Commission of Inquiry into the 
Australian Secret Intelligence Service

Report on 
the Australian Secret 
Intelligence Service

Public Edition

MARCH 1995
Commission of Inquiry into the Australian Secret Intelligence Service

Report on the Australian Secret Intelligence Service

Public Edition

MARCH 1995
NOTE ON PUBLIC EDITION


In presenting their 3-volume, 33-chapter Report to Government, the Commissioners recommended public release in whole or substantial part of 15 chapters of that Report. They described their approach in the following terms:

In preparing our more detailed secret report, we took account of evidence presented to us by ASIS and other Government witnesses advocating the potential value of more authorised material, without operational sensitivity, being made available publicly about the accountability and control arrangements within which ASIS operates.

We were also conscious of the potential value, in relation to our third term of reference dealing with protection of sources and methods, of publishing material which might set an appropriate framework for parliamentary (and associated public) debate on these matters. Such publication may facilitate consultation between the Government and media representatives, if the Government wishes to reinvigorate the D Notice system as we recommend.

Accordingly, the chapters we have prepared which bear on these matters have been constructed, so far as we have been able to manage, in a way which would facilitate public release should the Government wish to do so.

We have taken the view, also, that the matters meriting wider release are topics of principle and structure likely to attract parliamentary and public consideration, rather than matters of administrative detail or management practice.

On those administrative matters and on the individual grievance cases we considered, we regard our discussion in the proposed Public Report as appropriate and sufficient for public dissemination.

Finally, we are mindful that material which relates to agencies of other countries and which is not on the public record cannot appropriately be released by the Australian Government.

This Public Edition contains the fifteen chapters identified by the Commissioners as appropriate for release, edited to delete national security sensitive material. The chapters, pages and paragraphs of the full report have been renumbered to the extent necessary to achieve presentational continuity.

While the Commissioners did not recommend release of those chapters considering the administrative practices of ASIS, nor those containing detailed consideration of individual grievance cases brought by former ASIS officers, some discussion of these matters was contained in the 18 page summary Public Report prepared by the Commissioners and tabled in the Parliament on 24 April 1995.
# Contents

Note on Public Edition ......................................................................................... iii

Contents ................................................................................................................ v

Acronyms and Abbreviations ............................................................................... xiii

Preface .................................................................................................................. xvii

Public Report .......................................................................................................... xix

Chapter 1 - Introduction ....................................................................................... 1

The functions of ASIS ......................................................................................... 1

The Royal Commission on Intelligence and Security – the first Hope Report ........................................................................ 2

The move to Canberra ......................................................................................... 3

The Royal Commission on Australia’s Security and Intelligence Agencies – the second Hope Report ........................................................................ 4

Report on the Australian intelligence community in a changing international environment – the Richardson Report ........................................................................ 4

Intelligence collection in a more complex world – the Hollway Report ........................................................................ 5

The present inquiry .............................................................................................. 5

Chapter 2 - The Accountability Framework ...................................................... 10

The meaning of accountability ............................................................................ 10

The existing framework ...................................................................................... 11

The accountability of ASIS within the executive government ......................... 12

The Directive ......................................................................................................... 12
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The case for formal briefings</td>
<td>39</td>
</tr>
<tr>
<td>Chapter 5 - Parliamentary Scrutiny</td>
<td>42</td>
</tr>
<tr>
<td>Accountability and responsible government</td>
<td>42</td>
</tr>
<tr>
<td>Secrecy and ministerial responsibility</td>
<td>44</td>
</tr>
<tr>
<td>Overseas comparisons</td>
<td>45</td>
</tr>
<tr>
<td>The United States</td>
<td>45</td>
</tr>
<tr>
<td>The United Kingdom</td>
<td>48</td>
</tr>
<tr>
<td>Canada</td>
<td>48</td>
</tr>
<tr>
<td>The ASIO committee</td>
<td>49</td>
</tr>
<tr>
<td>A parliamentary committee for ASIS</td>
<td>50</td>
</tr>
<tr>
<td>The case for a parliamentary committee</td>
<td>54</td>
</tr>
<tr>
<td>Committee oversight models</td>
<td>56</td>
</tr>
<tr>
<td>The UK model</td>
<td>56</td>
</tr>
<tr>
<td>Committee for ad hoc inquiries</td>
<td>57</td>
</tr>
<tr>
<td>The ASIO Committee model</td>
<td>58</td>
</tr>
<tr>
<td>A standing, joint, statutory committee with a broad charter</td>
<td>58</td>
</tr>
<tr>
<td>Features of the preferred model</td>
<td>59</td>
</tr>
<tr>
<td>A single intelligence and security committee</td>
<td>59</td>
</tr>
<tr>
<td>Powers, functions and access</td>
<td>61</td>
</tr>
<tr>
<td>Membership and staffing</td>
<td>62</td>
</tr>
<tr>
<td>Initiation of inquiries</td>
<td>63</td>
</tr>
<tr>
<td>Other provisions</td>
<td>63</td>
</tr>
<tr>
<td>Chapter 6 - The Minister, the Director-General and the Directive</td>
<td>64</td>
</tr>
<tr>
<td>Changes in the relationship between the Minister and the Director-</td>
<td>64</td>
</tr>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>The role of the Minister and the Department</td>
<td>67</td>
</tr>
<tr>
<td>Direct ministerial control</td>
<td>67</td>
</tr>
</tbody>
</table>

vii
Annual report and corporate plan .................................................................68
The role of the Department ........................................................................69
The Directive in the control of ASIS ............................................................69
Chapter 7 - Cabinet and Official Control ....................................................71
  Security Committee of Cabinet ................................................................71
  Secretaries Committee on Intelligence and Security ...............................73
  Control and oversight ...............................................................................76
  Annual reports and budgets .....................................................................76
  Intelligence priorities ...............................................................................77
  The Richardson and Hollway reviews ....................................................78
  Conclusion ...............................................................................................78
Should ASIS be part of SCIS? ....................................................................79
National Intelligence Committee ...............................................................81
Heads of Intelligence Agencies Meeting ....................................................82
Chapter 8 - Tasking .....................................................................................84
  Introduction ..............................................................................................84
    The Hope Royal Commissions ..............................................................84
    The Richardson and Hollway reviews ..................................................85
  National Intelligence Collection Requirements Committee ...................86
  Direct tasking of ASIS .............................................................................89
    Improving customer liaison ....................................................................89
    Tasking and customer feedback ............................................................90
Chapter 9 - Oversight by the Inspector-General of Intelligence and Security ..........................................................................................................................93
  The role first envisaged for the Inspector-General ......................................93
  The jurisdiction and powers assigned to the Inspector-General ...............95
  How oversight by the Inspector-General has developed ............................96
How the Inspector-General should oversee ASIS.................................99
Monitorsing of ASIS dealings with information on Australians.........................103
The gap in assurance.................................................................................104
Chapter 10 - The Protection of Sources and Methods............................106
What should be protected?.....................................................................106
The mechanics of protection..................................................................110
Chapter 11 - The D Notice System.......................................................113
The present system..................................................................................113
Revitalising the system..........................................................................114
A new Notice and a new committee......................................................118
Reviewing the ASIS D Notice.................................................................119
ASIS media liaison officer.......................................................................123
Chapter 12 - Civil Remedies to Prevent Unauthorised Disclosures........125
Background............................................................................................125
The existing remedies............................................................................126
Proposals for law reform.........................................................................130
Substantive law.........................................................................................130
Procedural mechanisms.........................................................................132
Conclusion...............................................................................................134
Chapter 13 - Criminal Sanctions Against Publication.........................135
The existing provisions: Crimes Act ss.70 and 79....................................135
Criticisms of the existing provisions.....................................................136
The Gibbs Committee recommendations..............................................139
A whistleblower scheme........................................................................140
Proof of damage......................................................................................142
Defence of prior publication...................................................................146
Defence of public interest ................................................................. 147
Secondary disclosures ........................................................................ 149
Identification of individuals: a mirror provision to ASIO Act s.92? ....152
Secrecy provisions in ASIS legislation ............................................. 154

Chapter 14 - Complaints and Grievances : External Review .............. 155
Inquiries into complaints and grievances .............................................. 155
The power to inquire ........................................................................ 156
The value of inquiries into complaints and grievances .................. 157
The experience of complaints and grievances ................................ 158
Public complaints ........................................................................... 161

Inquiries into grievances .................................................................. 162
The experience with ASIS grievances .............................................. 165
The need for determinative power .................................................... 166
A new review body? ....................................................................... 169

Chapter 15 - The Public Face of ASIS .............................................. 173
The ASIS approach: the blanket of secrecy ...................................... 174
The media approach: ‘a good story’ ................................................. 176
The ASIS assassin ........................................................................... 177
The CIA assassin ........................................................................... 179
The ASIS fire .................................................................................. 179
‘Tens of thousands of files’ ............................................................... 180
Listings ........................................................................................... 182
Persons of operational interest ....................................................... 182
Staff ............................................................................................... 183
Persons of security interest ............................................................. 183
The need for verification .................................................................. 185
Alternative approaches to media relations ..............................................185

UK Secret Intelligence Service .............................................................187

US Central Intelligence Agency .........................................................187

A new approach for ASIS .................................................................188

The policy of 'neither confirm nor deny' .............................................192

A public information strategy ............................................................193

Conclusion ..........................................................................................195

Appendix A - Letters Patent ..................................................................197
## Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAT</td>
<td>Administrative Appeals Tribunal</td>
</tr>
<tr>
<td>ABC</td>
<td>Australian Broadcasting Corporation</td>
</tr>
<tr>
<td>ADG</td>
<td>Assistant Director-General</td>
</tr>
<tr>
<td>AFP</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>AG's</td>
<td>Attorney-General's Department</td>
</tr>
<tr>
<td>AGPS</td>
<td>Australian Government Publishing Service</td>
</tr>
<tr>
<td>AISA</td>
<td>Australia's Security and Intelligence Agencies</td>
</tr>
<tr>
<td>ANAO</td>
<td>Australian National Audit Office</td>
</tr>
<tr>
<td>APS</td>
<td>Australian Public Service</td>
</tr>
<tr>
<td>ASIO</td>
<td>Australian Security Intelligence Organisation</td>
</tr>
<tr>
<td>ASIS</td>
<td>Australian Secret Intelligence Service</td>
</tr>
<tr>
<td>ASL</td>
<td>Average Staffing Level</td>
</tr>
<tr>
<td>CDFS</td>
<td>Chief of the Defence Force Staff</td>
</tr>
<tr>
<td>CI</td>
<td>Counter-Intelligence</td>
</tr>
<tr>
<td>CIA</td>
<td>Central Intelligence Agency</td>
</tr>
<tr>
<td>CIP</td>
<td>Counter-Intelligence and Proliferation</td>
</tr>
<tr>
<td>CSIS</td>
<td>Canadian Security Intelligence Service</td>
</tr>
<tr>
<td>DDG</td>
<td>Deputy Director-General</td>
</tr>
<tr>
<td>DFA</td>
<td>Department of Foreign Affairs</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>DFAT</td>
<td>Department of Foreign Affairs and Trade</td>
</tr>
<tr>
<td>DG</td>
<td>Director-General</td>
</tr>
<tr>
<td>DIO</td>
<td>Defence Intelligence Organisation</td>
</tr>
<tr>
<td>DIR</td>
<td>Department of Industrial Relations</td>
</tr>
<tr>
<td>DSD</td>
<td>Defence Signals Directorate</td>
</tr>
<tr>
<td>EAP</td>
<td>Employment Assistance Program</td>
</tr>
<tr>
<td>EEO</td>
<td>Equal Employment Opportunity</td>
</tr>
<tr>
<td>FIC</td>
<td>Foreign Intelligence Collection</td>
</tr>
<tr>
<td>FIPD</td>
<td>Foreign Intelligence Planning Document</td>
</tr>
<tr>
<td>GCHQ</td>
<td>Government Communications Headquarters (UK)</td>
</tr>
<tr>
<td>HIAM</td>
<td>Heads of Intelligence Agencies Meeting</td>
</tr>
<tr>
<td>IGIS</td>
<td>Inspector-General of Intelligence and Security</td>
</tr>
<tr>
<td>JCPA</td>
<td>Joint Committee on Public Accounts</td>
</tr>
<tr>
<td>JIO</td>
<td>Joint Intelligence Organisation</td>
</tr>
<tr>
<td>MAB</td>
<td>Management Advisory Board</td>
</tr>
<tr>
<td>MIAC</td>
<td>Management Improvement Advisory Committee</td>
</tr>
<tr>
<td>MPRA</td>
<td>Merit Protection Review Agency</td>
</tr>
<tr>
<td>NCND</td>
<td>'Neither Confirm Nor Deny'</td>
</tr>
<tr>
<td>NFIAP</td>
<td>National Foreign Intelligence Assessment Priority</td>
</tr>
<tr>
<td>NIC</td>
<td>National Intelligence Committee</td>
</tr>
<tr>
<td>NICRC</td>
<td>National Intelligence Collection Requirements Committee</td>
</tr>
<tr>
<td>NISC</td>
<td>National and International Security Committee</td>
</tr>
<tr>
<td>ONA</td>
<td>Office of National Assessments</td>
</tr>
<tr>
<td>OSIC</td>
<td>Office of Security and Intelligence Coordination</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PM&amp;C</td>
<td>Department of the Prime Minister and Cabinet</td>
</tr>
<tr>
<td>PSC</td>
<td>Public Service Commission</td>
</tr>
<tr>
<td>RCASIA</td>
<td>Royal Commission on Australia's Security and Intelligence Agencies</td>
</tr>
<tr>
<td>RCIS</td>
<td>Royal Commission on Intelligence and Security</td>
</tr>
<tr>
<td>SCC</td>
<td>Service Consultative Council</td>
</tr>
<tr>
<td>SCIS</td>
<td>Secretaries Committee on Intelligence and Security</td>
</tr>
<tr>
<td>SCOC</td>
<td>Security Committee of Cabinet</td>
</tr>
<tr>
<td>SES</td>
<td>Senior Executive Service</td>
</tr>
<tr>
<td>SIRC</td>
<td>Security Intelligence Review Committee (Canada)</td>
</tr>
<tr>
<td>SIS</td>
<td>Secret Intelligence Service (UK)</td>
</tr>
<tr>
<td>SWA</td>
<td>Staff Welfare Association</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>
Preface

The work of the Inquiry has been much assisted by all those who have provided evidence to us, including those who attended hearings as witnesses.

We owe a considerable debt of gratitude to our Counsel Assisting, Mr Christopher Maxwell, our Instructing Solicitor, Mr Brian McMillan, our Inquiry Secretary, Ms Barbara Belcher, and to all of the staff in our Inquiry Secretariat, for their cheerful, efficient and devoted cooperation.

The Honourable Gordon J Samuels AC QC
Michael H Codd AC

31 March 1995

Note: In our Report, we have adopted some presentational conventions. Where an organisation is first mentioned in each chapter, we use its title: then we use its initials our acronym: and we have preserved a single well-recognised acronym for a single entity, regardless of changes of its name over the period with which we deal (so that DFAT could, in context, mean the Department of Foreign Affairs or the current Department of Foreign Affairs and Trade). Similarly, we have adopted for ease of reference a consistent rather than a strictly verbatim approach to the presentation of material quoted, spelling out in full many internal acronyms, and standardising references, particularly to individuals.
This is a summary account of the major aspects of the inquiry and of
the principal recommendations, from which all sensitive material has been
excluded*.

The functions of ASIS

2. In 1977 the Australian Secret Intelligence Service (ASIS), established by
executive direction on 13 May 1952, was publicly acknowledged by the
Government as Australia’s foreign intelligence agency. It is responsible for the
cover foreign intelligence collection of which the Prime Minister spoke in his
Because of their sensitivity, details of its operations are not revealed.

3. Secret foreign intelligence is of continuing significance to Australia. It
represents a valuable element in the advancement of Australia’s policies and in
the protection of its security. It provides vital information in areas such as
nuclear policy, arms control and defence capacity. The collection of such secret
material depends on people who often put their lives and liberties at
considerable risk. It is for that reason that secrecy about operations and the
people engaged in them is necessary in the national interest.

4. The disclosure of information about operational matters, whether true,
partly true or false, can prejudice the effective performance of the collection
function and thereby threaten Australia’s national interests as well as the
physical safety of the individuals involved.

The genesis of the Inquiry

5. During 1993 and early 1994 the media published a number of stories
about ASIS, disclosing what purported to be details of certain of its operations
and the locations in which they had been carried out. These articles were

* This summary public report was tabled in the Parliament on 24 April 1995.
uniformly critical of ASIS, asserting various examples of operational and administrative inefficiency. They substantially reproduced, or were based upon, information supplied by two former officers of the Service and the wife of one of them. Their general tenor was that ASIS was uncontrolled and unaccountable, pursued its own objectives (albeit only incompetently) without any adequate external guidance or restraint, and was contemptuous of the needs and well-being of its own officers.

6. This series of disclosures by the media culminated in a *Four Corners* program on 21 February 1994. The two former officers and the wife appeared in it, with their features lightly obscured to hinder recognition, and they made (in some instances repeated) a number of allegations of the kind described above. Although information published in the *Four Corners* program on operational matters was skewed towards the false, evidence presented to us of action and reaction in other countries satisfies us that the publication was damaging.

**The Inquiry is established**

7. On 23 February 1994, Senator Gareth Evans, the Minister for Foreign Affairs, and as such the Minister responsible for ASIS, announced that the Government had decided to set up a judicial inquiry ‘into the operations and management of ASIS’. Its terms of reference were -

(a) to inquire into the effectiveness and suitability of existing arrangements for -

(i) the control and accountability of ASIS;
(ii) the organisation and management of ASIS;
(iii) the protection of ASIS intelligence sources and methods;
(iv) the resolution of grievances and complaints relating to ASIS; and

(b) to consider whether any changes in existing arrangements are required or desirable.

8. The Minister indicated that it was not proposed that the Inquiry should address ‘the functional role and priorities of ASIS’. Nevertheless, in the course of examining other matters within our terms of reference it has proved necessary to consider the Service’s professional reputation.
The proceedings of the Inquiry

9. The Inquiry held its initial sitting in public on 2 May 1994. Thereafter it has sat in camera. It conducted hearings on 67 days between 2 May and 13 December 1994 and took evidence from 89 witnesses, alone or in groups. Commissioners also visited ASIS establishments and held discussions with staff in the course of those visits. Commissioner Samuels held discussions in the United Kingdom, the United States and Canada with relevant intelligence and security organisations and officials from those countries, and with some Australian officials. The Commission has not released any transcript of the evidence which it has taken, or any copies of the many exhibits it has admitted, save for the edited transcripts of hearings at which media representatives gave evidence. These were published on 21 February 1995 in order to promote discussion in the media about various aspects of the treatment of sensitive information, which we await with the keenest anticipation. We consider that there are parts of our full report which should remain secret, but other substantial parts which, with some editing, could usefully be published in addition to this summary account. We have recommended this course to the Government.

The reasons for the Inquiry

10. The reasons for establishing the Commission of Inquiry were said (on 28 February 1994 by the Minister) to be the perception of the Government that there was a normative case for periodic root and branch review of secret organisations, and a wish, in view of the end of the Cold War and the recent expansion of ASIS, to consider the desirability of a legislative charter and the adequacy of existing management systems and protection mechanisms. The genesis of that wish appears to have fortuitously coincided with the culmination, in the *Four Corners* program, of the staged campaign which the former officers had undertaken in order to bring escalating pressure to bear on ASIS to remedy their various complaints.

11. It is probably true to say that had it not been for the disclosures made by the former officers to the media (and in particular to *Four Corners*) the inquiry would not have been established. On that assumption the media played a prominent role - by publishing what they were told - in procuring the investigation which the Commission has conducted.
The reasons for the disclosures

12. Both the former officers who appeared on the *Four Corners* program admitted to us that their disclosure of sensitive information which they ought to have kept secret represented a serious breach of the promises of confidentiality which they had made to ASIS. But they sought to justify their conduct not only as the sole means remaining to them of achieving their individual goals of personal vindication and financial compensation, but also of forcing on the Government an inquiry into the Service. This, it was said, was necessary to expose serious tactical and managerial ineptitude, and to reveal grave shortcomings in the direction, control and accountability of ASIS. Finally, it was put to us that since the Inquiry had been established and would presumably produce beneficial results, their actions had 'redeeming social value'.

13. We do not think that the 'means and ends' argument, which attempts to weigh the detection and correction of supposed error or abuse against serious breaches of confidentiality which themselves have produced actual damage, constitutes a legitimate calculus. The test we have formulated is that it was incumbent upon those former officers who had made public disclosure of information which it was their duty to keep secret, to show that they believed on reasonable grounds that the disclosure was made in the public interest. To rephrase that test in the context of present circumstances, it was necessary for them to establish that the disclosure was necessary to provoke the only, or the most effective, means of investigating and remedying deficiencies which required urgent attention.

