	544	529	577



*Table 15: SES equivalent staff location, classification and gender (number at 30 June each year)*

	1993-94	1994-95	1995-96
Central Office			
Band 1 - Female	3	3	3
- Male	4	4	6
Band 2 - Female		1	1
- Male	2	1	2
Band 3 - Male	1	1	
Seconded			
Band 3 - Male			1
States and territories			
Band 1 - Female			
- Male	2	2	1
Band 2 - Male		1	
Total	12	13	14

### **Performance pay**

Within a total of 12.9 FSE in ASIO's SES during the reporting period, 9.1 were Band 1, 2.8 were Band 2 and 1 was Band 3. Total expenditure on SES performance pay for 1994-95 was \$71 036.25 and Table 16 shows the distribution of ratings (the nature of the payment cycle means that the previous year's figures are reported each year). For 1995-96 SES performance pay totalled \$39 100, divided equally among 14 officers who were all rated 3. Senior officers were also all rated 3 when performance pay arrangements were finalised with a total payment of \$244 677 to 119 officers.

*Table 16: Distribution of ratings for SES performance pay 1994-95*

	Rating 5	Rating 4	Rating 3	Rating 2	Rating 1
No. of officers	2	8	2.9	nil	nil

## Training

*Table 17: Participation in internal training sessions, 1995–96*

Training area	No. of training sessions	No. of participants
Intelligence and operations	10	99
Management development	18	127
Systems education training	700	700
Total	728	926

*Table 18: Net eligible expenditure on training, 1995–96*

	\$
External training expenditure	626 432
Internal training expenditure	303 650
Salaries of the three corporate training areas	547 439
Total	1 477 521

## Occupational health and safety—reportable accidents

Table 19 shows the incidence of accidents during the year reportable under s.68 of the *Occupational Health and Safety (Commonwealth Employment) Act 1991*.

*Table 19: Reportable accidents 1994–95 and 1995–96*

Nature of accident	Notifications	
	1994–95	1995–96
Accidents resulting in death	-	-
Accidents causing serious personal injury	-	-
Accidents causing incapacity of 5 or more days	6	7 <sup>1</sup>
Dangerous occurrences not resulting in death, serious personal injury or incapacity	-	1 <sup>2</sup>

<sup>1</sup> Five of the seven accidents resulting in incapacity for five days or more were related to stress. Of the other two accidents causing incapacity, one related to the lifting of equipment and the other to a car accident. Action has been taken to promote safe techniques for lifting heavy objects.

<sup>2</sup> The dangerous occurrence was a lithium battery explosion. After an investigation of the incident, measures were put in place to prevent a similar occurrence.

## **Consultants**

ASIO employed 42 consultants during the year. Total expenditure on consultants was \$645 000. A partial list of consultants employed, excluding those classified for security reasons, is available on request.

## C: Equal employment opportunity statistics

*Table 20: Representation of designated groups within ASIO occupational groups, at 30 June 1996*

Group	Total staff No.	Women <sup>1</sup> No.(%)	NESB No.(%)	ATSI No.(%)	PWD No.(%)	Staff with EEO data <sup>1</sup> No.(%)
SES	14	4 (29)	-	-	1 (7)	13 (93)
Mgr A <sup>2</sup>	9	1 (11)	-	-	-	8 (89)
AM <sup>3</sup>	103	9 (9)	4 (4)	-	4 (4)	99 (96)
GIO1 <sup>4</sup>	132	31 (23)	6 (5)	-	2 (2)	113 (86)
SIO4 <sup>4</sup>	155	49 (32)	26 (18)	-	8 (6)	146 (94)
SIO1-3	190	120 (63)	7 (4)	1 (.5)	8 (5)	179 (92)
ITO1-2	16	2 (13)	1 (8)	-	-	12 (75)
ENG1-2	2	-	-	-	-	-
Other	4	-	-	-	-	2
Total	625	216 (34)	44 (7)	1 (0.2)	23 (4)	572 (91)

Source: CHRIS (Complete Human Resource Information System—ASIO's computerised personnel system). Percentages indicated in brackets.

<sup>1</sup> Percentages for headings 'Women' and 'Staff with EEO data' based on 'Total staff'; percentages for all other groups based on staff for whom EEO data was available. Provision of EEO data by staff is voluntary.

<sup>2</sup> Mgr A = Branch Manager equivalent to APS Senior Officer Grade A.

<sup>3</sup> AM (Assistant Manager) classification is the equivalent of the APS SOG C to SOG B classifications and includes Senior Officers in the Engineer and Information Technology Classifications.