The disclosures examined

14. The disclosures made by the former officers in the course of their campaign fall broadly into two categories. First, they alleged general deficiencies and irregularities in the Service's operational methods and activities. Secondly, they complained of personal injustice, and of procedural unfairness inflicted upon them in consequence of defects in the Service's internal management procedures.

The general allegations

15. The *Four Corners* program contained disclosures in both categories; with the allegations about operational matters included no doubt for their dramatic content and in order to focus attention upon the individual complaints. We have investigated them all, together with the assertions made in other media.
outlets. To take the *Four Corners* program as an example, the introduction promised stories of 'Australia's disturbing secret involvement in wars, coups and political intrigue'. But the level of factual accuracy about operational matters was not high - neither here nor in other media reports. Indeed, to paraphrase a book review attributed to A E Houseman, 'what was disturbing was not true, and what was true was not disturbing'. We have discovered no evidence capable of supporting the conclusion that ASIS is operating out of control (the 'loose cannon' metaphor is well wide of the mark), or pursuing its own targets unrestrained by any government agency, or is unaccountable for the activities it undertakes or the funds it expends.

16. On the contrary its operational management is well structured and its tactical decisions are thoroughly considered and, in major instances, subject to external approval. Its operational people are skilled and discreet, and the product it gathers is well regarded by its customers and professional assessors. It does not maintain 'tens of thousands of files' containing dossiers about Australian citizens, as alleged in the media. We have absolutely no reason to suppose that, again as alleged, in November 1994 it set fire to embarrassing records so as to prejudice the work of this inquiry. It does not represent a threat to Australian democracy. We have set out in our full report the results and methodology of the detailed investigations which the Commission made and which, in our view, enable us to express these conclusions.

17. Hence the inquiry was not required in order to eradicate the more dramatic sins which have been urged against the Service, or to rectify urgently a continuing series of administrative or tactical faults likely to affect adversely the freedom of Australian citizens or Australia's relations with other nations. Our detailed examination of the matters covered by our terms of reference has led us to conclude that, in a number of respects, the control and accountability, and the internal organisation and management, of the Service could and should be improved, and we have recommended accordingly. These conclusions and recommendations do not represent a response to disorder, but rather, as we see it, a prescription for enhancement.

**The individual complaints**

18. We have devoted more time to the examination of the individual complaints than to any other single element of our inquiry. This was not only because of the history and nature of these matters, and of the influence which they have had upon the genesis of the Inquiry and upon the attitudes of the media, but because they reveal important aspects of ASIS's culture and style of
internal management. Our lengthy investigation did not reveal the gamut of inefficiency and impropriety which had been alleged. But the complaints did demonstrate that there had been significant shortcomings in the Service's internal management; and in the methods adopted within the Service to deal with allegations of misconduct.

**The complainants**

19. The complaints which we examined in detail were made by four former officers and the wife of one of them. We consider that two of the complainants failed to make good any grievance against the Service, save of the most minor kind, and we need say nothing further about them here. We have set out our findings in detail in our full report, as we have done in respect of all the complaints.

**The first complainant**

20. This officer, while posted overseas, fell out with a senior Australian official: a complete rupture occurred in the relationship between them. The officer complained to ASIS in vehement terms that the integrity of ASIS operations was being threatened. A joint team of two senior officers went to investigate the situation. They recommended that the complainant be withdrawn to Australia, and he was. In our view the investigation was procedurally flawed and the report unfairly weighted against the complainant. We consider, however, that even if the report had been better balanced and without procedural flaw, the then Director-General would probably still have decided to withdraw his officer, which was an operational choice well open in the circumstances. We do not accept the assertions of the complainant that he was 'abandoned' by the Service.

21. After his return to Australia in the mid 1980s the complainant accepted a suggestion by the then Director-General to discuss with ASIS's Director of Psychology his experiences overseas. We think it probable that the then Director-General did not intend this to furnish the occasion for the obtaining of a psychological report about the complainant without his knowledge. Following an interview of some four hours the Director of Psychology, however, supplied to the then Director-General a report about the complainant which diagnosed an abnormal or dysfunctional psychological condition. The report was never provided to the complainant. We are satisfied that the then Director-General had determined to terminate the complainant's contract before he read the psychological report which therefore had only minimal impact on his decision.
22. The complainant's separation from the Service was conducted correctly and the then Director-General acted properly in providing him with reasons for termination which he was not required to give. However, we think it clear that the complainant should have been given a copy of the psychological report, at least in discharge of the Service's duty as the complainant's employer to enable him to take such steps as he might think necessary in the light of the information conveyed to him. We do not know, of course, what response the complainant might have made to the report (when he finally saw it he regarded it as 'just plain silly'); and we of course express no view as to whether it was or was not an accurate indication of the complainant's psychological condition. It is therefore impossible to say whether the complainant suffered any detriment by having been deprived of it.

23. In June 1991 he made a complaint about the circumstances in which ASIS had withdrawn him, and a claim for compensation, to the Inspector-General of Intelligence and Security, of whose existence the complainant had only just become aware. The Inspector-General holds an independent statutory office, first created in February 1987, with power to receive and investigate complaints about ASIS and to make a report to Government in respect of them.

24. By late 1993 that complaint had not been fully dealt with and the former officer conveyed his concerns to Senator Knowles, a member of the Opposition, who sought information about his case. A briefing was provided by the Inspector-General and the Director-General of ASIS, with an officer of DFAT and an adviser to Senator Knowles also present. In the course of the briefing reference was made to the psychological report. We consider that this use of the report, however it occurred and whatever the intended purpose, was highly inappropriate. The complainant subsequently became aware of the existence of a report. He inferred that material which he had never seen but which asserted his psychological instability had been used to discredit his complaints and to deflect political support for his cause.

25. He sought to obtain a copy of the report from the Inspector-General, who had no power to provide it to him, and later from the Minister. The report was not provided, and he did not in fact see the report until July 1994 in the course of this Inquiry. We take a serious view of circumstances in which such a report was generated without his knowledge, never shown to him before he left the Service, but kept on his file and thus available to the Inspector-General, who annexed it to his final report; and then referred to in the course of the briefing of Senator Knowles; with the consequences, no doubt, which the complainant had apprehended.
26. We do not, however, regard the complainant as having been justified in disclosing the matters which he revealed, in breach of his promises of secrecy. The test is whether he satisfied us that he believed, on reasonable grounds, that he was justified in the public interest in disclosing the information. Whatever his belief may have been, we do not consider that he had reasonable grounds.

The second complainant

27. The second complainant was accompanied by his wife on an overseas posting. After their return to Australia in 1990 they were subjected to two investigations, conducted by a senior officer of ASIS, into allegations of misconduct in his case; and, in hers, of emotional and psychiatric instability, based upon little more than unauthenticated gossip. In respect of the first investigation the former officer was never told anything of the allegations which had been made about him, and the second investigation concerned complaints of an indefinite kind which were never adequately particularised. The officer’s wife was inevitably caught up in the investigations of her husband’s conduct, and was herself the subject of investigation following the publication of the wounding allegations against her, of which she was herself never directly informed. In the end, they were not substantiated, and were dismissed by the Service as ‘unproven or unfounded’. Following the second investigation, restrictions were placed by the then Director-General upon the officer’s eligibility for posting overseas. He appealed successfully to an internal Grievance Panel which recommended that the limitations on his professional deployment be lifted. However, the Panel expressed the view that in the circumstances he had no future in the Service; a conclusion which the Acting Director-General rejected, although accepting the Panel’s reversal of the results of the internal investigation.

28. We are satisfied that the officer was amply justified in accepting the conclusion of the Grievance Panel and in seeking the generous redundancy they proposed. However, he was unable to reach agreement with the Service and in 1991 he appealed to the Inspector-General who in December 1992 ultimately recommended a financial settlement which the officer and his wife accepted in April 1993. We are satisfied that they entered into the settlement without any improper pressure or inducement by the Service, although the wife may have been genuinely under the misapprehension that if she had declined to join in the settlement agreement some part of the compensation offered to her husband would have been withdrawn.
29. These events caused both the complainant and his wife considerable emotional stress over a prolonged period. The Service’s response to the allegations made against the wife was deplorable. The Director-General expressed the opinion in evidence that in the circumstances the wife was entitled to an apology for the stress and hurt caused by the investigation. We consider that an apology should be made.

30. We consider that there was no justification for the complainant’s or his wife’s breach of their various promises of confidentiality by supplying to the media, after the settlement, information which they each knew to be confidential and covered by their promises.

All complainants

31. We have recommended to the Government that all five complainants whose cases we have considered in detail should be able to see our full assessment of their complaints and our conclusions concerning them.

Control and accountability

32. It is essential that those who wish to understand how the Service works should appreciate the manner in which it is controlled and the means by which its accountability is ensured. At present the Director-General of ASIS is directly responsible to the Minister for Foreign Affairs, and is bound by the terms of a secret Directive which establishes the nature of the Service’s mission and the extent, and the limits, of the Director-General’s authority. It requires the Director-General to seek ministerial approval before the Service can undertake certain classes of operational activity. The Director-General himself must approve the initiation of tactical schemes for the collection of intelligence. Examination by the Commission’s staff, and personal scrutiny by the Commissioners, satisfies us that these procedures, and the requirement that the Minister’s or the Director-General’s approval, where necessary, be fully recorded, have been meticulously observed.

33. ASIS collects secret intelligence pursuant to the directions of the Government. Its targets and priorities are set according to the decisions of an interlocking structure of committees, headed by the Security Committee of Cabinet (SCOC) over which the Prime Minister presides. It is the responsibility of SCOC to set broad intelligence priorities, to approve guidelines for the operation of intelligence agencies and to approve significant changes in the intelligence effort. Material for this Committee is ordinarily channelled through
a supporting body of officials at head of agency level, the Secretaries Committee on Intelligence and Security (SCIS). SCIS furnishes general oversight of the Australian intelligence community (AIC) and policy guidance on behalf of SCOC to the principal departments and agencies involved in intelligence, including ASIS. Within the policy guidelines established by SCOC more specialised committees determine the broad priorities by which the intelligence collectors, both overt and covert, should focus their collection efforts. Within that framework of priorities established by this central system, ASIS may be tasked directly by policy or assessment agencies.

34. Our terms of reference do not require us to consider ASIS's performance of its operational role or whether it should be expanded, curtailed, or, indeed, abolished. Nevertheless, in considering questions of control and accountability we have necessarily paid some attention to ASIS's reputation as a collector of intelligence, and the extent to which it satisfies the requirements of its tasking and assessing agencies. Naturally we appreciate that these opinions, which were wholly favourable, are largely those of other members of the AIC. But, in these circumstances, and for this purpose, we regard them as dependable. The impression we obtained from discussions with intelligence agencies overseas was that ASIS was regarded as efficient and reliable.

35. The most important implication for present purposes of the manner in which ASIS is tasked to collect intelligence is that its tasking and its priorities are established for it by others and are not self-selected. This is a powerful rejoinder to any arguments that ASIS is free to pursue such intelligence efforts as it pleases, without the approval, or even the knowledge, of other agencies or the executive government. We do not consider that frolics of this kind would be feasible within the present framework and arrangements for the exercise of control. We are satisfied that the committees which deal closely with ASIS, and on which the Service is itself represented, and which are responsible for tasking and setting priorities, operate in a thoroughly professional manner and with a proper awareness of their responsibilities. Moreover, ASIS's internal operational procedures and the rotation of tasks among its officers, both overseas and in Australia, would make it impossible to conceal illicit operational activity.

**Recommendations for enhancement**

**Legislation**

36. One of the specific matters which it was contemplated that this Inquiry should consider was whether ASIS should be provided with a legislative charter.
There are arguments both for and against the provision of a statutory basis. We are, however, very firmly of the view that legislation to affirm ASIS’s existence and to provide authority for its activities is desirable in principle and will be of benefit in practice. ASIS carries out important functions in the national interest. Its operations are usually sensitive and potentially controversial. It is no longer appropriate that the authority for the exercise of these functions should be conferred exclusively by the executive arm of government. It is appropriate that, in a parliamentary democracy, the existence of an agency such as ASIS should be endorsed by the Parliament and the scope and limits of its functions defined by legislation. Accordingly, we recommend that legislative authority be furnished to the Service, and we have annexed to our report a draft bill which defines the functions of ASIS, and which also specifies that in performing its functions it must not ‘use force or lethal means; or provide training in the use of force or lethal means’. We do not suggest that in its intelligence operations it has ever used such methods.

37. Our recommendation in favour of legislation should not be taken to imply that the present arrangements for accountability have failed. All the evidence is, as we have already indicated, that ASIS has been carefully managed and responsive to the direction of successive governments. We consider, however, that the move from executive to legislative authority would add a significant new dimension to the accountability framework, bringing with it qualities of legitimacy and transparency which the Service needs. The enactment of legislation should serve to reassure the public, in a way that statements by the Minister or the Director-General cannot do, that the activities of ASIS are properly authorised and controlled; and the legislation should help to dispel the persistent mythology that the Service is unaccountable and out of control.

38. The Service itself through the Director-General has expressed the view that a statutory basis for ASIS ‘would enhance both the sense and the reality of its accountability’. We appreciate that one consequence of legislation may be to heighten public expectations of complete transparency which, in the nature of things, cannot be satisfied.

A new role for the Inspector-General

39. We have no reason, as we have said, to conclude that current arrangements for control of ASIS are defective. However, we recommend the adoption of a system of retrospective auditing of the Service’s compliance with Australian law and with approved rules and operational procedures. We have discussed elsewhere in the Report the type of audit we propose. It should be
undertaken by the Inspector-General, will not hamper ASIS in the conduct of its operational activities, and will furnish further assurance to the Minister, and to a parliamentary committee if our recommendation in the report is accepted, that the rules are being followed and the procedures applied.

A parliamentary committee for ASIS

40. As the Minister pointed out, it does not follow that the acceptance of legislation for ASIS entails acceptance of a parliamentary oversight committee. Nevertheless, if the Parliament is to approve ASIS’s charter by lending it statutory authority, the Parliament should also be able to review the manner in which that authority is exercised. A parliamentary committee represents one way in which that scrutiny might be performed.

41. Parliamentary oversight through a special committee is the appropriate vehicle for ASIS because of the sensitivity of the issues involved and the associated need to ensure the security of information provided. The government could not, in practice, share much of the information necessary to accountability with the whole Parliament nor could that information be published. Under appropriate security arrangements, however, a committee could be provided with fuller information. Oversight by a committee would, moreover, be consistent with the general approach to public sector accountability in Australia and in other parliamentary democracies.

42. There are, we think, a number of possible models ranging from the committee of parliamentarians established by the British Parliament to the Joint Statutory Committee for which the ASIO Act provides. That committee is, however, unable to initiate its own inquiries.

43. We prefer the establishment of a standing parliamentary joint committee with a broad charter enabling it to review the activities, expenditure and administration of ASIS. It would be able to initiate its own inquiries, but not into operationally sensitive matters. The committee would exercise its functions principally through the medium of hearings in camera. It would have sufficient access to information to assure effective oversight, but under secure conditions designed to maintain operational integrity, and subject to rules capable of preventing the release of information without authority. The membership would be comparatively small, appointed by the Parliament on the nomination of the Government and with a government majority.
44. Our draft bill also provides that the Director-General must regularly brief the Leader of the Opposition in the House of Representatives about ASIS.

A single intelligence and security committee

45. It would be anomalous if ASIS were to be subject to more extensive parliamentary review than ASIO. Since both are small organisations with similar needs for secrecy, it would seem sensible for a single committee to oversee them both. If our preferred model is adopted we recommend that it be in the form of a single parliamentary joint committee on intelligence and security to cover both these agencies and the Inspector-General. The draft bill has been prepared on that basis.

Organisation and management

46. The organisation and management culture of ASIS is very much determined by its core function - the collection of secret intelligence. This function requires particular training, skills and dedication, not only on the part of those directly gathering the intelligence but also amongst those who support that activity. The Commission has found ASIS members to be both skilled and dedicated.

47. Our recommendations for improvement of organisation and management principles and practices within ASIS necessarily are framed against an assessment of what we see as present problems or challenges. We do not say, however, that we see ASIS as seriously deficient in an overall sense. In fact we consider ASIS to be well managed and highly focussed on its core function and on achieving success. We believe that the problems which we identify are well recognised in the organisation, and particularly by the present Director-General, and that efforts to deal with them are under way.

48. However, the problems and challenges for ASIS in the areas of organisation and management derive from the nature of the core function itself, and, most particularly, from the need for operational secrecy and for thoroughness of control over operational activity. Bearing in mind the context in which the members of ASIS work, it is not surprising that there should develop a culture which sets great store by faithfulness and stoicism and tends to elevate conformity to undue heights and to regard the exercise of authority rather than consultation as the managerial norm.
49. The Director-General himself maintains a high level of personal contact with staff. His door is open to all members and he is available to talk to them to a degree that would not normally be found in a public service department. The Commission has been impressed by the evidence it has heard of the access staff have to him, and by evidence of their feelings of loyalty to and respect for him. We commend his example and encourage others within ASIS to follow it.

50. The nature of ASIS's operational activities inevitably means that members of staff are subject to pressures and restrictions, present in Australia but more onerous at postings overseas. They are bound to a level of secrecy rarely imposed on individuals in other organisations and cannot talk freely about their work even to family and friends. All of this entails adjustment or restriction of outside activities.

51. These restrictive conditions of employment have led to the view that ASIS owes what was described to us as 'a special duty of care' to its employees. We do not accept that the duty of care is special, or is different from the duty of care owed by any employer to its employees. However, by reason of the matters which we have outlined above, proper discharge of the duty requires special consideration and action. It is important, we think, to make this clear, because otherwise the assumption of some special duty tends to encourage a culture of dependence which is undesirable.

The need for change

52. There must be an acceptance within ASIS that staff will disagree with management decisions from time to time. Not only is that not disloyal, but it can contribute to the diversity of ideas and the general health of the organisation. We do not doubt that the Director-General accepts this, just as we accept that control of ASIS's operational activity requires, in the end, obedience to direction. Again, it is a case of managers not allowing the requirements of intelligence collection to dictate attitudes and actions in ordinary dealings with staff.

53. The Director-General has been forthright in acknowledging the need for change and the priority which it must be given. At his first appearance before the Commission, he listed as one of the challenges for the future the need to 'introduce reform and cultural change in the Service'. At his final appearance, he acknowledged the pivotal role which he himself must play in managing the process of change.
54. He has recognised the need for better delegation, for greater transparency in promotion and other procedures, for greater application of the principles of industrial democracy, and, in particular, for a more participative style of management. But it is necessary, of course, that the Director-General's own commitment to change should be embraced also by all of his senior managers.

The resolution of grievances and complaints

55. The culture of stoicism to which we have already referred has inevitably had an adverse and constricting effect upon the availability of proper procedures within ASIS for the ventilation and resolution of staff grievances. One of ASIS's senior managers, in expressing his belief that the attitudes in the Service are now changing, has described the type of attitude which must first be rectified in order to enable change to occur:

The relationship between the loyalty culture and the need for proper grievance procedures is evolving. It's evolving in the right direction. At the moment there is a justified fear that by lodging a grievance one separates oneself from the Service which gives one life and salary. ASIS has to become - ASIS staff have to become more sophisticated about that. They have to be able to accommodate elements of conflict in their relationship with the management because the monolithic arrangement whereby everybody is totally loyal to the Service, and to question that loyalty is a disgrace, has resulted in individuals suffering.

56. That analysis was echoed by one of the complainants who pointed out that in a closed organisation, 'in a closed family like that is, you don't make waves'. It seems to us from our consideration of the individual complaints and our contact, both formal and informal, with members of the Service, that there still prevails a notion that dissent, and particularly dissent translated into a formal complaint, is equivalent to disloyalty. It is necessary to overcome what has appeared to be some uneasiness in addressing internal grievances, and we have recommended an approach which better acknowledges that a complaint by an officer against the Service is not an act of treachery.

57. In relation to external review we have suggested that the functions of dealing with personal grievances by members or ex-members of the Service and complaints against the Service (most often from the public) should be separated. The Inspector-General should deal with complaints. Staff grievances which cannot be resolved within the Service should be directed to a division of the Administrative Appeals Tribunal, which has determinative power.
58. We think that an inquisitorial or investigative system is suitable for the purpose of examining complaints which may well be in a generalised form and which may first require to be formulated in some specific shape. But personal grievances by staff or former staff usually present an issue which can ultimately be dealt with more effectively by a modified and comparatively informal mode of adversarial procedure.

Protection of sources and methods

59. We have considered very carefully whether it is appropriate to recommend changes in the law in order to provide a proper degree of protection against the public disclosure of security sensitive information. It was for the purpose of a general and informed discussion upon this topic that we invited a number of media editors to attend and express their views, and we are grateful to those who did so. We had also extended the invitation to other journalists who declined, apparently on the footing - for which there was no basis - that we were seeking either to extract from them the sources of the media pieces to which we have referred, or to gather evidence to support some new and draconian methods of suppressing the publication of information about ASIS.

60. Our purpose was rather to consider, and in doing so to take the advice of those professionally involved in the field, how best a balance could be maintained between the public interest in the free transmission of information and opinion and the public interest in preserving the national security. We were interested also in ascertaining the criteria by which editors determined whether or not they would publish matter which clearly was sensitive from the security point of view; and, in this connection, to seek the views of media representatives about the desirability and feasibility of regenerating the D Notice system, which is a voluntary process by which media editors are requested not to publish certain sensitive information (for example, material which relates to current operations being conducted by ASIS).

61. Based on this evidence and the other evidence gathered from government sources, we have concluded that there is value in the maintenance of a voluntary D Notice system which, however, requires reinvigoration through a consultative process between government and media representatives. We have also formed views upon the quality and value of civil and criminal remedies which the government may wish to apply in protection of sources and methods. We have recommended some changes, taking account of the final report of the Review of Commonwealth Criminal Law (conducted by the Gibbs Committee).
The changes we suggest we perceive as refinements designed to supplement, rather than to supplant, a voluntary system.

62. We generally support the approach of the Gibbs Committee to the amendment of the Crimes Act. But we do not agree that proof of damage should be dispensed with in every case where information is disclosed by an officer or former officer. We recommend that in such cases proof of damage be required save where the likelihood of harm is overwhelming e.g. the disclosure of current operations.

63. We support the Committee’s recommendation on protection of whistleblowers. In addition, we recommend the provision of a defence (to disclosure) of public interest. We favour the Gibbs Committee’s recommendations about secondary disclosure. However, because this provision would apply most often to journalists it must be considered in the context of the D Notice system. We recommend that the Government should not proceed to introduce the proposed offence of secondary disclosure until a restored D Notice system has been given a chance to function.

The public face of ASIS

64. The public face of ASIS is the face presented in the media. Perhaps more accurately it is the face drawn by the media, since a degree of artifice is often involved in order to supply by invention the facts which a firm policy of secrecy must conceal.

65. Unfortunately, as the media witnesses who appeared before the Commission acknowledged, and as we record in our Report, ‘ASIS makes a good story primarily because it is shrouded in secrecy’. The fascination which journalists apparently feel for secret organisations tends to expel judgment and restraint. In March 1994 a mass circulation magazine published a story by one Wendi Holland in which she claimed to have been employed by ASIS between 1969 and 1989 as an assassin. She had, she said, committed more than ten murders - with the knife it seems - on orders from ASIS. This lurid fantasy was repeated in separate media interviews in June and July 1994. It is entirely untrue. Ms Holland was never employed by ASIS, and the Service does not engage in the kind of activities she described.

66. The portrait of ASIS painted in the media is seldom other than unflattering. There are several reasons for this. First of all, there are journalists who are sceptical about the need for an agency such as ASIS and some are
therefore predisposed to denigrate it on principle. Secondly, unfavourable media attitudes reflect community values in Australia, where there is a strong tradition of dislike of spying and of doing things in a way presumed to be underhanded or unfair. Thirdly, it is almost inevitable that there should be mutual suspicion and even hostility between the media, which trade in the free flow of information and opinion, and a Service which is dedicated to secrecy.

67. It is necessary, in our opinion, to arrive at some better compromise which will enable the media to carry out their mission and will enable ASIS to preserve its necessary secrets without an unjustifiable degree of protection from comment and criticism. A number of the steps we propose are directed to that end including:

- legislation and parliamentary scrutiny;
- publication of more information about ASIS and the wider intelligence community, and about arrangements for accountability and control;
- an appropriately limited modification of the Government's 'neither confirm nor deny' policy;
- more open contact between ASIS and the media, including through the appointment to ASIS of a media liaison officer, a step which has proved worthwhile in the case of ASIO;
- a reinvigorated D Notice system.

The Honourable Gordon J Samuels AC QC
Michael H Codd AC
31 March 1995
Chapter 1

Introduction

The functions of ASIS

1.1 The Australian Secret Intelligence Service (ASIS) was established by executive direction on 13 May 1952, its role being 'to obtain and distribute secret intelligence, and to plan for and conduct such special operations as may be required'.

1.2 ASIS was closely modelled on its United Kingdom counterpart where both functions (that is, intelligence collection and covert action) were the responsibility of the Secret Intelligence Service.

1.3 From the beginning, ASIS had a regional focus. This was reflected in reasons put forward in 1950 for its establishment. They included: the Communist victories in China; the situation in Indo-China and Malaya; the rise of nationalism in Asia; the gradual resurgence of Japan; the deterioration in the position of the UK as a world power; and the emergence of Australia as the leading Commonwealth power in the Pacific, able to assume increased defence responsibility in the region and thus relieve the UK of a portion of her worldwide burden.

1.4 With the exception of a covert action function, which was abolished following the recommendation of the second Hope Royal Commission (the Royal Commission on Australian Intelligence and Security Agencies 1983-84), the functions of ASIS have remained essentially unchanged from its establishment until today. They embrace the collection and distribution of secret foreign

---

1 Exhibit 1.1, paragraph 5.
2 Exhibit 20.1.2, paragraph 2.
intelligence, associated counter-intelligence activities, and liaison with similar foreign organisations.³

1.5 Since the establishment of the Service, its functions have also been tied in the Directive to the requirements of Government. Thus, in the first Directive, the Service was directed to ‘base its efforts to collect secret intelligence on requirements of Government Departments and central intelligence agencies’. The present Directive lays down that ‘ASIS shall accept the guidance on targets and priorities issued from time to time by the Security Committee of Cabinet, or under arrangements approved by that Committee’.⁴

1.6 We describe below some notable events in the development of the Service.

The Royal Commission on Intelligence and Security – the first Hope Report

1.7 The Commission was established on 21 August 1974 and charged with making recommendations ‘on the intelligence and security services which the nation should have available to it’. Mr Justice Hope was invited to consider issues of efficiency and effectiveness, including arrangements for co-ordinating and evaluating intelligence and its distribution and use, and to review the machinery for ministerial and official control.⁵

1.8 The Government’s responses to his reports were announced in 1977. First, on 5 May 1977, the Government announced the establishment of new co-ordinating machinery at both the ministerial and official levels, and the decision to establish the Office of National Assessments. On 25 October 1977, the Government announced decisions relating to other recommendations, including decisions directly affecting ASIS and arising from the Fifth Report. This was the first official acknowledgment of the existence of ASIS – public acknowledgment having been recommended by Mr Justice Hope. The Commissioner had recommended ‘that the Government accept the continuing need for an Australian secret intelligence service and that ASIS be retained to fulfil that role’. He reported that ASIS was a ‘singularly well-run and well-managed agency’ and was ‘right in concept for Australian circumstances’.⁶

---

³ Exhibit 1.8, Attachment B, paragraph 3.
⁴ Exhibit 1.1, paragraph 5 (1952); Exhibit 1.8, Attachment B, paragraph 13 (1985).
⁵ Exhibit 2.1.4.
⁶ Exhibit 2.1.1, paragraphs 614, 609, 603, 541, respectively.
1.9 The Government affirmed in the October statement that the main function of ASIS was to obtain, by such means and subject to such conditions as were prescribed by the Government, foreign intelligence for the purpose of protecting or promoting Australia or its interests. The Government also accepted recommendations that ASIS should be made responsible to and placed under the control of the Minister for Foreign Affairs, and that its funding should in future be the subject of a one-line appropriation.

1.10 The statement declared that ASIS's capacity to serve Australia's national interest would continue to depend on full protection of the secrecy of its activities; and it indicated that the Government would therefore adhere strictly to the practice of refusing to provide details of those activities, and would not enter into any discussion about the Service.

1.11 The Commission had described the functions it considered appropriate for ASIS and had recommended legislation embracing those functions. It had also recommended that the Headquarters of ASIS be moved from Melbourne to Canberra and co-located with the Department of Foreign Affairs. Apart from detailed recommendations about matters such as cover and personnel management, the other main recommendations bearing on ASIS were to do with the new co-ordinating machinery announced in the May 1977 statement.

The move to Canberra

1.12 The Headquarters of the Service was relocated to Canberra, and co-located with the then Department of Foreign Affairs, in March 1984. The move brought ASIS closer to its customers and, as subsequent reviews have shown, into progressively closer working relationships with them and with the Department of Foreign Affairs and Trade. Thus, the move contributed to the closer integration of ASIS into the control and accountability arrangements which applied to the Australian intelligence community as a whole. The adjustments necessary were considerable, not least because ASIS lost some 50 per cent of its staff, mainly on the support side, at the time of the move.

---

8 Exhibit 2.1.1, paragraph 57; Exhibit 2.1.2.2, Annex 1, s.6.
9 Exhibit 2.1.1, paragraph 618.
The Royal Commission on Australia’s Security and Intelligence Agencies – the second Hope Report

1.13 This Commission was established on 17 May 1983 to review Australia’s security and intelligence agencies, especially as they had operated in the period since the first Hope Report, and to assess the implementation of Government decisions on that earlier report. The terms of reference included issues of efficiency and effectiveness and of accountability and control.

1.14 After the Commission had been established, and following the incident at the Sheraton Hotel, Melbourne, on 30 November 1983, the Commissioner was asked to provide a report on that incident as well.10

1.15 In his report on the events of 30 November, the Commissioner recommended that the covert action function previously assigned to ASIS be abolished. The Government accepted that recommendation and amended the Directive accordingly in December 1985. The Directive revised at that time remains in force today.

1.16 Other recommendations made by Mr Justice Hope in 1984 and accepted by the Government dealt with reporting capabilities and product, operations in Australia under the Australian Security Intelligence Organization Act, overseas operations, machinery of government, resources management and training.

1.17 Of the general recommendations accepted by the Government, the one with most relevance for and impact on ASIS was the recommendation that an office of Inspector-General of Intelligence and Security be established. The Inspector-General was to have an oversight role in relation to ASIS, a role which is discussed more fully later in this report, and a role in the review of public complaints and staff grievances.

Report on the Australian intelligence community in a changing international environment – the Richardson Report

1.18 This report was prepared by the Secretaries Committee on Intelligence and Security (SCIS) and presented to the Security Committee of Cabinet (SCOC)

---

10 It was reported that participants in an ASIS covert action training exercise had broken down a door in the hotel with a sledgehammer and had threatened hotel staff with guns.
in June 1992.\textsuperscript{11} It reviewed the roles and relationships of the collection agencies as they would be affected by the collapse of the Soviet Union and the disappearance of the strategic and ideological divide between East and West.\textsuperscript{12} In that context, the report considered the contribution made by ASIS in the past and its potential future contribution, and generally offered a favourable assessment.

1.19 It also came to the conclusion that the overall structure put in place after the two Hope Royal Commissions remained appropriate in the 1990s, as did the existing roles of the agencies. It indicated, however, that management and co-ordination arrangements would need to be adjusted so that they could cope with the pressures of a more diverse international environment.

1.20 Findings of a general character in the report were accepted by SCOC.

\textbf{Intelligence collection in a more complex world – the Hollway Report}

1.21 After considering the Richardson Report, SCOC commissioned a further report on shortfalls in Australia’s foreign intelligence collection and means of addressing them.

1.22 The resulting Hollway Report\textsuperscript{13} was presented to SCOC in December 1992. The report assessed in some depth the performance of the various collection agencies and shortfalls in collection. In general, it rated highly the performance of ASIS in undertaking the tasks assigned to it, and, proposed more refined tasking arrangements.\textsuperscript{14}

\textbf{The present inquiry}

1.23 The intention to establish this Commission of Inquiry was announced by the Minister for Foreign Affairs and Trade, Senator the Hon. Gareth Evans, in the Senate on 23 February 1994. The composition of the Commission and its terms of reference were announced on 28 February 1994 and Commissioners were appointed on 15 March 1994.

\textsuperscript{11} The principal author of the report was Mr D Richardson, a senior officer in the Department of the Prime Minister and Cabinet.
\textsuperscript{12} Exhibit 2.3.1.
\textsuperscript{13} Or the Hollway-Kean Report, its authors being Mr DA Hollway, Deputy Secretary, Department of the Prime Minister and Cabinet, and Dr D Kean, Deputy Director-General, Office of National Assessments.
\textsuperscript{14} Exhibit 2.4
1.24 The terms of reference, as they appear in the Letters Patent, are to inquire into:

(a) the effectiveness and suitability of existing arrangements for:
   (i) the control and accountability of the Service;
   (ii) the organisation and management of the Service;
   (iii) the protection of the Service's intelligence sources and methods;
   (iv) the resolution of grievances and complaints relating to the Service; and

(b) whether any changes in existing arrangements are required or are desirable.\textsuperscript{15}

1.25 The 'functional role and priorities of ASIS' were considered to have been exhaustively addressed by the Government in 1992 and it was not proposed that the Inquiry should address those matters.\textsuperscript{16}

1.26 The reasons for establishing the Commission of Inquiry were said to be a feeling that there is a case for periodic root-and-branch review of secret organisations, and a wish, in view of the end of the Cold War and the recent expansion of ASIS, to consider the desirability of a legislative charter and the adequacy of existing management systems and protection mechanisms.\textsuperscript{17}

1.27 The Minister's announcement in the Senate followed a series of newspaper reports and the broadcast of a \textit{Four Corners} program on 21 February 1994 in which allegations were made about activities of ASIS. The Minister's statement of 28 February referred to purported revelations by former ASIS officers, saying that the Government expected those former officers to make known their concerns about the organisation and management of ASIS to the Inquiry. In response to subsequent questioning in the Parliament, Senator Evans gave assurances that the Commission would be able to consider policy or process issues which arose out of particular cases.\textsuperscript{18}

\textsuperscript{15} The Letters Patent are reproduced at Appendix A.
\textsuperscript{16} Senate \textit{Hansard}, 28 February 1994, p.1087.
\textsuperscript{17} Ibid, p.948.
1.28 In his evidence before us, the Minister again acknowledged the link between the Inquiry and 'escalating tensions and disclosures' and expressed the hope that the Inquiry would be a 'circuit breaker'.

1.29 At the outset of the Inquiry, we published our approach to the terms of reference, indicating we would first need to understand:

- what arrangements currently existed in each of the four categories of our terms of reference;
- how and where those arrangements were defined or laid down; and
- how those arrangements operated or were applied in practice.

We went on to say:

In addition to general descriptions of how the arrangements actually operate, the Commissioners will need to examine some illustrative examples of the application of the arrangements to particular cases.

It is not the function of this Inquiry to investigate or evaluate the functional role or priorities of ASIS as an intelligence agency. Nevertheless, the effectiveness and suitability of the existing arrangements will be assessed, in part at least, by reference to the objectives and functions of ASIS and the nature and purpose of the operations which it conducts. Information of a reasonably detailed kind will be required with respect to these topics.

In deciding whether to recommend any change to existing arrangements, the Commissioners will need to identify, in relation to each category of arrangements, the various purposes and interests which the arrangements should serve. Questions may also arise as to the way in which competing interests should be resolved.

In addition to the national interest and the public interest, as broadly defined, consideration would need to be given for this purpose to the interests of:

- national security;
- ASIS as an organisation;
- ASIS management;
- ASIS staff;
- other government agencies;
- other governments.

1.30 The Commission also announced the procedures which it intended to follow in taking evidence. These procedures were formulated with the aims of

---

19 T2465.
20 Exhibit 2.6.3.
encouraging people and parties with an interest to participate and make submissions, and of ensuring fairness.\textsuperscript{21}

1.31 The Commission held its first hearing, in public, on 2 May 1994. Further hearings were held between that date and 13 December 1994. At the first hearing Mr Christopher Maxwell announced his appointment as Counsel Assisting the Inquiry. Leave to appear was granted to counsel for ASIS, IGIS and some former ASIS officers. It had been the intention and wish of the Commission to conduct some hearings in public, but in practice the matters being considered invariably impinged, at least in part, on areas of national security sensitivity and we judged it impractical to conduct public hearings in such circumstances. Edited transcripts of hearings at which media representatives gave evidence were published on 21 February 1995.

1.32 The Commission conducted hearings on 67 days over the period from May to December and heard from 89 witnesses. Commissioners also visited ASIS establishments in Australia and held discussions with staff in the course of those visits. Commissioner Samuels held discussions in the United Kingdom, the United States and Canada with relevant intelligence and security organisations and officials from those countries, and with some Australian officials and ASIS staff stationed overseas.

1.33 Almost 7,000 pages of transcript were produced from the Commission's hearings, and over 2,000 documents went into evidence. Extensive submissions were received from the Director-General of ASIS, the Inspector-General of Intelligence and Security and the individuals whose cases the Commission examined in detail. Submissions were also received from many Commonwealth departments and agencies and from other organisations and individuals, including former ASIS officers, academics, authors, civil rights proponents, media representatives and people with general or personal interests in various of our terms of reference.

1.34 The cases of individual former officers of ASIS and the spouse of one took a large part of the Commission's time. Some 40 per cent of hearing time was consumed in dealing with those cases. Volume 2 of our report addresses the cases in some detail, as well as applying the lessons arising from them to the general matters embraced in our terms of reference.

\textsuperscript{21} T3-4.
1.35 In addition to this detailed report, parts of which are necessarily secret, the Commission has prepared a summary report which it has recommended that the Government make public.
The Accountability Framework

The meaning of accountability

2.1 The Government has endorsed a definition of accountability that was prepared for the Management Advisory Board (MAB) of the Australian Public Service by its Management Improvement Advisory Committee (MIAC):

In the context of the relationship between public servants, secretaries of departments and ministers, and ministers and the Parliament, accountability is defined as existing where there is a direct authority relationship within which one party accounts to a person or body for the performance of tasks or functions conferred, or able to be conferred by that person or body.\(^{22}\)

2.2 The MAB/MIAC document begins by noting that accountability is 'fundamental to good governance in modern, open societies'. It describes accountability as 'one of the essential guarantees and underpinnings, not just of the kinds of civic freedoms [Australians] enjoy, but of efficient, impartial and ethical public administration'.\(^{23}\) Accountability guarantees these things through controls which ensure that those who are entrusted with governmental responsibilities carry them out efficiently and effectively and that the responsibilities assumed at each level within government are appropriate.

2.3 Control means that an individual or body is 'subject to an institution's or person's oversight, direction or request that they provide information on their action or justify it before a review authority'.\(^{24}\) The accountability obligations of public officials and bodies are met through controls which, according to MAB/MIAC, operate at three levels. Public servants are responsible, through a

---

\(^{22}\) MAB/MIAC, *Accountability in the Commonwealth Public Sector*, June 1993, p.1, (Exhibit 3.3.5).

\(^{23}\) Ibid., p.3.

managerial hierarchy, to the heads of their agencies, heads of agencies are responsible to ministers, and ministers are responsible to the Parliament. The Parliament itself is accountable to the people through elections. In addition, individuals and agencies at each level of government are subject to external review bodies such as courts and tribunals and investigative bodies such as the Auditor-General and the Ombudsman.25

2.4 Although they exist at different levels, the controls that make up the system of public accountability do not operate in a strictly hierarchical way. Lines of responsibility and flows of information and responses are not always vertical, and ministers and departmental secretaries obtain information directly from officers at various levels in departments and agencies. Independent external review, parliamentary control of government and popular control of the Parliament are even less hierarchical than the control relationships within government. They rely on networks of reporting and responsibility which draw information from and provide responses to all levels of the governmental structure.

2.5 Information is central to effective control in accountability relationships. Each kind of control depends on the availability of information to those by whom it is exercised. An individual or body can be held to account only by those who have access to relevant information on performance.

2.6 The MAB/MIAC statement provides an appropriate framework within which to consider the accountability and control of ASIS. Although ASIS is not a part of the public service in the sense of being governed by the Public Service Act, it is an instrument of the Australian Government, funded from the budget and under direct ministerial control. The Minister for Foreign Affairs, the Director-General and senior Government officials accepted that the Service should be part of the system of public accountability, with appropriate modifications to meet security needs.26

The existing framework

2.7 The existing system by which ASIS is controlled and is held accountable comprises elements which operate within the executive government and others which provide external scrutiny. The executive government components are the Directive, the Minister for Foreign Affairs, the Director-
General and internal controls, the Internal Auditor, the Department of Foreign Affairs and Trade, the Security Committee of Cabinet and the Secretaries Committee on Intelligence and Security, the Office of National Assessments (and the National Intelligence Collection Requirements Committee and the National Intelligence Committee), the Inspector-General of Intelligence and Security, and internal inquiries. External components comprise the Parliament, the Opposition, the Auditor-General, and external inquiries.