<sup>4</sup> Salaries for GIO (Generalist Intelligence Officer) Grade 1 and SIO (Specialist Intelligence Officer) Grades 1-4 span the APS ASO 1-6 salary range.

*Table 21: Percentage representation of designated groups in ASIO, 1993–96*

<b>Group</b>	<b>June 1993</b>	<b>June 1994</b>	<b>June 1995</b>	<b>June 1996</b>
Women	33.5	34.5	34.7	34.6
NESB	7	6	7	7
ATSI	0.1	0.2	0.2	0.2
PWD	4.7	4.7	4.8	4.0

*Source: CHRIS (Complete Human Resource Information System—ASIO’s computerised personnel system). Percentages for ‘Women’ based on total staff; percentages for other groups based on staff for whom EEO data was available.*

**Key to abbreviations:** NESB = Non-English-speaking background; ATSI = Aboriginal and Torres Strait Islander; PWD = People with a disability.

## D: Evaluations

This appendix contains summaries of evaluations and reviews conducted during the year (comprehensive details of which are contained in separate, mainly classified, documents) together with reporting on the implementation of recommendations from evaluations completed during the year. Table 22 shows ASIO's evaluation program for the period 1996–97 to 1997–98 together with evaluations completed in the last 18 months.

Much of this appendix, including elements of the table, is excluded from the unclassified *Report to Parliament*.

*Table 22: ASIO internal evaluation program, 1996–97 to 1997–98*

Program/area	Evaluation subject area	Indicative timing
<i>Cross-program corporate support</i>	Public Research Section	Completed March 1995
	OASYS replacement program	Sep 95–Dec 97
	Flexible working hours and higher duties arrangements (both elements of ASIO Continuous Improvement Program)	Jul–Dec 96 Sep–Dec 96
<i>Security Intelligence (SI) Program</i>		
Requirements and assessments	Review of subject risk matrix process	From mid–97
	Threat assessments	To commence around Sep 97
Other SI-related evaluations		
	Special powers operations—planning and approval (element of ASIO Continuous Improvement Program)	Commenced Dec 95
<i>Protective Security Program</i>	Security access checking processing of requests (element of ASIO Continuous Improvement Program)	Dec 95–Dec 96
<i>Foreign Intelligence Collection Program</i>	Foreign intelligence collection	tba

### *Proposed evaluations in preliminary stage*

- OASYS replacement system

### *Proposed evaluation of the OASYS replacement program*

The replacement program for ASIO's office automation systems (OASYS) has been split into two stages over a five year period. Phase 1 started in 1994–95 and the first three items will be completed by the end of 1996–97. The last item in Phase 1 is not expected to be completed until the middle of 1998. Phase 1 has been extended so that recommendations of the security inquiry conducted by Mr Michael Cook (see page 6) can be implemented. Phase 2 will then commence and is scheduled to be completed late in the 1998–99 financial year. Phase 1 involves:

- replacing all 'dumb' terminals and 286 PCs with 486 work stations
- replacing the existing, separate and unsupportable character-based electronic mail system
- standardising the various application-to-user interfaces into a common graphical interface for all new applications developed and most of those currently existing
- introducing client/server and associated object-oriented technologies.

Phase 2 involves replacing the VAX cluster, upgrading the network to handle high image transmission loads and fully re-engineering existing applications where such upgrading is shown to be economically viable.

### *Purpose of evaluation*

To test the extent to which the outcomes flowing from the activities specified above are achieved.

### *Key issues*

The key issues to be addressed are identified in the statement of outcomes and their evaluation could be phased as follows:

- introduction of PC workstations and replacement of the electronic mail system—1st quarter of 1997
- standardisation of user interface—3rd quarter 1997
- introduction of client/server and object oriented technologies—3rd quarter 1998.

### *Steering committee*

The steering committee will be chaired by the ASIO SES Band 1 officer responsible for engineering and systems development and will comprise another SES Band 1 officer (chairing a committee of client managers) together with an SES level officer from outside the Organization.

## E: Public access to ASIO's records

Researchers and other members of the public can apply to the Australian Archives for access to ASIO records that fall into the open access period of being at least 30 years old. Records may consist of file papers, photographs or cine film.

Under provisions of the *Archives Act 1983*, ASIO may seek exemption from releasing material if it would, or could reasonably be expected to:

- reveal modus operandi
- prejudice current operations
- reveal the identity or existence of past or current sources, agents and ASIO officers
- endanger foreign liaison.

The task of finding material requested and scrutinising it to remove any sensitive information is time consuming, even when aided by technology. In recent years ASIO has liaised more with the people applying for release of records, and has found that gaining a better understanding of their interests and needs helps considerably in locating the material they want.

Generally the highest priority is given to requests from the public seeking records relating to themselves or their immediate family. Next in priority come occasional or less complex requests from researchers. We also give priority to requests from other commonwealth agencies preparing to release material that includes ASIO information. This material is assessed using the same criteria as we apply to our own records. Large and backlogged requests are addressed as the workload permits. During the year, in spite of an increase in requests, we succeeded in reducing a backlog of 202 to 143.

In 1995–96 we received 270 requests covering 1121 subjects of interest. Of these requests all but 28 were serviced within 90 days. Table 23 shows the general trend of continuous improvement in servicing requests.

*Table 23: Trend in servicing public requests for ASIO records 1991–92 to 1995–96*

	1991–92	1992–93	1993–94	1994–95	1995–96
Number of requests	403	317	241	221	270
Percentage serviced within 90 days	15.4%	26.8%	82.5%	85.0%	89.6%



Applicants dissatisfied with the exemptions claimed by ASIO can request an 'internal reconsideration', in accordance with the Archives Act. During the year 29 internal reconsiderations were conducted.

If applicants are dissatisfied with the result of an internal reconsideration, they may appeal to the Administrative Appeals Tribunal (AAT). In 1995–96 three appeals were lodged with the AAT. One of these was withdrawn by the appellant at the preliminary hearing stage, with the remaining two appeals scheduled for hearing in August 1996.

## **F: Program and notional breakdown of expenditure**

Table 24 and Table 25 are excluded from the unclassified *Report to Parliament*.

## G: Significant threat assessments

*Table 26: Significant visits to Australia for which threat assessments were issued in 1995–96*

Date of Visit	Visitor
29 Jul–4 Aug 1995	Secretary-General of the Socialist Republic of Vietnam, SRV, Mr Do Muoi
18–23 Aug 1995	President of Philippines, Fidel Ramos
23–28 Aug 1995	Minister for Defence and Security, Indonesia, General Edi Sudradjat
24 Aug–7 Sep 1995	His Holiness, Pope Shenouda III, Coptic Orthodox Patriarch
9–16 Oct 1995	Their Imperial Highnesses, Prince and Princess Akishino of Japan
13–15 Oct 1995	Prime Minister of Fiji, Major-General Sitiveni Rabuka
23–30 Oct 1995	Vice-Chairman of State Planning Commission, People's Republic of China, (PRC), Zeng Peiyan
24–30 Oct 1995	Minister for Commerce and Industry, Kuwait, Mr Al-Mutairi
2–9 Nov 1995	Prime Minister of Malta, Mr Eddie Fenech Adami
4–12 Nov 1995	Minister for Youth and Sport, Malaysia, Dr Dato Haji Muhyiddin Yasin
10–14 Nov 1995	His Royal Highness, Prince Edward
11–15 Nov 1995	Former US Secretary of State, Dr Henry Kissinger
13–14 Nov 1995	Minister for Foreign Affairs, Sri Lanka, Mr Lakshman Kadirgamar
14–16 Nov 1995	Prime Minister of Canada, Mr Jean Chretien
17–25 Nov 1995	Former British Prime Minister, Baroness (Lady) Thatcher
19–25 Nov 1995	Foreign Minister of Cambodia, Mr Ung Huot
21–25 Nov 1995	Foreign Minister of Cuba, Mr Roberto Robaina
28 Jan–2 Feb 1996	Deputy Prime Minister of Solomon Islands, the Honourable Danny Philip
29 Feb–6 Mar 1996	Chairman of the Ho Chi Minh City People's Committee, Vietnam, Mr Truong Tan Sang
7–16 Mar 1996	Minister of State, Ireland, Ms Avril Doyle
20 Mar 1996	Prime Minister of New Zealand, Mr Jim Bolger
25–29 Mar 1996	Prime Minister of Malaysia, Dr Mahathir bin Mohamad
8–12 May 1996	US Secretary of Navy, Mr John Dalton
12–14 May 1996	Prime Minister of Papua New Guinea, Sir Julius Chan
20–26 May 1996	President of Palau, His Excellency Kuniwo Nakamura
2–8 Jun 1996	Minister of Trade, the Netherlands, Mrs Van Dok

*Table 27: Significant Australian overseas visits for which threat assessments were issued in 1995–96*