2.8 These various elements are described briefly in the next sections of this chapter in order to provide an integrated summary – and are then described in more detail and assessed in chapters which follow.

The accountability of ASIS within the executive government

The Directive

2.9 The basis for the control and accountability of ASIS within the executive government is the Directive, issued to the Director-General by the Minister for Foreign Affairs after being endorsed by the Security Committee of Cabinet (SCOC). The Directive provides for the existence of the Service and establishes many of the arrangements for accountability and administration under which it works. It sets out the functions of ASIS, and proscribes one former function: training for or carrying out covert action. It requires that ASIS obey Australian law, and that its activities conform to the foreign policy of the Government of the day. The Directive places the Service under the control of the Director-General who, in turn, is made subject to direction by the Minister for Foreign Affairs. It provides for the Director-General, as authorised by the Prime Minister, to brief the Leader of the Opposition. It also contains provisions for the employment of staff and the administration and financial control of the Service.

The Minister for Foreign Affairs

2.10 The responsibility assigned by the Directive to the Minister for Foreign Affairs makes the Minister the most important element in the control and accountability of ASIS. The Minister bears the political responsibility for what the Service does. The effectiveness of the control and accountability of ASIS depends crucially on the competence of both the Minister and the Director-General and the trust between them.
The Director-General and internal controls

2.11 The Director-General's control of ASIS involves a high level of personal responsibility. ASIS officers are employed under contract with the Director-General, and the Directive makes him or her personally responsible to the Minister for the individual and collective performance of officers. In consequence, the Director-General personally exercises a wide range of operational and administrative powers. These include all decisions to engage or dismiss staff, and approval of all recruitments, terminations, promotions and postings.

2.12 The internal management of operations, which we examined in detail, embraces a web of checks and balances which we found to be extensive, thorough and effective. The Director-General is then personally responsible for all key operational decisions.

2.13 The Service's program of overseas postings ensures regular movement of staff. The handover of responsibilities from one officer to another guarantees periodic review of the reliability and integrity with which each function has been carried out. As the Director-General pointed out, a conspiracy, progressively expanding over time, would be required to defeat this system.27

The Internal Auditor

2.14 The Internal Auditor carries a responsibility going beyond that of counterparts in most other government agencies. This is because the ASIS internal auditor has been the sole auditor of the exempt accounts relating to ASIS operational expenditure, as well as carrying the normal responsibilities relating to the non-exempt accounts which are also subject to external audit. Assurances to the Minister on the exempt accounts thus depend on the Internal Auditor and the Director-General.

The Department of Foreign Affairs and Trade (DFAT)

2.15 The line of responsibility from the Director-General to the Minister is direct and personal. The current Directive prohibits the interposition of any official between the Minister and the Director-General, a prohibition that dates from Mr Justice Hope's comments in the report of his first Royal Commission on Intelligence and Security on the arrangements that applied for 20 years from 1958. During that period ASIS had been subordinated to the then Department of

27 Exhibit 20.3, p.1; T3153.
Foreign Affairs although the Department, in practice, accepted no responsibility for the exercise of its control of ASIS.28

2.16 The Directive retains from that period a provision, subject to any direction by the Minister, that the Secretary of DFAT, or a Deputy Secretary accompany the Director-General when he or she discusses ASIS policy or operations with the Minister. The present practice is that DFAT officers attend such meetings only when required by the Minister. We commend this approach. The Department now has no controlling role over ASIS in either a managerial or operational sense.

2.17 Although the Directive empowers the Secretary of DFAT or a Deputy Secretary to obtain from ASIS any information that is required, the Department does not seek to be privy to the details of the Service's most sensitive work, considering that such knowledge risks complicating its own business as well as making that of ASIS more difficult.29 Consultative mechanisms in Canberra and overseas ensure that ASIS and DFAT are each generally aware of the other's activities and concerns and, in normal circumstances, this should be sufficient. We consider that the power given to the Secretary of DFAT, to obtain information from ASIS is anachronistic and that any such demands by DFAT should be at the Minister's initiative. Recommendations later in this report for revision to the Directive reflect this view.

2.18 Both ASIS and DFAT believe that the current consultative regime works well.30 It is important that it should, since DFAT is a major source of information and advice relevant to many of the decisions that both the Minister and the Director-General must make in respect of ASIS.

SCOC and SCIS

2.19 The Minister and ASIS are held accountable within the executive government through the structure in place for control of the Australian intelligence community. At the peak of this structure is the Security Committee of Cabinet (SCOC) which normally meets three to five times per year. SCOC currently comprises the Prime Minister (Chair), the Minister for Foreign Affairs (Deputy Chair), the Ministers for Defence and Finance, the Treasurer and the Attorney-General, with the Minister for Trade an alternate member for the

28 Exhibit 2.1.1, paragraphs 317, 347-8.
29 Exhibit 24.1, paragraph 7.
30 Ibid., paragraph 11; Exhibit 20.1.10, p.16; T98-99; T618.
Foreign Minister. SCOC determines the policies and oversees the performance of Australia's security and intelligence agencies, including consideration of their budgetary allocations. The budgetary function is supported by an annual financial report on the Australian intelligence community from the Department of Finance. SCOC is supported by the Secretaries Committee on Intelligence and Security (SCIS), which is chaired by the Secretary of PM&C, and comprises heads of relevant departments as well as the Directors-General of the Office of National Assessments (ONA) and of Security. We examine these arrangements in greater detail in Chapter 7.

**The Office of National Assessments**

2.20 General tasking of intelligence collection activities and the assessment of intelligence product are carried out by ONA or by committees and processes it chairs or directs. One of ONA's assessment responsibilities is to report annually on the performance of the intelligence collection agencies, including ASIS.

2.21 ONA has the lead responsibility for preparing the biennial National Foreign Intelligence Assessments Priorities (NFIAP) document. ONA chairs the National Intelligence Committee (NIC) which refines the draft NFIAP through collective discussion and clears it for consideration by SCIS and SCOC. The NFIAP, when approved, provides the framework within which more detailed collection priorities are defined. NIC also meets monthly for general discussion of intelligence tasking and product and provides a forum, primarily for users of ONA product, to discuss the Office's work program and the relevance of intelligence reports to the needs of users. ONA provides the chair for the National Intelligence Collection Requirements Committee (NICRC) which refines intelligence requirements and highlights current issues in overseas intelligence. A longer-term Foreign Intelligence Planning Document (FIPD) is now expected to be prepared every three years for consideration by SCOC, the first having been endorsed by that Committee on 3 November 1994. ASIS representatives participate in NIC and NICRC and attend SCIS meetings when required.

2.22 ONA, the committees it services, and the documents they produce, contribute to the general tasking and assessment of ASIS from outside the Minister-ASIS-DFAT relationship. This strengthens the extent to which the

---

31 Exhibit 25.2, p.6.
32 Exhibit 2.3, Attachment E, p.5.
33 Exhibit 2.3, pp.62-69.
34 Exhibit 28.1, p.5.
35 Exhibit 2.3; pp.62-69, Exhibit 4.3.6.1, p.vi; Exhibit 4.4.4.
Government, particularly through SCOC and SCIS, is able to assure the accountability and control of ASIS. Intelligence reports from ASIS and the Service's responses to intelligence tasks assigned to it provide a basis on which performance can be measured within the governmental control mechanisms. This aspect of procedures is supported by an annual report produced by the Director-General which is considered by SCOC and reviewed by ONA in its own annual report. Further discussion of the role of ONA appears in Chapters 7 and 8.

The Inspector-General of Intelligence and Security

2.23 The Inspector-General of Intelligence and Security (IGIS) has jurisdiction over the five intelligence and security agencies. IGIS has oversight responsibilities in respect of ASIS for the Service's compliance with Australian law, compliance with directions or guidelines given by the Minister, the propriety of particular activities, staff grievances, and acts or practices referred to IGIS by the Human Rights and Equal Opportunity Commission. There are, however, substantial limits on the scope of inquiries under these headings. IGIS may not inquire into ASIS of his or her own motion or in response to a complaint unless the complainant is an Australian citizen or resident, or the complaint or matter of concern involves a possible breach of Australian law. Complaints relating to most ASIS staff grievances are reviewable by IGIS only so long as he or she considers that internal procedures for redress of grievance are not fair and effective. Ministerial approval is required for an inquiry into any matter which occurred outside Australia or before 1 February 1987.

2.24 Most of ASIS's activities take place overseas, have no direct effect on Australians and have no potential to breach Australian law. The areas of ASIS's activities in which IGIS may initiate own-motion inquiries is therefore small. The Government has the power under the IGIS Act to refer a wider range of matters to the Inspector-General but no such matters have been referred since 1987.

Internal inquiries

2.25 The Government can also effect review of the role and performance of ASIS by commissioning inquiries. Some such inquiries have been initiated for internal use by the government, including, recently, the Richardson and Hollway reviews described briefly in the introductory chapter, embracing the Australian intelligence community as a whole.
Conclusion

2.26 The arrangements for the accountability and control of ASIS within the executive Government are thus extensive, and the evidence is that they have been exercised effectively in the years since the second Hope Royal Commission. However, some refinements are recommended in later chapters of this report, where the arrangements are also described in greater detail.

External accountability

2.27 The Service has been subject to little direct scrutiny from outside the executive government. This can be attributed to the need for operational secrecy and the limited scope for ASIS directly to affect the rights of Australians. It means that the normal instruments of external accountability, direct parliamentary scrutiny and oversight by the Auditor-General, do not apply fully to ASIS, although they have some application.

The Parliament

2.28 For ASIS as for any public sector body, an important mechanism of parliamentary oversight is the pressure that can be placed on ministers and government as a result of publicity about alleged or actual failures by ASIS. Ministers can face severe questioning in Parliament when ASIS failures become apparent, as in the Sheraton Hotel incident, or are alleged, as in the lead-up to the establishment of this Commission. The Government and ASIS can thus be held accountable by the Parliament for failures which come to public attention. But not all failures may become known to the parliamentary overseers.

2.29 Even when they do, a significant limit on parliamentary oversight is the policy of successive governments, accepted by successive parliaments, that the Government neither confirms nor denies non-official claims about the security and intelligence agencies. This means that parliamentary oversight is subject to Government control, since the Government can refuse access to necessary information.

2.30 Scrutiny of the budget and other aspects of agency operations by parliamentary committees provides another mechanism for oversight of the public sector. Little use has been made of this technique in respect of ASIS. The Service is funded through a one-line entry in the appropriation bills and budget

36 Exhibit 25.2, pp.17-18.
papers which are considered at Senate legislation committee hearings; but ASIS officers do not attend the hearings. The Minister, who may be questioned on ASIS at these hearings, is constrained in the answers he or she may give by security considerations and the neither-confirm-nor-deny policy. Other parliamentary committees have not examined ASIS's activities or administration. Overall, there has been little direct parliamentary review of ASIS.

The Opposition

2.31 The Directive provides for the Leader of the Opposition to be briefed by the Director-General. This process has developed so that briefings are normally provided to the Leader of the Opposition or to the Shadow Foreign Minister on their request and at the discretion of the Prime Minister. In some cases the Leader of the Opposition has also been informed of important developments on the initiative of the Government. He was, for example, given a copy of the Richardson Report and informed in advance of the Government's intention to appoint the current Director-General.

The Auditor-General

2.32 The Auditor-General's financial audits across the public sector, and performance audits within the public service, are an important means by which Parliament obtains information relevant to the accountability of most departments and agencies. In the case of ASIS, however, the Auditor-General audits only the non-operational accounts and has never conducted a performance audit in any area of its work.

External inquiries

2.33 Governments have from time to time instituted external inquiries with their powers and independence assured by the Royal Commissions Act 1902. Although the full reports of the external inquiries have not been released, public knowledge that there have been independent external reviews of ASIS and the publication of parts of some of these reports have contributed significantly to the public accountability of ASIS.

---

37 Senate legislation committees were, until October 1994, known as Senate estimates committees.
38 For a reference to an in-camera briefing given by the Director-General to the Parliamentary Works Committee in November 1992, see Exhibit 20.1.9, p.5.
39 See Chapter 5 for further discussion.
40 Exhibit 25.2, p.15. See Chapter 4 below.
41 T3216. Paragraph 48(d) of the Audit Act gives authority for performance audits.
Conclusion

2.34 The mechanisms for the accountability of ASIS outside the executive government are thus more restricted in their coverage than those that apply to most public sector agencies. Significantly, however, as with internal accountability, there is no evidence that the limited applicability of the normal external control mechanisms has resulted in any loss of effective accountability or control.

The present limits to accountability

2.35 The restrictions on the flow of information necessary to successful secret intelligence operations limit the application to ASIS of standard public accountability controls. The Service is subject to a range of controls exercised by the executive government, but the secrecy imperative has meant that the availability of information on the full range of ASIS's activities has been restricted even for this internal accountability. Security restrictions fall with greater force on external accountability mechanisms. ASIS may be questioned and required to justify its actions by review bodies external to the executive, but there are restrictions on the range of matters subject to their review and on the types of information they may request. The Parliament's access to information and its capacity to require justification from ASIS or the Government are even more severely limited. Governments have, on occasion, responded to parliamentary questioning on ASIS's activities, but they usually decline to do so and the Parliament generally has not pressed such requests.

2.36 An intelligence agency cannot carry out many of its legitimate functions, and thus serve the interests of national security, without a high level of secrecy about its operations, personnel and techniques. Secrecy in these areas often will be necessary also to protect the security of individuals. It is security in these two senses which provides the only valid argument for limiting or modifying the application to ASIS of the standard system for accountability in the public service. It is important to ensure that limits on the flow of information, and hence on the accountability and control of ASIS, are no more rigorous than is essential to these security interests.

2.37 Judging what is essential will generally need to be left to the intelligence agency (within a framework established by the Government) for reasons of practicality and relevant knowledge and expertise. But review occasionally of the framework itself and its application will be necessary to an effective system of accountability and control. Such review should ensure,
amongst other things, that those responsible for the accountability of ASIS at every level have access to the necessary information. Restrictions on the flow of information should not continue merely through habit, or because ASIS has been overlooked in progressive changes to the wider system of public accountability.

2.38 Much of the contemporary structure of public accountability has developed recently and a degree of slowness and caution in its extension to ASIS is understandable. A comprehensive system of parliamentary committees was first established in the Senate in 1971 but extended to the House of Representatives only in 1987. The joint committee which oversees ASIO also dates from 1987. Public annual reporting by public service departments and agencies became systematic in the late 1970s and was formalised in 1982, while the comprehensive system of financial reports to Parliament developed between the mid-1970s and the late 1980s. The Commonwealth Ombudsman was established in 1976 and efficiency auditing by the Auditor-General began in 1978. Freedom of Information legislation took effect in 1982. The Parliamentary Privileges Act, which declared and codified important aspects of parliamentary control, was passed in 1987.

2.39 Progress was made over the same period in developing special external accountability and control mechanisms for the intelligence and security agencies. The Security Appeals Tribunal commenced operations in 1980 while the office of the Inspector-General of Intelligence and Security was established in 1987. The existence of ASIS was officially acknowledged in public in 1977 and legislative controls on ASIO were strengthened in the 1970s and 1980s. Substantial strengthening of controls on ASIS within the executive followed the Hope Royal Commissions of 1974-77 and 1983-84.

2.40 The external components of this new system of accountability have limits on their jurisdiction arising from contemporary judgments about the security interests referred to earlier. Thus, the structure of control and accountability within which ASIS operates is considerably less extensive than that which applies elsewhere in the Australian public sector. It is also significantly less extensive than is the case for ASIO. Many of the foreign intelligence agencies of other countries now face more comprehensive systems of control and accountability than does ASIS. In particular, the comparable agencies in the United States and the United Kingdom both have a statutory base, and formal relationships with review committees of their legislatures. The Canadian Security Intelligence Service, which has only domestic security functions, has been subject to oversight by an independent statutory committee.
of privy councillors since 1984 and, more recently, has come under the oversight of a parliamentary sub-committee.

2.41 The general arguments for the reforms to public sector accountability in recent years have components both of principle and pragmatism. As a matter of principle, agencies which exercise the powers and use the resources which Australians give their governments should be accountable to the Australian community for their actions. At the pragmatic level, if the controls by which that accountability is realised function properly, the agencies can also be expected to be more efficient and effective. This is because effective controls should promote a greater focus on performance and on linking resource allocation to performance. The challenge in giving effect to appropriate controls in the intelligence sphere is to devise methods that can realise the benefits of accountability without exposing aspects of operations which must be secret if they are to be effective.

2.42 These propositions apply with equal force to the intelligence community. The 1993 annual report of ONA acknowledged that the intelligence and security agencies should not be overlooked in the reform of structures for accountability in the public sector:

Recent years have seen a strengthening of arrangements for accountability in all aspects of government activity. The Australian Intelligence Community cannot be immune from that trend, despite – indeed, especially because of – its being substantially protected from the public eye by the requirements of security.42

2.43 Proposals to enhance the accountability of ASIS need not imply that there has been any significant failure of accountability in respect of the Service. In fact, there is no evidence of such a failure since the Sheraton Hotel incident of 1983. The Service was not involved in significant public controversy between that incident and the recent events which led to this Inquiry. Detailed review by the Commission of the contentions by former ASIS officers that led to the Inquiry, supplemented by an audit of ASIS files by the Commission’s staff, did not reveal any significant lapses in accountability. On the contrary, all the evidence was of a carefully managed organisation under tight internal and ministerial control. This Inquiry has provided an opportunity for a review of the arrangements for control and accountability of ASIS in the context of the relevant reforms of recent years in the Australian public sector, and of current practice in intelligence communities overseas. The changes proposed in this report are a response to that opportunity, not a criticism of the current accountability regime.

42 Exhibit 4.3.6.1, p.1.
2.44 Any adaptation of the recent reforms so as to improve the accountability of ASIS while retaining necessary secrecy must take account of ASIS's status as only one component of an intelligence community. It will not always be possible or desirable to change the arrangements for its accountability and control in isolation. The intelligence and security agencies have common interests, deal with common issues and share a special need for secrecy. It is sensible that arrangements for their accountability and control be based on common principles and, where practicable, shared mechanisms and practices. Some of the recommendations in this report may therefore have implications for agencies other than ASIS, and they have been framed, where appropriate, with that in mind.

Reasons for enhancing accountability

2.45 Although we have found that the system of accountability and control of ASIS is extensive and effective, especially within the executive government, it is subject to the limits outlined in the preceding section, and we have suggested some modifications in later chapters. We see these enhancements as desirable for two reasons. First, the accountability and control of the Service rests very heavily on the Minister and the Director-General. However competent and effective particular ministers and directors-general may be, and however professional the relationships between them, the accountability and control of a secret organisation with sensitive functions should not depend so much on the personal characteristics and capabilities of two individuals and the relationship established between them.

2.46 Secondly, it is desirable that external accountability for ASIS be enhanced because the Service exercises significant governmental powers. The exercise of these powers ought to be subject as far as possible to the same processes of democratic control and authorisation as apply to other aspects of government decision making. In the report of the first Hope Royal Commission, Mr Justice Hope wrote in words quoted to this Commission by ASIS, that the fundamental consideration favouring legislative authority for ASIS is that 'Parliament is the instrument of democratic control of government in this country.' We see scope for enhancing the controls which ensure that ASIS's actions remain within the bounds authorised by the Parliament, and acceptable to the Australian people.

43 Exhibit 2.1.2.2, paragraph 10; Exhibit 6.3.1, paragraph 13.
2.47 The mechanisms for the control of ASIS, especially those external to the executive, have developed less extensively in recent years than have the comparable arrangements for public agencies outside the Australian intelligence community. It is opportune to make enhancements directed at reducing this imbalance.
Chapter 3

Legislation

The Hope view

3.1 The idea of legislation for ASIS is not new. In the report of the Royal Commission on Intelligence and Security in 1977, Mr Justice Hope recommended the statutory incorporation of ASIS. He saw the principal advantage as being the conferral of legitimacy:

Legislation, by giving the service a proper role assigned to it by Parliament, would establish it as part of the family of government. It would thereby favourably improve its efficiency and effectiveness, and, by removing a cause of unease amongst some of its officers, enhance its morale.

He considered that legislation would also make regular the financial transactions of ASIS and give its officers desirable security of tenure.

3.2 In notes he prepared on draft legislation, Mr Justice Hope expanded on his reasons for supporting a statutory basis for ASIS:

The fundamental considerations favouring Parliamentary sanction for ASIS is that the Parliament is the instrument of democratic control of government in this country. So a statute establishing ASIS is a statute authorizing the Minister to act to control the service on behalf of the Parliament itself, speaking for the people. And the Minister is responsible to the Parliament, in a general way, for ASIS.

3.3 Mr Justice Hope acknowledged that any statute which established and regulated a secret service ‘must to some extent break with recognized legislative drafting norms’. A statute could not lay down precise rules as to the methods

44 Exhibit 2.1.1, paragraphs 302-8.
45 Ibid., paragraph 305.
46 Exhibit 2.1.2.2, paragraph 10.
47 Ibid., paragraph 2.
ASIS should use in conducting secret intelligence operations. Nor could it say with particularity how or under what conditions ASIS should operate in Australia to collect foreign intelligence, save in compliance with Australian law. But his Honour believed that it was worthwhile, nevertheless, to attempt to obtain from Parliament 'the maximum authority and control consistent with the essential need for secrecy'.\(^{48}\) The recommendation for legislation was not, however, taken up by the then Government, and Mr Justice Hope did not renew it in his 1984 report.

**Current views**

3.4  The question of legislation for ASIS was widely canvassed in evidence and submissions to this Inquiry. ASIS itself argued strongly in favour of legislation.\(^{49}\) The Service stressed that legislation was needed to ensure adequate protection of ASIS's sources, staff and methods, and of its relations with foreign liaisons.\(^{50}\) The need for such protection had been raised with the Minister before this Inquiry was instituted.\(^{51}\) It was the Service's main objective at the outset and is still seen by ASIS as the principal practical benefit of legislation.\(^{52}\) Following the *Four Corners* program in February 1994 and 'a massive ... amount of hostile media attention', the thinking of the Service moved beyond the initial concern about protection of sources to the question of the standing of the Service in the community. The Service came to the view that it should look ahead and that, for the future standing of the Service, it would be much better if it were put on a legislative basis.\(^{53}\) It therefore became an important ASIS objective to regularise the position of the Service in the eyes of the community.\(^{54}\)

3.5  The Service considers that changing community expectations of intelligence and security services mean that executive direction may no longer be an appropriate legal basis for the Service:

> The present legal basis of the Service may no longer be as appropriate as it once was. This, together with the policy of not commenting on allegations about ASIS, may lead to concern among members of the public and Parliament that ASIS is somehow 'out of control'. Greater transparency in regard to the already

\(^{48}\) Ibid., paragraph 9.

\(^{49}\) *T*958*.

\(^{50}\) Exhibit 6.3.1, paragraphs 4, 5.

\(^{51}\) Exhibit 4.2.1, paragraph 15; T65.

\(^{52}\) *T*957*.

\(^{53}\) T66-7.

\(^{54}\) *T*957*.
extant oversight and accountability arrangements for ASIS is, in the Service’s view, easily achieved and would allay what concerns there are in the Parliament, government and the wider community. A statutory basis for ASIS would enhance both the sense and the reality of its accountability.55

The Service recognised that legislation to achieve these ends would involve a higher public profile for the Service generally and perhaps for some of its more senior officers.56

3.6 The Inspector-General of Intelligence and Security also favoured legislation for ASIS, along the lines of the ASIO model. In his view, the legislation and guidelines governing ASIO:

   (a) specify clearly what ASIO may and may not do;
   (b) define with some precision and care the roles of the Minister and the Director-General;
   (c) provide protection for ASIO staff and ASIO intelligence; and
   (d) cover in greater or lesser depth the various accountability mechanisms.57

These elements combined to provide a detailed framework within which ASIO officers could perform their duties. This made their task easier, and also enhanced public confidence that ASIO was under control and was carrying out legitimate functions in an appropriate way.58

3.7 The Minister for Foreign Affairs was more equivocal. He acknowledged that legislation would offer some advantages to ASIS. In particular:

   (a) some of the mystery and drive to speculate about ASIS might be defused;

   (b) ASIS would be seen to be properly established under Australian law;

   (c) a general objective for ASIS could be publicly defined;

---

55 Exhibit 6.3.1, paragraph 15.
56 T46.
57 Exhibit 23.1, paragraph 107. See also T195.
58 Exhibit 23.1, paragraph 108.
(d) safeguards and guarantees could (perhaps with some difficulty) be written into legislation to reduce the possibility that ASIS could be misused or misdirected to perform irregular tasks of political benefit to a government or of personal benefit to individuals;

(e) additional protection could be provided for staff; and

(f) the Minister could be authorised to issue warrants, as with ASIO.

3.8 The disadvantages of legislation for ASIS which the Minister nominated were that it would:

(a) represent a movement away from the 'neither confirm nor deny' policy;

(b) amount to a 'public' declaration that Australia had a foreign intelligence service and, accordingly, could complicate Australia's foreign relations;

(c) need to be so vague and general as to be virtually meaningless, and of no satisfaction to those (few) clamouring for it;

(d) still need to be supplemented with a directive;

(e) be no substitute for close and effective ministerial control, for close working relationships with clients, or for high ethical standards set by ASIS management; and

(f) not be necessary in order to achieve those advantages – such as enhanced definition, interchange and mobility of staff and added protection for staff – which were sought.59

3.9 The Minister said that he did not find any of these arguments against legislation 'especially compelling'. He saw the balance of argument as favouring a statute and considered that the precedent of the UK legislation (see below) would assist the passage of legislation through the Australian Parliament. He would anticipate Opposition support.60 The Minister was confident, however, that the existing institutional mechanisms required no reinforcement.61 He

59 Exhibit 39.1, answer to question 47.
60 T2489-90.
61 T2476.
remained concerned that legislation might generate expectations of disclosure of information and accountability which could never be satisfied.62

3.10 The Department of Foreign Affairs and Trade (DFAT) presented a similar list of arguments in favour of and against legislation. Like the Minister, the Department considered that, on balance, there seemed to be more advantages than disadvantages in the legislative option.63 The Department of Foreign Affairs and Trade indicated a leaning towards legislation but doubted whether it would really solve any problems. It thought the legislation would need to be quite uninformative about the functions of ASIS, and might have to be so non-specific as to be useless. There would, however, be value in legislative protection for ASIS officers similar to that available to ASIO officers under the Australian Security Intelligence Organization Act 1979.64 DFAT saw legislation as being unlikely to contribute much in practical terms towards meeting the 'totally desirable goal' of greater public accountability and greater public information, and saw in this the risk of raising excessive expectations.65

3.11 The submission from the Department of the Prime Minister and Cabinet referred to the need in considering legislation to balance various interests. On the one hand, ASIS should be seen to be accountable and its powers should be clearly limited. Legislation might achieve this and so allay misconceptions that ASIS was above the law. It might also provide greater protection against disclosure of sensitive information and officers' names, thus increasing the security of the Service. On the other hand, the introduction of legislation to the Parliament could lead to discussion of specific ASIS activities and so might draw attention to sensitive matters. It could also give Parliament the opportunity to place too many restrictions on ASIS or seeking a greater role for itself in overseeing ASIS activities.66

3.12 The Department suggested as an alternative to legislation that ASIS's role and the limits on its activities be set out in a detailed statement to Parliament by the Minister setting out the limits to ASIS's powers. While such a statement would not have the same force as legislation, it would be treated seriously as a considered statement of Government policy.67

62 T2488; T2489-90; T2495.
63 Exhibit 24.1, paragraphs 71, 72.
64 T627.
65 T2570-1.
66 Exhibit 25.2, paragraphs 36, 37.
67 Ibid., paragraph 39.
3.13 The Attorney-General’s Department expressed the view that legislation did not appear to be necessary to provide adequate legal authority for ASIS’s present charter. Advice was given to the first Hope Royal Commission in 1977 by the then Solicitor-General, Sir Maurice Byers QC, that ASIS was validly constituted under sections 61 and 67 of the Constitution. There was, moreover, an inherent difficulty, the Department argued, in legislating for the performance of intelligence-gathering activities. It would not be in Australia’s interests to seek to confer ‘legitimacy’ on the precise means by which such activities were to be conducted.

3.14 According to the Department, legislation could nevertheless:

(a) set out a basic charter of ASIS’s roles and functions with appropriate restrictions;

(b) implement and regulate some form of parliamentary oversight; and

(c) provide express legal regulation of ASIS activities within Australia.

The Department pointed out that reforms could be achieved otherwise than by means of comprehensive legislation for ASIS. For example, an Act could be introduced to establish a parliamentary oversight committee if such a committee were thought desirable, and greater legal protection of official information relating to ASIS could be secured, through the implementation of the Gibbs Committee’s recommendations, in an amended Crimes Act.

3.15 The Federal Opposition has not adopted a formal policy position on the question of legislation for ASIS. The former Shadow Foreign Minister, Mr Reith, told the Inquiry that ‘the general view in the Coalition parties would be that we would be favourably disposed ... to a proposal for legislation to establish the framework for ASIS’.

3.16 The Australian Democrats emphasised the importance of the accountability of ASIS to Parliament. They saw a parliamentary oversight committee as essential to this and considered that ‘the only realistic basis’ for

---

68 Exhibit 27.1, paragraph 12; T2348.
69 Exhibit 27.1, paragraph 15.
70 Ibid., paragraphs 22-23. See Chapter 13 for consideration of the Gibbs Committee recommendations.
71 *T1170*. 

29
establishing such a committee would be by statute.\textsuperscript{72} The Democrats expressed no view on the need for a statutory basis for ASIS itself.

3.17 The Commission took evidence from senior representatives of several major media organisations, principally directed at issues arising under the third term of reference (see Chapters 10 to 13 and 15). With one exception, these witnesses supported the idea of legislation for ASIS, on the grounds that it would enhance the actual and perceived legitimacy of ASIS and would make ASIS more accountable to Parliament, as had occurred with ASIO.\textsuperscript{73} There was recognition that the specification of functions would necessarily be limited, as would the amount of information that could be released to Parliament and the public, and that legislation might therefore raise expectations that would not be met. Legislation would, nevertheless, be an important step in the right direction. One organisation, however, submitted that the difficulties of giving legislative authorisation to the activities of ASIS meant that it should remain under executive direction.\textsuperscript{74}

3.18 Separate submissions supporting legislation were received from three academics and a civil liberties group.\textsuperscript{75} Two of these urged that ASIS be banned from engaging in activities that would break the laws of other countries.\textsuperscript{76} A fifth submission put the view that it would be difficult to give legislative authorisation to the types of activities engaged in by ASIS.\textsuperscript{77}

**Overseas experience**

3.19 ASIS submitted in support of legislation that almost all parliamentary democracies have a legislative basis for their intelligence services.\textsuperscript{78} The following comparisons were offered as relevant:

(a) UK: the *Intelligence Services Act 1994*, continuing in existence the UK Secret Intelligence Service (SIS);

(b) USA: the *National Security Act 1947*, establishing the CIA;

\textsuperscript{72} Exhibit 47.1, p.4.
\textsuperscript{73} T\textsuperscript{*}673*; T\textsuperscript{*}751*; T\textsuperscript{*}755*; T\textsuperscript{*}837*.
\textsuperscript{74} Exhibit 12.10.5, pp.1-2.
\textsuperscript{75} Exhibit 46.1; Exhibit 46.2; Exhibit 46.3; Exhibit 46.5.
\textsuperscript{76} Exhibit 46.3; Exhibit 46.5.
\textsuperscript{77} Exhibit 46.4.
\textsuperscript{78} Exhibit 6.3.1, paragraph 20.
(c) Canada: the Canadian Security Intelligence Service Act 1984, establishing CSIS;

(d) New Zealand: the New Zealand Security Intelligence Service Act 1969;

(e) Germany: the foreign intelligence service (BND) is supervised by a Parliamentary Control Commission and the Trust Committee of the Budget Commission of Parliament, which have extensive oversight and control powers; and

(f) South Africa: the Government proposes to legislate to govern the activities of the agency which will replace the National Intelligence Service.

3.20 There are, of course, limitations on the utility of these comparisons. Neither Canada nor New Zealand has established a foreign intelligence service and different considerations apply to agencies with domestic security responsibilities. The political and administrative systems in the United States, Germany and South Africa differ from those of Australia in ways that also affect any comparison with ASIS.

3.21 The British example deserves closer consideration in view of the similarities between the parliamentary systems of the UK and Australia. Although widely known and discussed, the existence of SIS was not publicly acknowledged by the British Government until May 1992. At that time, the Prime Minister informed the House of Commons that SIS was distinct and separate from the Security Service and provided foreign intelligence in furtherance of the Government's foreign, defence, security and economic policies. The Prime Minister undertook to introduce legislation to place SIS on a statutory basis. This ultimately took the form of the Intelligence Services Act 1994.

3.22 As well as removing uncertainty about the position of SIS under European law, the legislation was seen as a means of promoting greater accountability. In introducing the Bill, the Foreign Secretary described it as 'the next logical step in this policy of greater openness in security and intelligence

---

79 Exhibit 5.7.1.2, column 65.
matters, wherever possible'. In the House of Lords, the Lord Chancellor described the objective of the bill as:

to ensure that Parliament establishes the framework within which the intelligence services must operate. It establishes clearly the arrangements for ministerial control and decides where the balance must lie between greater openness and continued secrecy.

The Lord Chancellor also thought it 'worth emphasising that both SIS and [Government Communications Headquarters] welcome this Bill which they have been awaiting for some time'.

3.23 The parliamentary debate on the Bill reflected general acceptance across the political spectrum of the need for the continued existence of SIS. Much emphasis was laid by Government ministers on the benefits to the nation of the work of the Secret Intelligence Service, and this was not seriously questioned.

The ASIO experience

3.24 The legislation for ASIO provides another relevant comparison. ASIO was established in 1949 and operated for some years under a charter issued by the Prime Minister, similar to that later issued for ASIS. Legislation in 1956 continued ASIO in existence and conferred telephone interception powers. In the 1970s, following the first Hope Royal Commission, the legislation was amended to provide for warrant authorisation for intrusive methods, a public annual report, briefings for the Opposition, controls on dissemination of information, and the establishment of the Security Appeals Tribunal. In the 1980s, after the second Hope Royal Commission, additional legislation established IGIS, a parliamentary oversight committee, and controls on ASIO’s investigation of political movements.

3.25 The Director-General of ASIO considers that being under this legislative regime is very much to the advantage of the organisation. The legislation gives legitimacy to ASIO and an assurance to the public that it is legally accountable. Legislation gives:

---

80 Exhibit 5.7.1.4, column 154.
81 Exhibit 5.7.1.3, column 1026.
82 Ibid, column 1028.
[a] clear indication to members of the public that this is not a freewheeling body in government or in society – it is subject to control and accountability, to the laws of the land – and that having been established by Act of Parliament it is something which the Parliament and therefore, in the end, the public, the people if you like, have agreed ought to be set up. Therefore it has a legitimate role to play.84

The Director-General identified other benefits. Being known to be a legal body allows ASIO to gain better co-operation from the public when this is required, and the ability to counter negative media comment by pointing to the legislative limits on ASIO is beneficial for staff morale.85

3.26 In his first report, Mr Justice Hope cited the ASIO legislation as an illustration of the feasibility of operating an intelligence agency secretly but under the authority of a statute.86 In his 1984 report, he described the enactment of the ASIO Act as one of the reasons for the increase in ASIO’s concern for compliance with the requirements of the law and of propriety.87 He concluded that public and political awareness of ASIO had imposed a greater accountability on the organisation.

The arguments for and against

3.27 The arguments for and against a legislative basis for ASIS can now be summarised. The arguments in favour of legislation are that it would:

(a) give legislative authority of the type which should exist for the activities of all significant, continuing government agencies;

(b) restrict ASIS activities to functions authorised by the legislature and establish appropriate arrangements for accountability, thus providing the opportunity to refute the common misconception that the Service is a ‘loose cannon’;

(c) confer legitimacy on ASIS in the eyes of the community, and reduce the suspicion surrounding its activities;

(d) provide increased protection for ASIS officers, sources, methods and product;

84 T2583.
85 T2583-4.
86 Exhibit 2.1.1, paragraph 303.
87 Exhibit 2.2.1.1, paragraphs 2, 3-5.
(e) provide stability and continuity for the organisation, with consequent improvements to staff morale;

(f) bring ASIS into line with ASIO and with intelligence services in most other parliamentary democracies.

3.28 The arguments against legislation for ASIS are that:

(a) it is simply unnecessary or, alternatively, the specific issues requiring legislative treatment do not justify comprehensive ASIS legislation;

(b) it would be likely to raise expectations in the community – as to accountability and the flow of information – which could not be met;

(c) it could not be framed with sufficient specificity to be of practical value without also causing undesirable international repercussions;

(d) it would invite intrusive parliamentary debate on the existence, role and function of ASIS; and

(e) it would represent a significant move away from the 'neither-confirm-nor-deny' policy which is essential to security.

3.29 After considering these arguments, we have concluded that legislation to continue ASIS in existence and to provide authority for its activities is desirable in principle and will be of benefit in practice. ASIS carries out important functions in the national interest. Its operations are usually sensitive and potentially controversial. It is no longer appropriate that the formal conferral of authority for the exercise of these functions should be the exclusive province of the executive arm of government. The existence of ASIS should be endorsed by Parliament and the scope and limits of its functions defined by legislation. International comparisons demonstrate how widely this principle is now accepted in parliamentary democracies.

3.30 ASIS is now the only substantial, continuing agency in the Commonwealth public sector not subject either to enabling statute or to general statutory control through public service or corporations legislation. Both main forms of government organisation – departments of state and statutory bodies – are governed by extensive legislative controls. Government-owned corporations
are subject to the corporations law and to additional requirements for public reporting to Parliament.

3.31 As we have already pointed out, our recommendation in favour of legislation should not be taken as implying that the present accountability arrangements have failed or that ASIS is out of control. All the evidence is that ASIS has been carefully managed and responsive to the direction of successive governments; arrangements for ASIS within the executive, at least those current since the second Hope Report, have been comprehensive and, in our view, effective.

3.32 We consider, however, that the move from executive to legislative authority would add a significant new dimension to the accountability framework, bringing with it qualities of legitimacy and transparency which the Service needs. The enactment of legislation should serve to reassure the public, in a way that statements by the Minister or the Director-General cannot do, that the activities of ASIS are properly authorised and controlled. By defining key elements of the arrangements for control and oversight – involving the Minister, the Director-General and, as we shall recommend, the Parliament itself – the legislation should help to dispel the persistent mythology that ASIS is unaccountable and out of control.

3.33 None of the other arguments for legislation is as compelling. Specific legislative requirements, to confer legal protection on ASIS officers, sources and methods or to deal with unauthorised disclosures, could be addressed in separate measures. But once it is accepted that ASIS should, as a matter of principle, operate under the authority of legislation, it is obviously sensible that the legislation should deal comprehensively with all such ASIS-related issues.

3.34 We have not neglected the arguments advanced against legislation. Of these, perhaps the most important is the difficulty of satisfying public expectations. Care will need to be taken to dispel any public impression that the introduction of legislation implies a complete opening up of ASIS to public view. Careful preparation and management of its introduction should ensure that the Parliament and the public for the most part see even generalised legislation as providing advantage. Importantly, we are aware of no suggestion in Britain that the generalised statement of the functions of SIS in the Intelligence Services Act 1994 was seen as discrediting that legislative exercise. The terms in which the

88 See paragraph 2.43 above.
89 See Chapter 5.
functions and purposes of ASIS are defined would nevertheless need to be formulated in a way which enabled the maximum possible to be said about what ASIS can and cannot do.

3.35 The case for legislation will be strengthened if our recommendation for the creation of a parliamentary committee on ASIS is accepted. As was recognised when the Joint Committees on ASIO and on the National Crime Authority were established, it is desirable that the membership, terms of reference, powers and procedures of committees overseeing sensitive areas be defined by legislation.

3.36 It is to be expected that the introduction of legislation on ASIS will encourage parliamentary debate about the functions of the Service. In a healthy democracy, such debate should be welcomed. If there are misgivings in the community about ASIS, then it is proper that they be aired. The likelihood is that, as in the debate in the British Parliament, there will be no serious challenge to the existence of ASIS. The debate will, on the contrary, provide the Government with an opportunity to reaffirm the rationale for the collection of foreign intelligence, to define its objectives and to explain the benefits to the national interest, both generally and by example. In the British Parliament the Foreign Secretary used examples drawn from actual operations to demonstrate how SIS served the national interest in the fields of counter-terrorism, counter-proliferation and the detection of drug trafficking. A parliamentary debate would also provide a suitable opportunity to dispel some of the misconceptions about ASIS and to deny some particular allegations.

3.37 We referred earlier to the suggestion that parliamentary debate over ASIS might draw attention to sensitive matters. A distinction needs to be drawn between speculation by parliamentarians about what ASIS might be doing – which might well occur in a debate about its legislative charter – and disclosure of operational information. There is no reason to believe that the introduction of legislation would lead to undesirable disclosures, and speculation can be treated as such with reference to the statutory definition of functions and, where appropriate, to the examples given officially.

3.38 Application of the neither-confirm-nor-deny policy is not inconsistent with legislation, nor would legislation necessarily weaken it. Legislation, as we envisage it, would merely confirm in a formal way matters which are, with no serious exception, on the public record already. It would remain within the

---

90 Exhibit 5.7.1.4, columns 155-7.
Government's discretion to comment or not, as it chose, on other issues which might be raised in parliamentary debate or elsewhere.