<b>Date</b>	<b>Visitor</b>
September 1995	Minister for Human Services and Health, Dr Lawrence, visit to Beijing for the UN World Women's Conference  Prime Minister, Mr Keating, visit to Papua New Guinea for South Pacific Forum and 20th anniversary of PNG independence
November 1995	Prime Minister, Mr Keating, visit to Japan for APEC meetings
February 1996	Australian Cricket Team, trip to Sri Lanka for the World Cup
May 1996	Minister for Foreign Affairs, Mr Downer, visit to PNG
June 1996	Deputy Prime Minister and Minister for Trade, Mr Fischer, visit to the United States and South America

## H: Recommendations against entry or residence

Table 29 shows the grounds on which 16 people applying for entry to or permanent residence in Australia were given adverse security assessments during 1995–96 compared with 19 in 1994–95). An adverse security assessment constitutes a recommendation by ASIO that the agency which requested the security assessment (DIMA or DFAT) should refuse the application. In each case, a final decision rests with the requesting agency. In all but one of the cases listed, the requesting agency refused the application. In the one case which was approved, DFAT decided to grant the application on national interest grounds. Denial of permanent entry or permanent residence applies to all members of the applicant's family unit.

In the unclassified *Report to Parliament*, the national or terrorist affiliations of the applicants are excluded from the table.

*Table 29: Adverse security assessments issued to applicants for entry to or residence in Australia 1995–96*

Type of application	Affiliation [S]	Reason for ASIO adverse assessment
Temporary entry		Espionage potential
		Espionage potential
		Espionage potential
		Espionage potential
		WMD procurement
		Espionage potential
		Espionage potential
		Espionage potential
		Espionage potential
		Espionage potential
		Terrorist links
		Espionage potential with terrorist links
		Espionage potential
Permanent entry		Espionage potential
Permanent residence		Terrorist links
		Terrorist links

# Compliance index

This index is a guide to the report's compliance with the *Guidelines for the preparation of departmental annual reports*, issued by the Secretary to the Department of the Prime Minister and Cabinet. Items are marked 'na' when the requirement does not apply to ASIO because of the nature of the Organization's statutory functions, certain legislative provisions, or its status within the portfolio.

Annual report requirement	See page(s)
<b>Letter of transmission</b>	iii
<b>Aids to access</b>	
Table of contents	v
Index	98
Glossary of acronyms and abbreviations	vi
Other major documents	iv
Contact officer	iv, 101
Corporate overview	1–33
<b>Portfolio and corporate overview</b>	
Portfolio overview	na
Corporate overview	1–33
Social justice and equity	21–22, 30–31, 86–87
Internal and external scrutiny	24, 28–31
Occupational health and safety	21, 84
Freedom of information	na
Advertising and market research	19
<b>Program performance reporting</b>	35–54
<b>Staffing overview</b>	19–23
<b>Financial statements</b>	55–76
<b>Financial and staffing resources summary</b>	81–83
<b>Portfolio bodies</b>	na
<b>Social justice and equity</b>	
Equal employment opportunity	22, 86–87
Access and equity	21, 30–31

Annual report requirement	See page(s)
<b>Staffing matters</b>	
Performance pay	22, 83
Training	19–21, 84
Interchange program	na
<b>Financial matters</b>	
Claims and losses	54
Purchasing	54
Information technology purchasing arrangements	54
Payment of accounts	54
Consultancy services	54, 85
Capital works management	54
<b>Internal and external scrutiny</b>	
Fraud control	24
Reports by the Auditor-General	30
Inquiries by Parliamentary Committees	30
Comments by the Ombudsman (see Inspector-General of Intelligence and Security)	29
Decisions of courts and tribunals	30, 46
<b>Privacy</b>	
<b>Environmental matters</b>	
<b>Other matters</b>	
Property usage	54
Business regulations	na

# General index

## **a**

abbreviations and acronyms (list) vi  
accountability 11, 21, 28–31  
Administrative Appeals Tribunal 11, 30, 90  
adverse security assessments 43–46, 95  
advertising (recruitment) 24  
annual report 28, 32  
appeal mechanisms  
    public 31  
    staff 31  
Archives Act 31, 90  
Asia subprogram 37  
ASIO's  
    management structure 7  
    records, public access to 31, 90  
    special powers iv, 29  
audio counter-measure testing 48  
audit (of ASIO accounts) 30, 57–59  
Audit and Evaluation Committee 24  
Australian, Pacific, Europe and Americas  
    (APEA) subprogram 37  
aviation interests, threats to 41

## **b**

benchmarking 23, 24

## **c**

client relations 12–14  
commonwealth holders of high public office 13  
competencies 19  
compliance index 96  
consultants 54, 85  
Consultative Committee on Security Intelligence 12, 15  
continuous improvement 9, 23, 26  
Cook Inquiry 6  
corporate plan 6  
Corporate Support Program 53

counter proliferation 5, 41  
counter terrorism exercises 52  
Counter Terrorism Support Program 51–52