**The content of legislation**

3.39 The Fifth Report of the first Hope Royal Commission was accompanied by a draft bill to continue ASIS in existence. We have had a new draft bill prepared, which draws heavily on the ASIO Act and, to a lesser extent, on the *Intelligence Services Act 1994* (UK) and the Hope draft. It has been prepared for the purpose both of clarifying our own thinking and of providing assistance to the Government in the event that our recommendation for legislation is accepted.
Chapter 4
Briefing the Opposition

The current arrangements

4.1 When ASIS was established in 1952, the prime ministerial charter made no provision for Parliament or the public to be informed of its existence or activities. If the Opposition was officially made cognisant of ASIS in its early years, the arrangements for doing so did not last. Mr Whitlam became Leader of the Opposition early in 1967 but did not receive an official briefing on ASIS until after the change of government in December 1972, long after he had learned of its existence from unofficial – including foreign – sources.91

4.2 The Whitlam Government adopted the policy of authorising briefings on intelligence matters for the Leader of the Opposition. This policy was strongly endorsed by Mr Justice Hope in his 1977 report and has been followed by all governments since. The current Directive provides, in the following terms, for the Leader of the Opposition to be briefed on matters relating to ASIS:

The Director-General shall, as authorised by the Prime Minister, provide briefings in relation to ASIS to the Leader of the Opposition. The Director-General shall inform the Prime Minister and the Minister for Foreign Affairs of matters covered in those briefings.92

4.3 In practice, according to the Secretary of the Department of the Prime Minister and Cabinet,93 the Leader of the Opposition and the Shadow Foreign Minister are kept informed of significant developments affecting ASIS. Except in some special circumstances, briefings are provided to the Opposition only on request and at the discretion of the Prime Minister. Briefings are usually

92 Exhibit 1.8, Attachment B, p.32.
93 Exhibit 25.2, p.15. See also Exhibit 25.3, p.7.
provided by the Director-General, and do not usually address operational matters. In some cases the Leader of the Opposition has been informed of important developments on the initiative of the Government. This was done as a courtesy. There was no legal or other requirement to do so. The Leader of the Opposition and the Shadow Foreign Minister have been provided with briefings relating to the Inspector-General’s investigations of the complaints of some former ASIS officers. A briefing was also provided to an Opposition senator who had raised the complainants’ cases in Parliament.

4.4 These arrangements, which are dependent on the Prime Minister’s discretion, may be contrasted with the statutory requirement for briefings by ASIO, imposed by s.21 of the ASIO Act. That Act also provides (s.94) for the Leader of the Opposition to receive a copy of the full, classified version of the ASIO annual report, at the same time obliging the Leader to keep the classified sections of the report secret.

The case for formal briefings

4.5 The Director-General considers that his responsibility for briefing the Opposition should be more clearly defined. He would prefer to see ASIS on the same basis as ASIO, with a set schedule of meetings to brief nominated members of the Opposition. Formalising the ASIS briefing process would remove any uncertainty as to how the Director-General should conduct himself to avoid allegations of political partisanship.

4.6 In the Minister’s view, ‘provided that the principle of bipartisanship in matters of intelligence and security is both honoured and served,’ there would be advantages in twice-yearly briefings on the ASIO model. Such briefings should focus on the Service’s major intelligence-gathering objectives and related geographical deployments.

4.7 The Hon. Andrew Peacock (himself a former Foreign Minister) advised the Inquiry that, when he became Shadow Minister in March 1993, he was surprised to find that no process existed for regular briefing of the Opposition. Eight months had elapsed before ASIS briefed the then Opposition Leader and himself. He also suggested that the Commission consider whether such

---

94 Exhibit 20.1, pp.9-10.
95 T74; T*973*.
96 Exhibit 20.1, p.10.
97 Exhibit 39.1, paragraph 34.
arrangements should be put on a more regular footing. Mr Peter Reith, proposed that briefings should take place every six months, with additional briefings following requests in writing to the Minister. Mr Reith argued that the Leader of the Opposition, the Shadow Foreign Minister and, perhaps, the Shadow Defence Minister should have a reasonable understanding of the operations of ASIS.

4.8 In our view, the Opposition should have assured access to briefings by ASIS. Three considerations are relevant. First, the obligation on the Service to explain itself to senior members of Parliament who are not part of the Government is a form of parliamentary accountability. Although this must take place under conditions of secrecy, it provides some assurance to the Parliament and the public that such accountability exists. A second reason for a right of Opposition access to briefings is the importance of bipartisanship on issues of national security. Significant national security issues are involved in ASIS's activities and the need for secrecy is obvious. The briefing process, while not necessarily achieving a uniformity of view, helps promote a bipartisan approach. This in turn can be expected to reassure the foreign governments with which Australia has liaison arrangements and so to enhance the value of those arrangements. Thirdly, the briefing process is a means by which the alternative government can maintain a familiarity with this agency of government in the same way as, under well-established convention, it is kept informed of the activities of other public sector agencies.

4.9 We recommend that a system be established under which the Opposition Leader and relevant Shadow Ministers are briefed on ASIS by the Director-General regularly and as of right. Briefings on the policy, administration, budgets or the performance— in general terms— of ASIS should not require the prior approval of the Prime Minister or the Minister for Foreign Affairs. The prior approval of the Minister should, however, be obtained before operational matters are dealt with in a briefing.

4.10 Briefings should be arranged at least every six months. The Opposition should also have a right to briefings outside the normal schedule, on request in writing to the Minister. A provision establishing the right of the Opposition Leader to briefings on ASIS is included in the proposed draft bill.

98 Exhibit 44.3, p.1.
99 T*1181*. 
4.11 The draft bill also provides for the Leader of the Opposition to be given the full annual report of ASIS, subject to a duty to keep its contents secret.\textsuperscript{100} This corresponds with the position under the ASIO Act.\textsuperscript{101} An alternative, favoured by the Minister, would be for the Leader to be provided with the section of Part 2 of the ONA Annual Report dealing with ASIS, to be supplemented as necessary by oral briefings.\textsuperscript{102} As a further alternative, an edited version of the ASIS annual report could be provided with operational detail removed, supplemented in the same way. The full access for which the draft bill provides is consistent with the views we have expressed regarding briefings, and there is nothing in the ASIO experience to suggest that such access will give rise to security concerns.

4.12 The Inspector-General of Intelligence and Security (IGIS) has participated in briefing of the Opposition on particular matters, with ministerial approval.\textsuperscript{103} This practice seems to us to be valuable and consistent with practices followed in other government agencies. We recommend that the Opposition should have a right to be briefed by IGIS, on request in writing to the Minister. Any briefing by IGIS should be subject to the same constraints on reference to ASIS operational matters as would apply to a briefing by ASIS.

4.13 There may be occasions on which it would be appropriate for members of Parliament, other than the Opposition Leader or a shadow minister, to be briefed on matters concerning ASIS. Specific ministerial approval should be required for any such briefing.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{100} Similar provisions should be included in a stand-alone directive, if legislation were not proceeded with.
\item \textsuperscript{101} s.94(2).
\item \textsuperscript{102} Exhibit 39.1, answer to question 36
\item \textsuperscript{103} T2855-6.
\end{itemize}
\end{footnotesize}
Chapter 5
Parliamentary Scrutiny

Accountability and responsible government

5.1 The concept of ministerial responsibility, which is entrenched in the Australian parliamentary system, creates relationships of accountability between the Parliament, ministers and officials. The general principles underlying these relationships are set out in the MAB/MIAC paper on accountability and may be summarised as follows:

(a) Ministers are accountable to the Parliament for the overall administration of their portfolios, in terms both of policy and of management;

(b) the duty of the public servant is to assist ministers to fulfil their obligation to be accountable by providing full and accurate information to the Parliament about the factual and technical background to policies and their administration;

(c) heads of agencies and their staff are accountable to the Parliament through their ministers, according to long-established convention. For example, a head of agency's annual report, detailing among other things administrative efficiency, is addressed to the minister who, in turn, presents the report to the Parliament.104

5.2 The Minister for Foreign Affairs, Senator the Hon. Gareth Evans, accepted in his evidence that the arguments, both principled and pragmatic, for greater accountability to the Parliament entail that creative efforts be made to maximise that accountability while protecting what needs to remain secret. He accepted that he should be accountable to the Parliament for ASIS to the

---

104 Exhibit 3.3.5, pp.6, 14; see also T1575-6.
maximum extent possible consistent with the requirements of operational security. The then Shadow Minister for Foreign Affairs, Mr Peter Reith, and the Australian Democrats in a written submission, advocated strengthening parliamentary accountability for ASIS. Mr Reith identified four areas in which arrangements for accountability could be improved, including the establishment of a parliamentary oversight committee. The Democrats cited a general trend towards greater accountability in government and advocated the establishment of one parliamentary committee to oversee the whole intelligence community.

5.3 The Secretary of the Department of the Prime Minister and Cabinet, Dr Michael Keating, agreed that accountability to the Parliament should be maximised, consistent with security. The Secretary of the Department of Finance, Mr Stephen Sedgwick, expressed similar views. Both accepted that the general principles of parliamentary accountability should apply to ASIS except to the extent that a case for exemption was made out.

5.4 Witnesses generally acknowledged that advantages flow from effective arrangements for accountability to Parliament. Mr Sedgwick, for example, described as one of the ‘very useful’ outcomes of public sector reform in recent years:

the discipline that’s imposed on organisations when they are required to write down what they do and the test by which they can be judged in that activity. Specifying what your objectives are and being able to defend them to somebody else is a useful device for clarifying thought and, in the course of that, improving organisational effectiveness, because you get greater clarity within the organisation of what it’s about and what it’s not.

Relating this to ASIS, he saw improvements to parliamentary accountability as potentially:

useful in requiring organisations and executive government to be clearer about what the role is of ASIS and how it goes about its business, in very broad terms, which can simply help the management of this organisation. I don’t believe that ASIS will be any different to any other organisation [or] that the executive government would find scrutiny any less valuable in this case than it does with any other part of the public administration.

105 T2494.5.
106 T1170*.
107 Exhibit 47.1, pp.1-3.
108 T1581-3.
109 T1197.
110 T1199.
111 Ibid.
5.5 The main difficulty in achieving fully the advantages of parliamentary accountability for ASIS, as witnesses also generally agreed, is the necessity to preserve a high level of secrecy about the activities of the Service. Over the course of ASIS's existence, there has been a gradual increase in the amount of information provided to the Parliament. But the requirements of secrecy apply especially to operational information and, so long as that is accepted as necessary, the nature and value of parliamentary scrutiny of ASIS will be more limited than for organisations where secrecy cannot be justified.

**Secrecy and ministerial responsibility**

5.6 The traditional vehicles through which ministers meet their obligations of accountability to the Parliament include parliamentary questions and debates and the provision of detailed information in the context of budget estimates. These mechanisms draw support from the tabling in the Parliament of reports of independent review bodies external to the agency under review.

5.7 In theory, a minister has been accountable to the Parliament for ASIS at all times since its establishment. Until the late 1970s, however, this was meaningless in practice because of the absence of authoritative information on the Service and a government policy (accepted by the Parliament) of refusing to comment on matters relating to intelligence and security. The public acknowledgment of ASIS in 1977, and the regularisation of its budget appropriations in the 1978-79 financial year, increased the scope for parliamentary questioning of governments on matters connected with ASIS. Briefing of the Opposition on ASIS and reports to the Parliament by the Auditor-General since 1978 and annual reports by the Inspector-General of Intelligence and Security (IGIS) since 1987 have also enhanced the accountability of the Service to the Parliament.

5.8 The Minister acknowledged, however, that his accountability to the Parliament for ASIS was, by ordinary public sector standards, very attenuated. He maintained that opportunities for accountability would arise:

> when things go overtly wrong - as with the Sheraton affair - and Ministerial responses will be tested accordingly. In any event, Ministerial survival has always depended in practice more on satisfactory accountability to one's Prime Minister (and to a lesser extent, Party colleagues) than to the Parliament: that mechanism

---

112 See Chapter 4.
113 Exhibit 39.1, answer to question 37; T2494.
will be applicable whatever the degree of secrecy maintained in public on
security-sensitive matters.\textsuperscript{114}

5.9 The comments on the Sheraton incident by Mr Bill Hayden, when he
was Minister for Foreign Affairs, like the responses by Senator Evans to the
media reports that helped to precipitate the present inquiry, departed to some
extent from the neither-confirm-nor-deny policy. There have been a few other
such departures,\textsuperscript{115} but in general the policy has greatly reduced the scope for
direct parliamentary scrutiny. This is true both of parliamentary questions and
of the kind of scrutiny which might be based on reports of investigations by IGIS
and the Auditor-General. ASIS also remains outside the coverage of other
external review bodies such as the Ombudsman, the Privacy Commissioner, and
the Human Rights and Equal Opportunity Commission, which collectively were
described in the MAB/MIAC paper as ‘an integral and vitally important part of
the modern accountability process’.\textsuperscript{116}

**Overseas comparisons**

**The United States**

5.10 The Central Intelligence Agency (CIA) answers to permanent select
committees and to separate appropriation committees of each House of
Congress.\textsuperscript{117} It is subject to the *Intelligence Oversight Act 1980* and to
accountability provisions in its own Act (the *National Security Act 1947*).
Members of the select committees, which have wide powers of oversight and
review, are appointed by the presiding officers of the respective Houses, subject
to maximum terms of membership of six years for the House Committee and
eight years for the Senate Committee. Each committee is given access, under
secure conditions, to extensive information on intelligence activities. A function
of the select committees is to authorise the CIA’s annual budget, separately from
the work of the appropriations committees. In this lengthy process, the CIA is

---

\textsuperscript{114} Exhibit 39.1, answer to question 37.

\textsuperscript{115} The then Prime Minister, Mr Malcolm Fraser, responded in 1981 to Opposition questioning on reports
that a UKSIS officer who had been associated with the establishment of ASIS had been a Soviet agent, by
saying that the allegations had been known to Commissioner Hope and they had ‘no present significance
for Australia’ (House of Representatives *Hansard*, 31.3.81, p.1086). In November 1983, Senator Evans
responded to public comments by the Hon. Clyde Cameron, telling the Senate that no Australian
intelligence agency was involved in any activity whatever in Chile at or around the time of the coup
against President Allende, and that any intelligence cooperation that may have occurred at an earlier time
did not involve assisting any other country in operations or activity directed against the Allende
Government (Senate *Hansard*, 29.11.83, p.2902).

\textsuperscript{116} Exhibit 3.3.5, p.9.

\textsuperscript{117} Except where otherwise noted, this section is based on Exhibit 6.3.1, Attachment C.
required to provide detailed justification of its budget to each committee. This power over the CIA's budget greatly strengthens the capacity of the committees to oversee the Agency.

5.11 There is no formal limit to the information which the committees can request. In practice, limits to access have been negotiated between them and the Agency. The committees are told in general terms about the methods used, the types of operations conducted and the sources which the Agency has. Particular sources and methods are not identified except in exceptional circumstances, when the information will be confined, for example, to a senior staff member and the chair and ranking minority member of the committee. The General Counsel to the Senate Select Committee said he had not, in eight years working for the committee, encountered an information problem which he could not negotiate satisfactorily with the CIA.

5.12 During his visit to the US, Commissioner Samuels discussed the system of congressional oversight with senior officers of the CIA, the National Security Council and the select committees. Apart from concerns about the significant administrative burdens which the system imposes on the Agency, the comments, both from within and outside the CIA, were overwhelmingly positive. For example:

(a) there is a strong message of accountability which is reinforced by congressional oversight;

(b) oversight helps the Agency to do its job better. Having to account to congressional committees concentrates the minds of managers in the Agency, who pay more attention to detail as a result;

(c) Congress is the advocate for the intelligence agencies, which do not have any other constituency. Congress legitimises the intelligence budget and is a layer of support and protection for the agencies;

(d) it is appropriate, and beneficial, for the Agency to have to justify what it is doing. The Agency can learn things from the members of the committees, who often have good questions to ask;

(e) the committees have a very good record of not leaking, with the result that the intelligence community has become progressively more trusting of them.
5.13 Most Directors of Central Intelligence in recent years have accepted that there are benefits in the system of congressional oversight. Admiral Turner, who was Director of Central Intelligence when much of the present oversight machinery was established, wrote in 1985:

If we want to have good intelligence over the long run, our only option is to make oversight work. The congressional committees on intelligence are in the best position to oversee, responsibly and adequately, what the intelligence agencies are doing.\footnote{Turner, Stansfield, *Secrecy and Democracy: The CIA in Transition*, Houghton Mifflin, Boston, 1985, pp.270-1.}

Mr William Colby, a career CIA officer who headed the Agency during contentious congressional and executive investigations before Admiral Turner’s appointment, expressed similar conclusions in his memoirs:

These committees, with the clear responsibility for reviewing intelligence activities, can replace previous congressional ‘oversight’ (in both senses of the word) with the kind of congressional consultation and responsibility in American decisions about intelligence operations called for by the Constitution.\footnote{Colby, William, and Forbath, Peter, *Honourable Men: My Life in the CIA*, Hutchinson, London, 1978, p.458.}

5.14 A more recent incumbent, Mr Robert Gates (1991-1993), who had also been a career CIA officer, commented in 1993:

Over the past 16 years, CIA accountability and legislative oversight have grown enormously. With this oversight, CIA and the other intelligence agencies have become the most scrutinised intelligence services in the world ... And, yet, I believe, under these circumstances we not only remain effective and capable, we enjoy a legitimacy and an acknowledged role in our government not shared by any foreign intelligence service.\footnote{Gates, Robert M., Speech to World Affairs Council of Boston, 15.1.93, Boston, Appendix 10 to Select Committee on Intelligence of the United States Senate, Legislative Oversight of Intelligence Activities: The U.S. Experience, October 1994.}

5.15 We emphasise, however, that the scrutiny undertaken by these committees is compelled by budgetary considerations. The main positive effect upon the CIA is to shape its skills in presenting a persuasive program. The committees’ oversight role does not appear to have imposed restraints, in every case, upon the CIA’s less successful initiatives.
The United Kingdom

5.16 Section 10 of the Intelligence Services Act 1994 establishes the Intelligence and Security Committee. Its function is to examine the expenditure, administration and policy of the Security Service, Secret Intelligence Service and Government Communications Headquarters. The Committee is to consist of nine members of Parliament, none of them ministers, who are to be appointed by the Prime Minister after consultation with the Leader of the Opposition. Information sought by the Committee can be withhold because it is sensitive information, that is, information which might lead to the identification of sources, other assistance or operational methods, information about particular operations, or information supplied by another government where that Government does not consent to its disclosure. Information may also be withheld where the Minister has determined that it should not be disclosed, but the Minister may not make such a determination on the grounds of national security alone. Sensitive information may be disclosed to the Committee if the Government considers it safe to do so.

5.17 This Committee has several distinctive features. First, it will be a committee of parliamentarians, not a parliamentary committee, since the members will be appointed by the Prime Minister rather than elected by Parliament. Secondly, the Committee will report to the Prime Minister rather than to Parliament, although the Prime Minister is required to table at least an edited version of a report by the Committee. Thirdly, the Committee will be staffed from the Cabinet Office, by a member of the staff of the Intelligence Co-ordinator, and not by staff appointed by the Committee as would ordinarily be the case. These arrangements are intended, respectively, to ensure high-calibre membership of the Committee and to maximise the level of security for information provided to the Committee.

Canada

5.18 In Canada, there is no foreign intelligence collection agency. The domestic security service is subject to extensive arrangements for accountability to the Parliament. The legislation which establishes and regulates the Canadian Security Intelligence Service (CSIS) provides for a permanent Security Intelligence Review Committee (SIRC) with oversight functions. SIRC reports annually to the Parliament. Its members must be Privy Councillors, an office usually, but not exclusively, reserved for former Cabinet Ministers. In recent times the members of SIRC have been respected citizens who have been created Privy Councillors for the purpose.
5.19 The Parliamentary Committee which reviewed the operation of the CSIS Act after five years, as required by the Act, recommended the establishment of a parliamentary committee to oversee CSIS. In response to the failure of the then Government to implement that recommendation, Parliament resolved to create a Sub-Committee of its own Justice Committee, as the sub-committee on National Security. This is not a standing committee and has to be mandated afresh by each Parliament. The Committee's mandate, as defined by resolution of the Justice Committee, is to review and consider the management and operations of CSIS and SIRC, including by reference to reports to Parliament by the two bodies and statements to Parliament by the Minister in charge of CSIS.

5.20 During his visit to Ottawa, Commissioner Samuels met with the Chairman and members of the Parliamentary Sub-Committee on National Security. There being no legislative framework, the Sub-Committee is defining its own functions and powers progressively. The Sub-Committee will rely on the prerogatives of the Parliament to require individuals to appear or produce documents. An important issue to be negotiated is the relationship between the functions of the Sub-Committee and those of SIRC. Sub-Committee members emphasised that the public nature of what it does and its accountability to the electorate put it in a different position from the other elements in the accountability framework. At the same time, the Chairman made it clear that he did not see it as workable for the Sub-Committee to get into an adversarial relationship either with CSIS or with SIRC.

The ASIO committee

5.21 Although the arrangements under which ASIO was inaugurated were similar to those still applying to ASIS, they have been changed to bring the Organization closer to the standard system of accountability for public agencies. The prime ministerial charter under which ASIS was established in 1952 followed closely the wording of a similar document which had earlier established ASIO. That Organization, however, was brought under legislation in 1956 and progressive changes to the legislation, including a new Act in 1979, have created an extensive public accountability structure for ASIO. The ASIO Act now specifies ASIO's functions and precludes it from some activities. It also establishes a standing parliamentary joint committee which may review aspects of the activities of ASIO on a reference from the Attorney-General or either House of Parliament.

5.22 The Committee is precluded from reviewing any matter related to ASIO's obtaining or communicating foreign intelligence, any aspect of ASIO's activities not affecting a person who is an Australian or permanent resident, and
any matter which is operationally sensitive. Nor can the Committee originate an
inquiry into individual complaints about ASIO activities. The Minister may ‘for
reasons relevant to security’ issue a conclusive certificate, preventing the
Committee from receiving evidence. The Committee’s members are appointed
by each House of Parliament on the nomination of the Government. The
Government’s nominations must be made after consultation with the leaders of
recognised parties in the Parliament and taking into account the representation
of parties in the Parliament.

5.23 The Committee is not permitted to disclose in a report to the
Parliament the identity of an ASIO officer (other than the Director-General), an
employee or an agent. It is also not to disclose classified information,
operationally sensitive information, or information the public disclosure of
which would be likely to prejudice the operations of ASIO. Before tabling any
report, it must seek the Attorney-General’s opinion on whether the report
discloses any information of these kinds.

5.24 In its seven years of operation, the Committee has reported on two
inquiries and begun a third. Each inquiry was initiated with the approval and
support of the Government. Some evidence emphasised the limits to the
Committee’s effectiveness.\textsuperscript{121}

A parliamentary committee for ASIS

5.25 The views of ASIS about parliamentary oversight developed as this
inquiry progressed. The Director-General’s initial statement asserted that the
existing arrangements for control and accountability of the Service were
‘extensive, effective and adequate’, and sufficiently formalised to ensure proper
accountability.\textsuperscript{122} Nevertheless, the Director-General accepted that a form of
parliamentary review was ‘a necessary part of the legislative basis which the
Service favours’,\textsuperscript{123} and would potentially be of benefit to the Service:

Members of Parliament have not always approved of the Service, and that may to
some extent be an attitude fostered by the absence of any formal accounting
procedures to Parliament ... A more positive attitude by ... parliamentarians
would assist the Service in its duties, and would assist morale of its officers.\textsuperscript{124}

\textsuperscript{121} Exhibit 20.1, para 6.2; Exhibit 20.1.9, para 49.
\textsuperscript{122} Exhibit 20.1.9, paragraph 49
\textsuperscript{123} Exhibit 20.1, paragraph 10.3-4.
5.26 In a later submission on legislative options, the Service proposed that any statute establishing and regulating ASIS should provide for a parliamentary committee. ASIS envisaged a committee which would review the performance of the Service’s duties and functions and would complement the role currently held by IGIS.\textsuperscript{125} It argued that the objective of bipartisan political support for the arrangements for control and accountability would be advanced by the existence of a parliamentary committee.\textsuperscript{126}

5.27 ASIS identified one potential benefit of such a committee as being its ability to deal with issues arising in the political arena.\textsuperscript{127} The Director-General raised the possibility that the chairperson of the committee might be someone who could speak publicly on issues concerning the Service.\textsuperscript{128} He acknowledged that questioning by a committee might also be of assistance in causing the Service to reconsider a particular matter but laid greater stress on the advantage he saw in having an opportunity to explain to such a committee what the Service was doing and why.\textsuperscript{129}

5.28 ASIS argued that the extent to which the committee could be taken into the confidence of the Service would depend on its composition. In particular, ASIS favoured high-level Opposition representation on any parliamentary oversight committee.\textsuperscript{130} In this regard, the Director-General considered that ‘whether you get the right sort of committee ... is absolutely crucial’.\textsuperscript{131} If his preferred model for the committee were adopted, he would expect it to have a wide brief to oversee what the Service was doing. The Director-General was confident that he could win the trust and support of a committee.

5.29 Although the Parliamentary Joint Committee on ASIO is modelled along somewhat different lines, ASIO has found its relationship with that Committee to be of considerable benefit. According to the Director-General of Security, it is a relationship which:

\begin{itemize}
\item \textsuperscript{125} Exhibit 6.3.1, paragraph 31(m).
\item \textsuperscript{126} T*970*.
\item \textsuperscript{127} T*967*.
\item \textsuperscript{128} T*969*.
\item \textsuperscript{129} Ibid.
\item \textsuperscript{130} T67-8; see also Exhibit 21.1, p.4.
\item \textsuperscript{131} T*967*.
\end{itemize}
(a) enables regular contact in depth with a representative group of parliamentarians, which is especially important in a body whose people otherwise have little professional contact with parliamentarians;

(b) brings home to everyone at ASIO that they are subject to the Parliament;

(c) is a sounding board for parliamentary and public opinion on matters of interest to ASIO or liable to affect its working environment;

(d) generates parliamentary and wider understanding and support of ASIO’s role and functions.¹³²

5.30 The Director-General of Security acknowledged, in addition, the benefits of parliamentary scrutiny and review. ‘It is a reminder of who and what you are accountable to.’¹³³ Having to answer to a parliamentary committee was good for ASIO, obliging people ‘to think carefully and consider what they are doing and therefore to improve the way in which their work is done and the outcome’.¹³⁴

5.31 The Minister for Foreign Affairs, while warning of raising public and parliamentary expectations unduly, acknowledged that ‘from time to time matters concerning ASIS do arise ... and there may be a case for a Committee to be established that would allow such matters to be addressed under agreed rules of engagement, in circumstances that preserved national security’.¹³⁵ Were such a committee to be established:

Its membership would need to be small, its members selected extremely carefully, its own reporting very limited, its function confined to reviewing and monitoring ASIS’s compliance with its Charter, some management issues, and perhaps some funding issues. Its powers would need to be recommendatory only, and its access to information about operations negligible. The mechanisms for protecting information would need to meet those currently applying to any ASIS material. Staff assisting the Committee would need to be selected rigorously and arrangements made for the security of material.¹³⁶

¹³² Exhibit 34.2, paragraph 30.
¹³³ T2593-4.
¹³⁴ T*330*.
¹³⁵ Ibid.
¹³⁶ Ibid.
5.32 The Minister emphasised that the acceptance of legislation for ASIS did not necessarily mean acceptance of a parliamentary oversight committee. He regarded the case for legislation as stronger than that for a committee, although he was not resolutely opposed to the concept of a committee. He recognised that the establishment of an Intelligence and Security Committee of the British Parliament added weight to the arguments in favour.

5.33 The then Shadow Minister for Foreign Affairs, Mr Reith, while not presenting a formal Opposition position, was inclined to favour a parliamentary committee ‘that had a real job and would therefore require people of standing in the Parliament to be on it’. For security reasons, important aspects of the UK model – appointment of members by the Government and provision of staff from within the executive – might be acceptable to the Opposition. While some in the Opposition might be concerned that involvement in any such committee would leave the Opposition ‘a bit hamstrung by ... prior knowledge’, Mr Reith saw this as outweighed by the benefits of greater accountability. He supported the idea that ASIO and ASIS be covered by a single parliamentary committee and suggested that, if any committee or other new oversight arrangements were to be established, the whole position should be reviewed after three years.

5.34 The Australian Democrats submitted that a statutory intelligence and security committee should be established to oversee the entire intelligence community. They proposed a committee with wide access to information but subject to restrictions on disclosure. In particular, the details of ASIS operations and the names of ASIS operatives should remain strictly confidential.

We are well aware of the limitations of this form of parliamentary scrutiny, given that security concerns would circumscribe the committee’s access to information and evidence, and that limitations on disclosure would limit the impact of its findings. However, it would provide an additional signal to the agencies concerned that scrutiny is more likely in the event that problems arise in the conduct of their operations.

137 T2496.
138 T*1173*.
139 Ibid.
140 T*1173-4*.
141 T*1174-5*.
142 Exhibit 47.1, pp.3-5.
143 Ibid., p.3.
144 Ibid., pp.3-4.
5.35 We sought the views of the Department of Prime Minister and Cabinet and the Department of Finance on a possible parliamentary committee. Neither Department considered that a committee was essential to parliamentary oversight, although the Department of Finance affirmed that the general arguments for accountability apply to ASIS as much as to other Commonwealth agencies. Both Departments proposed alternative accountability mechanisms.

5.36 The Department of the Prime Minister and Cabinet suggested as an alternative the expansion of the present practice of briefing shadow ministers. It stressed that the requirements of secrecy would limit the role of a parliamentary committee and suggested that, unless a system could be developed to protect the secrecy of the information provided to the committee, the balance of considerations would probably weigh strongly against access to anything other than very general information. A committee might be able to review budgets and priorities (without detail of operations and deployments), broad financial and personnel management issues, and reports by IGIS, other than on compliance with the Directive and ministerial directions. Limitations on the committee could be justified in part, the Department argued, because of the limited potential for the activities of ASIS to affect the interests of Australian citizens or residents. Given the far greater potential for ASIO’s activities to affect Australians, it argued, it would be anomalous for a parliamentary committee on ASIS to have powers greater than those of the Joint Committee on ASIO.

5.37 The Department of Finance considered that there was insufficient information available to determine whether it would be appropriate or useful to extend the framework of parliamentary committee oversight to include ASIS. The most that could be achieved at this stage would be the tabling in the Parliament of an unclassified ASIS annual report.

The case for a parliamentary committee

5.38 We have recommended in Chapter 3, that the charter under which ASIS operates should be set out in legislation, in which the Parliament specifies in broad terms what the Service can and cannot do. If the Parliament is to approve ASIS’s charter by passing legislation, the Parliament should also be able to review the way in which the charter is put into practice. A parliamentary committee is one way in which this review could be accomplished.

---

145 Exhibit 29.2.2, paragraphs 15, 16.
146 Exhibit 25.3, pp.7-8.
147 Exhibit 29.2.2, paragraphs 19-20.
5.39 Parliamentary oversight through a special committee is the appropriate vehicle for ASIS because of the sensitivity of the issues involved and the associated need to ensure the security of information provided. The Government could not, in practice, share much of the information necessary to accountability with the whole Parliament nor could that information be published. Parliamentary questioning of ministers and debate on intelligence matters will necessarily be limited for this reason. Under appropriate security arrangements, however, a committee could be provided with fuller information. Oversight by a committee would, moreover, be consistent with the general approach to public sector accountability in Australia and in other parliamentary democracies.

5.40 If legislation is introduced to give parliamentary authority for the continuation of ASIS and to set the parameters within which the Service operates, a parliamentary committee should be responsible for testing the way in which the legislation is administered. This will necessarily involve some review of activities, at least at a general level, as well as review of administration and budgets. A parliamentary committee could draw support in this role from the detailed monitoring and auditing carried out by IGIS and a committee responsible for overseeing ASIS should have access to IGIS reports.

5.41 The reservations about a parliamentary committee expressed by some witnesses from the executive government related largely to the difficulties of maintaining security, and to whether a committee could contribute in any significant way to management improvement. It was also argued that, because ASIS has relatively little scope to affect the rights of Australians, oversight by a parliamentary committee would have little to contribute to the public interest.\footnote{Exhibit 25.2, paragraph 43.} Any committee to oversee ASIS would require a legislative base including provisions to address security concerns by setting limits to the disclosure of information and prescribing penalties for unauthorised disclosure. Given an appropriate legislative base, the Australian and overseas experience suggests that security could be reasonably assured. Improving the management of ASIS would not be the primary role of a parliamentary oversight committee, although experience again suggests – including the experience of ASIO as submitted to us – that it could make a contribution in this direction. Although ASIS has few responsibilities with implications for the rights of Australians, its activities have the potential to affect their interests significantly, including, for example, through the effects on international relations that could be caused by an operational failure.
5.42 A further question in relation to a parliamentary committee for ASIS is whether the Service would require full-time parliamentary oversight. The Attorney-General's Department pointed out that few agencies have a direct responsibility to the parliament via a parliamentary committee. Most agencies, however, are subject to a wide range of general parliamentary accountability mechanisms from which ASIS is largely immune, and this the Department also acknowledged. A committee with specific responsibility for ASIS can thus be justified, although the extent of the committee's operations and the question of whether it should cover other intelligence agencies, especially ASIO, are issues to be considered.

5.43 With parliamentary oversight as with legislation, this inquiry provides an opportunity to implement reform not in response to any immediate crisis, but as a means of applying to ASIS the types of changes that have occurred in general public sector accountability, especially over the past ten years. Parliamentary oversight must be implemented in a way that protects operational security, broadly defined, and the need for oversight processes that will not place security at risk may mean that any parliamentary committee that could be established would not meet the expectations that might be held of it in some quarters. The issue of reconciling security with parliamentary and public expectations must be taken into account in the design and introduction of any accountability reforms.

Committee oversight models

5.44 We have examined four possible models for a parliamentary committee, and have identified the model which in our view is best suited to the task as we have defined it.

The UK model

5.45 The British Parliament has established a committee of parliamentarians, rather than a parliamentary committee, to oversee SIS. The essential elements of this approach are that members of the committee are appointed by and report to the Prime Minister, the committee is staffed from the executive, and there are tight controls on the matters which the committee may review. If adopted here, this would give Parliament a greater degree of assurance than is available from present mechanisms for accountability, while preserving a high level of security. But it would amount to no more than indirect accountability to Parliament for ASIS. Such a committee would not have

149 T2361-2.
the independence from the executive which characterises normal parliamentary oversight. Perceptions of lack of independence and of limited access to information would limit the reassurance which such a committee could give to Parliament or the public. The problem raised by Mr Reith, of the potential for non-government members to be constrained by their participation, would loom largest in this model.

5.46 The arrangement for the committee's staff to be drawn from the executive is a defining feature of this model, although it could be adapted to others. While it might be thought to increase both the security of information held by the committee and the likelihood of its being staffed by persons with relevant expertise, such an arrangement would raise further questions about the independence of the committee from the executive. It could also create conflicts of interest for the committee's staff.

Committee for ad hoc inquiries

5.47 A second model for committee oversight is suggested by the Minister's comment, quoted above, that 'from time to time matters concerning ASIS do arise ... and there may be a case for a Committee to be established that would allow such matters to be addressed under agreed rules of engagement, in circumstances that preserved national security'. An ASIS Act could provide for a parliamentary committee which would be activated by a reference from the Minister or from either House of Parliament to review a particular matter of concern. The legislation would set the basic rules for the committee's membership, operations, access to information and reporting. The detailed terms of reference for each inquiry and the membership of the committee when it was activated would be determined by normal parliamentary processes at the time. A possible task for such a committee would be to review the operation of the legislation after, say, three years.

5.48 This model would provide for detailed review when the Parliament thought it necessary while accepting that ASIS should not require continuous oversight by a parliamentary committee. It would, however, deprive ASIS of the advantages of regular interaction with a representative parliamentary body, and would deprive the Parliament of the opportunity to develop specialist expertise in the membership of a standing oversight committee. A further potential disadvantage is that the committee would normally operate only in the context of alarming or controversial events. To concentrate parliamentary scrutiny on

---

150 Exhibit 39.1, answer to question 41.
such events might give them greater prominence than was necessary, or desirable, and at the same time divert attention from less controversial matters of greater significance.

The ASIO Committee model

5.49 The ASIO Act provides for a joint standing committee to undertake inquiries and to report to the Parliament. The Committee is limited in its access to information, is barred from inquiring into some aspects of ASIO's activities, and may not initiate its own inquiries. Its membership comprises backbench members of both Houses and it is staffed from the parliamentary departments.

5.50 This model, providing for oversight of an intelligence agency by a representative back-bench committee, has advantages of the kinds adverted to by the Director-General of Security. The oversight provided by such a committee is, however, fairly limited, as most submissions, including those of the Opposition and the Australian Democrats, noted. As we observed above, the Director-General of Security seemed attracted to the idea of a higher-level committee that could be given 'more serious work'.

A standing, joint, statutory committee with a broad charter

5.51 A fourth model for committee oversight would be the establishment of a standing, joint, statutory committee with a broad charter to review the activities, expenditure and administration of ASIS. The committee would exercise its functions principally through in camera hearings. It would have enough access to information to assure effective oversight but that access would be under secure conditions and subject to rules capable of preventing release of information without authority. The membership would be small, appointed by the Parliament on the nomination of the Government and with a government majority.

5.52 By operating mainly through hearings, such a committee would maintain a level of oversight similar to that faced by other public sector agencies in the proceedings of Senate estimates committees, except that it would do so in private in recognition of security considerations. Within the constraints of security, the committee would seek to provide normal, robust parliamentary scrutiny. By analogy with Senate legislation committees, which consider the

---

151 See paragraph 5.29 above.
152 T°1175-6°; Exhibit 47.1, pp.4-5.
153 T°326°. See paragraph 5.26 above. Also 5.59.
appropriations, it would be desirable for the relevant minister to attend hearings on the ASIS estimates and to respond to questions as far as practicable. This would substantially strengthen the accountability of the Government for ASIS. This model should also lead to the development of specialist expertise on the part of committee members, a factor which is important to any effective parliamentary oversight.

5.53 The Commission prefers this fourth model. We consider it represents a good balance between the need for effective oversight and the need for security. The first and third models – the UK and ASIO committee approaches – would provide for less effective accountability than is realistically achievable. They would introduce to the control and accountability of ASIS some of the disadvantages of parliamentary committee oversight without gaining in return the maximum possible advantage. The second model – an ad hoc statutory committee – would permit effective parliamentary review from time to time but would forgo the advantages of continuity in the accountability relationship and the development of the expertise of the parliamentary overseers.

Features of the preferred model

5.54 The draft bill provides for a committee on the model which we prefer. Certain features of the draft deserve brief discussion here.

A single intelligence and security committee

5.55 It would be anomalous if ASIS were to be subject to more extensive parliamentary review than ASIO. Since both are small organisations with similar needs for secrecy, it would seem sensible for a single committee to oversee them. If our preferred model is adopted, we recommend that it be in the form of a single intelligence and security committee to cover both ASIS and ASIO. The draft bill has been prepared on that basis. Given the relative size of the two bodies and the likelihood that Parliament will have a greater interest in operations in Australia than in those overseas, such a committee could be expected normally to give more attention to ASIO than to ASIS.

5.56 Extending the coverage of the committee to include ASIO would mean a greater degree of parliamentary oversight of that Organization than is exercised by the present Joint Committee on ASIO, since the proposed new committee would have greater powers and access to information than the existing committee. The Director-General of Security saw benefits in the conferral of additional powers, including a power to initiate inquiries:
I would not see a problem with it being given the power to initiate [inquiries of] its own motion, provided, of course, there were safeguards on ... which areas it could go into. But I think that if you are going to make a ... serious effort to produce a committee of high calibre, and you are going to give it more serious work - both of which I think are desirable ... from the Organization's point of view; I do not have any difficulty with any greater accountability in relation to that - I think that you have to give it rather more power than the current Parliamentary Committee has in order to attract the kind of membership and to get those members to do the kind of work that you would like to see them doing. So I think it would be self-defeating to try to get or put together a higher level committee with the intention that it should deal perhaps with the somewhat more sensitive issues if necessary, without giving it the right to initiate its own inquiry within that wide area.154

5.57 The Committee’s oversight should extend to reviewing the discharge of the functions of IGIS in so far as they relate to ASIS or ASIO. On the Inspector-General’s current and likely future workload, this would imply that the committee would have coverage of the great majority of his activities. But, since IGIS is subject to the normal range of public sector accountability mechanisms, and the purpose of the proposed committee would be to improve the accountability of ASIS and ASIO, there would be no reason for the committee to have full coverage of IGIS.

5.58 The Australian Democrats proposed that such a committee should have a wider remit, embracing the Australian intelligence community as a whole. For us to have given proper consideration to this proposal would have required evidence from a range of agencies and from the Government, and would have taken us more than marginally beyond our terms of reference. But it is a proposition which we believe warrants consideration and which the Government may wish to explore.