## **d**

Director-General of Security iii, iv, 21, 22, 28, 29  
Disciplinary Appeal Board 31

## **e**

economic espionage 5, 14  
efficiency bonus 22  
encryption 17  
equal employment opportunity (EEO) 22, 86  
equipment testing 48  
ethics 21, 28  
evaluations 24, 88–89  
extreme nationalist militias 3  
expenditure, by program 92

## **f**

foreign intelligence activity 5  
Foreign Intelligence Collection Program 37, 50  
foreign interests in Australia 13–14, 41  
foreign liaison 15–16  
Fortnightly Digest 39  
fraud control 24–25

## **g**

Generalist Intelligence Officers 19  
global monitoring 25–26  
Grievance Review Committee 31  
grievances 22, 31

## **h**

Health Week 21



## **i**

incidental foreign intelligence 14, 40  
industrial democracy 21  
information management 18  
information technology 17  
Inspector-General of Intelligence and Security 21, 29, 30  
intelligence reporting 12–13, 39–40  
investigation methods 39

## **j**

Joint Intelligence Group (JIG) 51

## **k**

language database 16  
liaison with  
    Australian authorities 15, 16, 52  
    overseas services 15–16, 17, 80  
library 18  
linguists 16  
Loyal Regiment of Australian Guardians 4

## **m**

Middle East and Africa (MEA) subprogram 37  
mission statement iv

## **n**

National Anti-Terrorist Plan 51  
National Intelligence Group (NIG) 51  
National Security Committee 28  
nuclear, chemical and biological weapons 5, 40, 41, 95

## **o**

OASYS (office automation systems) 17, 88, 89  
occupational health and safety (OH&S) 21–22, 84  
Olympic Games 4, 51  
Ombudsman  
    ASIO 31  
    Commonwealth 21  
overseas communications link 16, 18, 25

## **p**

Parliamentary Joint Committee (PJC) on ASIO 30  
performance pay 22, 83  
politically motivated violence 41–42  
Port Arthur shootings 4  
program and notional breakdown of expenditure 92  
program outcomes (summary) 38  
proliferation 5, 41  
Promotion and Transfer Appeal Committee 31  
protective security advice 14, 47  
Protective Security Program 43–46  
Protective Services Co-ordination Centre 15  
protest activity iv, 4, 42  
publications about ASIO 32  
published intelligence reports 39–40

## **q**

qualified security assessment 11, 43–46

## **r**

recruiting 19, 26, 32  
risk management 14, 40, 47, 48  
risk management 14, 40  
Rushdie, Salman 4

## **s**

SAC-PAV 41, 51  
science and technology 5, 14, 41  
screening for entry or permanent residence 43–45  
scrutiny mechanisms 28–31  
Security and Counter Intelligence Division 6  
security assessments 30, 43–47, 95  
security awareness raising 48  
security clearances 45–47  
Security Appeals Tribunal 46  
security inquiry 6  
security intelligence planning 6  
Security Intelligence Program 16, 37, 39–42, 88  
Security intelligence reporting 12–13, 14, 39–40  
SIDC-PAV 40, 51

special powers (of ASIO) iv, 29  
Specialist Intelligence Officers 19  
staff development 20–21  
strategic planning 6

## **T**

tabled reports (on ASIO) 30  
technology exchange 17  
threat assessments 5, 13, 15, 40, 41–42, 51, 93  
traineeships 19, 21  
training 20–21, 54, 84

## **V**

visa checking 5, 43–47, 95  
visitor entry system 4

## **W**

warrants 29–30  
weapons of mass destruction 5, 40, 41, 95  
Wood Inquiry 13  
workplace bargaining 21, 22, 26  
world security scene 3

# ASIO contact information

## **Written inquiries**

The Director-General  
Central Office  
GPO Box 2176  
CANBERRA ACT 2601

## **General inquiries**

Central Office switchboard  
(toll-free number) 1800 020 648

## **Media inquiries**

Media Liaison Officer      (06) 249 8381

## **Collection office inquiries**

Australian Capital Territory	(06) 249 7415
Victoria	(03) 9654 8985
New South Wales	(02) 9281 0016
Queensland	(07) 3221 7157
South Australia	(08) 8223 2727
Western Australia	(09) 221 5066
Northern Territory	(08) 8981 2374

Tasmanian residents may call  
Canberra Central Office toll-free    1800 020 648