5.59 The estimates of ASIO are already examined in public by Senate legislation committees and an unclassified version of ASIO’s annual report is tabled in Parliament and published. These practices should continue in respect of ASIO, even if the proposed new committee has greater access to information in private. The scope for reviewing the ASIS estimates in public would be much smaller and the ASIS annual report contains much operationally sensitive material. Whilst we believe that the Government should consider the possibility of publishing an unclassified version of ASIS’s annual report, the security limits on what could be published would make review of that report by a Senate

154 T*326*. 
legislation committee less fruitful than review by a specialised committee which would have greater access to information in private.

5.60 If the ad hoc committee model were to be adopted instead, it should be implemented for ASIS only. It is a means of balancing the special need for secrecy of ASIS operations against the need for oversight of a small, highly specialised agency which mostly operates overseas and in ways which do not affect the rights of Australians. Although the evidence suggests a general willingness to consider improvements to the structure of parliamentary oversight for ASIO, there was no strong pressure for change and there would be no need to adapt the ad hoc model to ASIO’s circumstances. With that exception, the committee provisions in the draft bill would need little change to convert them to the ad hoc model.

**Powers, functions and access**

5.61 The draft bill seeks to balance wide powers, functions and access for the committee against restraints on the publication of information it receives. The draft bill gives the committee the wide function of reviewing and reporting to Parliament on the activities, expenditure and administration of ASIS, the power to initiate its own inquiries under these heads, and full access to information necessary to its functions. At the same time, it prohibits the committee from inquiring into operationally sensitive matters or reporting in a way which would disclose the identity of ASIS or ASIO officers and sources, operationally sensitive information or information that would be likely to prejudice national security or the conduct of Australia’s foreign relations. ‘Operationally sensitive’ is defined for this purpose to include the sources of information and operational assistance or methods available to ASIS and ASIO, information about particular operations and any information provided by a foreign government which that government is not prepared to have disclosed.\(^{155}\) Before presenting a report, the committee would be required to seek the advice of the Minister on whether it contained any information in these categories. If the Minister advised that it did contain such information, the committee would be prohibited from publishing the report.

5.62 The committee would have power to take evidence and to obtain documents but the relevant minister would have the power to prevent the committee from receiving operationally sensitive information if its disclosure to the committee would be likely to prejudice national security. The committee

\(^{155}\) This is based on a definition in the *Intelligence Services Act 1994* (U.K.).
would be required to conduct its proceedings in private unless the Minister approved otherwise. It would not be able to publish evidence without the written consent of those providing it. The restrictions applicable to reporting would apply equally to the publication of evidence. The committee would be required to maintain a level of security over classified documents acceptable to the head of the agency which supplied them.

**Membership and staffing**

5.63 The membership of the committee should be kept as small as possible, principally because the sensitivity of the information available to the committee makes that desirable for security reasons. In any case, the tasks we envisage for the committee should only require a small membership. We have proposed a maximum of eight members, drawn from both Houses, if the committee covers both ASIO and ASIS. A maximum of six would be sufficient if the committee were to cover ASIS only. A committee covering both ASIO and ASIS could operate through sub-committees of six members for each agency, reducing the demands on the full membership and the number of members with access to information on each agency.

5.64 The membership should be equally divided between the government and non-government parties, with the proviso that the chair be a government member and have a casting as well as a deliberative vote, thus assuring a government majority. As is presently prescribed for the Joint Committee on ASIO, the Prime Minister should consult with the leaders of recognised parties in the Parliament before the Government nominates members for appointment to the committee, and should take into account the representation of parties in the Parliament when considering nominations.

5.65 In line with long-standing Australian parliamentary practice and the UK, US and Canadian precedents, it should not be required that committee members be security cleared or vetted. It should be noted, however, that the draft bill follows the ASIO Act in making it an offence, carrying significant penalties, for any person, including a member of the committee, to make an unauthorised disclosure of information received by the committee. One effect of the conviction of a committee member for such an offence would be his or her disqualification from membership of the Parliament under s.44 of the Constitution.

5.66 Committee staff, as well as being covered by the unauthorised disclosure provisions, should be subject to the same level and frequency of security clearance and vetting as ASIS officers. The Auditor-General and ASIS
have agreed that, if the ANAO is given full access to ASIS’s operational accounts, the Auditor-General will consult with the Service before assigning an auditor to that task and will arrange for the auditor to be security cleared and vetted. ASIS proposes that this agreement be given force by regulations under the proposed Auditor-General Act. Similar arrangements, including appropriate regulations, should apply in respect of parliamentary officers appointed to support the committee.

**Initiation of inquiries**

5.67 As well as ongoing review of the activities, expenditure and administration of the agencies, the Committee would be a mechanism by which the Parliament could conduct specific inquiries. This raises the key issue of the power to initiate such inquiries. It is usual for a joint parliamentary committee to undertake inquiries on the reference of either House and, since governments will rarely have a majority in the Senate, application of the usual rules to a committee overseeing ASIS would allow the combined non-government parties in the Senate to initiate inquiries over the objections of the Government.

5.68 The draft bill proposes in addition that the committee have the power to initiate its own inquiries within the limits of its statutory functions. The assurance for the executive that self-initiated inquiries would not present a security problem resides in the prohibition of inquiries into operationally sensitive matters - sources, methods and particular operations - and in the controls over the release of information, both to and by the committee, and the penalties associated with unauthorised disclosure. With these safeguards in place, we believe that the conferral of an ‘own motion’ power will enhance the effectiveness of the committee’s oversight, strengthen its standing in the Parliament and increase the assurance which its existence gives the public.

**Other provisions**

5.69 Other matters relevant to the committee proposal included in the draft bill are: a requirement that heads of agencies brief the committee; provisions for the protection of witnesses; secrecy provisions; and a requirement for an annual report by the committee.
Chapter 6

The Minister, the Director-General and the Directive

Changes in the relationship between the Minister and the Director-General

6.1 ASIS was first established as part of the Defence Department, under a charter signed by the Prime Minister in May 1952. This first ASIS charter provided for the Service to receive higher direction on policy from a sub-committee of Cabinet, but such direction was to be transmitted to ASIS by the Secretary of the Department of Defence, to whom the Director of ASIS was made responsible for the general conduct of the activities of the Service. The Director was accountable to the Minister for Defence for the expenditures of the Service. Under this Charter, according to Mr Justice Hope in the report of his first Royal Commission into Intelligence and Security (RCIS):

an uneasy relationship had developed between the service and the Department of Defence. A considerable difference of opinion arose between the director and the secretary over the latter's responsibilities, particularly in regard to financial arrangements.

6.2 Under a revised charter signed by the Prime Minister in December 1954, the Service was removed from the Defence Department and made directly responsible to the Minister for External Affairs. The Director was given personal access to members of the Cabinet sub-committee, to heads of Commonwealth departments and to the Chiefs of Staff.

---

156 Exhibit 1.1
157 Exhibit 2.1.2.5, paragraph 83.
158 Exhibit 1.2, paragraphs 2, 12.
6.3 The higher status and greater autonomy conferred on ASIS by the 1954 charter was, however, short-lived. A new Directive was issued in August 1958, by the Minister for External Affairs. ASIS at that time was quite small. Its first Director, Mr Alfred Brookes, had resigned the year before, and the Government had seriously considered abolishing the Service.

6.4 The new Directive authorised the continuation of ASIS but under more detailed ministerial and public service control. It required the Minister to give approval before operations could be commenced in an overseas country, and it provided that the Minister, while not normally requiring to know details of operations, retained 'at all times the right to be given on request' such details.\textsuperscript{159} The first two charters, by contrast, had affirmed the 'well-established convention whereby Ministers do not concern themselves either with the sources providing secret information or with the detailed information which may be obtained by the Service in particular cases' and had provided that Ministers were to be given such information 'only as may be necessary for the determination of the issue'.\textsuperscript{160}

6.5 The 1958 Directive required the Director to report twice yearly to the Minister on the activities of ASIS. Access to the Minister for External Affairs was made subject to a requirement that the Secretaries to the Departments of External Affairs and Defence be consulted before matters affecting their respective departments were discussed. The Director's right of personal access to other members of Cabinet was removed. The Secretary, Department of External Affairs, was placed firmly in the line of control of ASIS. Like the Minister, the Secretary was given the right to obtain, on request, details of operations. The Secretary was to approve senior appointments in ASIS and the budget for the Service.

6.6 The Secretary's control over access by ASIS to the Minister was strengthened in May 1973 when the Prime Minister (also Foreign Affairs Minister at that time) decided that an officer of the Department of Foreign Affairs 'should always be present in any discussions you have, as Director MO9, (i.e. ASIS), with the Prime Minister'.\textsuperscript{161} In December 1973, the Director was further instructed that all his written communications to the Minister were to be sent by way of the Secretary, and 'in the rare cases in which it may be necessary for you to communicate with [the Minister] by telephone, the Secretary ... should,

\textsuperscript{159} Exhibit 1.3, paragraph 10.
\textsuperscript{160} Exhibit 1.1, paragraph 8; Exhibit 1.2, paragraph 8.
\textsuperscript{161} Exhibit 2.1.2.6, p.7.
without delay, be informed in writing by you of the subject and of the outcome'.

6.7 The Service had grown considerably by the mid-1970s. Reviewing the 1958 Directive, in RCIS, Mr Justice Hope concluded that it:

asserted 'ministerial control' by designing a set of instructions which, although ambiguous, withheld from the Director discretion in all matters except ASIS' internal management. The means of 'ministerial control' in fact turns out to be a process whereby the onus is placed upon ASIS to inform the department in any measure the department requires, about what it is doing, or thinking of doing ... This circumstance, combined with an attitude of mistrust on both sides, and exacerbated by the distance between Canberra and Melbourne - indeed between two different ways of life - generated an excess of conservatism and over-caution in ASIS management.

He described the Directive as containing 'a bizarre mixture of great and small constraints [which,] as a lawyer, I find it very hard to construe'.

6.8 As a result of RCIS, a revised Directive was issued in April 1978. The 1978 Directive removed or modified the controls criticised by Mr Justice Hope and made ASIS responsible directly to the Minister. It also altered the title of the head of ASIS to Director-General, reflecting an increase in the status of the position to public service agency head.

6.9 The 1978 Directive was further amended in 1985, after the Sheraton Hotel incident and the second Hope Royal Commission (RCASIA). The most significant changes were in removing from ASIS the responsibility for training for or carrying out any covert action, and in making explicit the obligation on the Service and its officers to comply with Australian law. Explicit provision was also made in the 1985 Directive for briefing the Leader of the Opposition. The new Directive embodying these amendments was approved by the Security Committee of Cabinet in December 1985 and remains in force.

---

162 Ibid.
163 Exhibit 2.1.1, paragraphs 337-8.
164 Ibid., paragraph 312.
165 Exhibit 1.7; Exhibit 1.8.
The role of the Minister and the Department

Direct ministerial control

6.10 The successive changes in the charters and directives governing ASIS have reflected the evolving views of government on the proper relationship between ministers and the Service. In its submissions to this Commission, ASIS emphasised the importance of the direct line of accountability to the Minister and the direct ministerial control which it achieved in 1978. The Service strongly opposed any suggestion that it should revert to a situation in which an official should hold responsibility between ASIS and the Minister.

6.11 It is now firmly established that ASIS is directly accountable to the Minister. The Minister in turn is accountable to the Parliament and the Government for the performance of ASIS. Both elements of accountability – Director-General to Minister and Minister to Parliament and Government – require that there be a clear understanding of what types of things the Minister should know and be called on to approve, and what types of things are the responsibility of the Director-General, for which he or she must account to the Minister. It has been one of the functions of the Directive to provide the formal element of this understanding, and we set out later in this Chapter our views on what the Directive should contain.

6.12 As we have said earlier (Chapter 2), the relationship between the Director-General and the Minister is central to the control and accountability arrangements. This will continue to be true whatever modifications are made to those arrangements. The optimal relationship is achieved when the two work constructively and harmoniously together, in an atmosphere of trust. All the evidence indicates that the present relationship is of this character. At the same time, there is a need for a formal set of rules, to allow for the possibility that the informal relationship between them breaks down and a resort to formal powers of direction becomes necessary. The Directive serves this purpose, by identifying those matters about which the Minister must be informed and by conferring on the Minister the power to require information, and to insist on the attendance of the Secretary of DFAT, where circumstances dictate.

6.13 In our view, the balance between formal and informal control, between Ministerial oversight and appropriate administrative autonomy for the Director-General, is being appropriately struck. The Minister for Foreign Affairs is kept informed of all matters requiring his approval under the Directive. The extent to

166 See for example, Exhibit 45.2.8, section 6.2.
which he is informed of other matters is left to the discretion of the Director-General who either makes a decision himself to inform the Minister of an operation, new form of activity or some other related development, or consults the Minister’s adviser and seeks his advice on whether it is desirable to inform the Minister formally about a particular subject. The audit conducted by Commission staff gave no suggestion that the Minister was not being appropriately involved.

6.14 Where ASIS undertakes an operation in response to a task which involves an unusual sensitivity of any kind, whether by reason of the nature of the task, the potential for political damage, or the methodology required being likely to fall outside routine operational activity, it is the practice of ASIS to signal the relevant aspect of the matter to the Minister or at least raise it in the first instance with his political adviser or other senior member of his staff. If the unusual aspect of the matter relates to foreign policy, the matter will also be discussed in the first instance with senior DFAT officers. Such communication with the Minister or his staff occurs before any implementation of the activity in question, and ASIS thereafter acts as directed by the Minister.

Annual report and corporate plan

6.15 Reporting by the Service is a central element in its accountability to the Minister. It is also essential to enable the Minister to exercise the necessary control over the Service, and to meet his accountability obligations to the Parliament and within the Government. The annual report of the Service is prepared on a program basis and gives the Minister an overview of what ASIS has done to achieve the objectives set for it. In accepting the report, and presenting it to SCOC, the Minister takes responsibility for ASIS’s activities as reported. The content of the annual report is discussed further in Chapter 7 in relation to control by SCOC.

6.16 Although prepared for different purposes, the corporate plan should also serve as a basis for reporting to the Minister which supplements the annual report. The Service should account to the Minister at least annually for its performance in achieving the objectives specified in the corporate plan, objectives which extend well beyond the program priorities with which the annual report is concerned. Reporting of this kind will further enhance the control/accountability relationship between Service and Minister.

167 Exhibit 20.1.10, p.8
168 Exhibit 20.3, paragraphs 5-6.
The role of the Department

6.17 Although the Department of Foreign Affairs and Trade (DFAT) no longer has any control over ASIS, the relationship between the two organisations remains of vital importance to ASIS.

6.18 DFAT also contributes to the control of ASIS in a significant way. It can influence operational decisions through the advice it gives ASIS, and where necessary the Minister, on the likely intelligence dividend from a proposed operation and on the foreign relations risks.

6.19 The existing arrangements for the performance by DFAT of its advisory role appear to be working satisfactorily. ASIS seeks advice from DFAT informally as the need arises, both at officer level and through Australian intelligence community consultative committees on which both organisations are represented. Where a proposal is submitted to the Minister, it will ordinarily have passed through the international security division of DFAT and any departmental comment will be recorded in the submission. The view of ASIS and of DFAT is that these procedures generally work smoothly and effectively, and there is no evidence to the contrary.

6.20 In the report of his second Royal Commission, Mr Justice Hope expressed the view that ASIS would benefit from the secondment of a senior DFAT officer, to serve in a line job. He rejected a proposal that the seconded officer should serve as a foreign affairs adviser, considering it impractical, unnecessary and likely to reduce the amount of informal discussion between ASIS and DFAT.169

6.21 We are satisfied that no change to existing processes is called for. All the indications are that the advice of DFAT is sought appropriately. The co-location of ASIS and DFAT encourages regular informal contact. This interaction, and the now considerable operational experience of the Service abroad, ensure that ASIS is well aware of the foreign policy implications of its operations.

The Directive in the control of ASIS

6.22 Until now, the Directive has been the backbone of the control and accountability framework for ASIS. It has defined, and governed, the key relationships which make up that framework. It prescribes the functions of ASIS,

169 Exhibit 2.2.2.6, paragraphs 7.25-7.
the roles and responsibilities of the Minister and the Director-General, the relationships between ASIS and other agencies, the main aspects of the administration of the Service, and the appointment and terms and conditions of the Director-General and members of ASIS. It is the source of legal authority for everything ASIS does.

6.23 In Chapter 3, we have concluded that it is no longer appropriate that the sole authority for the existence and activities of ASIS should reside in a Directive of the executive government. We have accordingly recommended that the Service be given a legislative foundation. Although much of what is in the present Directive could, and in our view should, be dealt with in legislation, acceptance of this recommendation will not altogether remove the need for a Directive. We see a continuing function for a Directive to deal with those matters which should remain secret, which are too detailed for legislation or which are likely to require frequent amendment.
Security Committee of Cabinet

7.1 The predecessor of the Security Committee of Cabinet (SCOC) was established in 1977, to overcome what the first Hope Royal Commission of 1977 considered was the poor co-ordination and control of the various intelligence agencies. Known as the National and International Security Committee, its brief was to provide general policy oversight for the intelligence community and to approve intelligence targets and priorities and agency budgets. The Committee today comprises the Prime Minister, the Ministers for Foreign Affairs, Defence and Finance, the Treasurer and the Attorney-General, with the Minister for Trade an alternate member for the Foreign Minister. The Office of Security and Intelligence Co-ordination (OSIC) in the Department of the Prime Minister and Cabinet acts as the secretariat for the Committee.

7.2 SCOC functions much as Mr Justice Hope envisaged. Its roles include:

(a) setting of broad intelligence priorities;
(b) consideration of the budgets of the intelligence agencies;
(c) approval of significant changes in the intelligence effort; and
(d) approval of broad guidelines for the operation of intelligence agencies.

7.3 SCOC usually meets between three and six times a year, depending on the number of issues requiring consideration. For the most part, material for the Committee is channelled through a supporting body at head of agency level, the
Secretaries Committee on Intelligence and Security (SCIS). SCOC’s most important recurrent activities are:

- consideration of an annual report from SCIS on the activities of the intelligence and security agencies, based on the annual reports of the agencies. (The individual annual reports are available for consideration by the Ministers at the same time);

- consideration of Part Two of the ONA Annual Report, containing an assessment of the performance of each agency;

- consideration of a Department of Finance report on the budgets and forward estimates of the agencies, including any new policy proposals, as part of the budget process;

- endorsement of the National Foreign Intelligence Assessment Priorities, usually every two to three years; and

- every three years, from 1994, endorsement of a Foreign Intelligence Planning Document prescribing longer-term strategic directions.

7.4 The depth and quality of SCOC’s oversight is dependent first on the time and interest of the Ministers and, secondly, on the quality of the information provided by the agencies, relevantly Finance, ONA and ASIS. We agree with the view expressed by Mr Justice Hope in his 1984 report (RCASIA) that SCOC cannot be expected to exercise close oversight of the intelligence community on a continuing basis. That is the responsibility of the individual Ministers. The Secretary PM&C, Dr Keating, confirmed that:

Security Committee Ministers are necessarily limited in the time and effort they can devote to overseeing agencies other than those for which they are responsible ... Finding the right balance of ministerial oversight is ultimately a matter for ministers themselves and will vary with different groups of ministers.172

According to Dr Keating, the Prime Minister takes an active interest in SCOC, and has not delegated his position as Chair to any other Minister. He is briefed on the performance of all intelligence agencies when the agency annual reports are considered by SCOC.173

172 Ibid., paragraph 21.
173 Ibid., paragraph 15.
7.5 The Minister for Foreign Affairs said that the Security Committee had not had occasion to play any 'really major role' in relation to ASIS during his tenure. He regarded it as a working body of well-informed colleagues on which he would be able to rely for advice in a crisis. 174 The main consideration of ASIS occurs during SCOC discussion of the annual SCIS Report on the intelligence agencies. According to the Minister, questioning and discussion varies from cursory to rigorous; it was quite sustained and penetrating in the context of SCOC's consideration of the Hollway Review. 175

Secretary Committee on Intelligence and Security

7.6 Like SCOC, the Secretaries Committee on Intelligence and Security (SCIS) was established in 1977 on the recommendation of RCIS, flowing from its assessment of deficiencies in the machinery for co-ordination and control of the intelligence community. 176 SCIS assists SCOC in its oversight of the intelligence community. Its functions are to provide policy guidance on behalf of SCOC to the principal departments and agencies involved in intelligence, to ensure that SCOC is kept regularly and fully informed of all relevant matters, and to coordinate the handling of issues requiring Ministerial consideration and the presentation of advice to SCOC. 177

7.7 The terms of reference for SCIS, revised in 1985 and endorsed by the Security Committee, include requirements that it:

- institute a regular cycle for examination of, and reporting to the Security Committee on, annual reports, forward estimates and budget estimates relating to the intelligence and security agencies;
- report regularly to the Security Committee on all relevant intelligence and security matters as required by the Prime Minister or the Security Committee, or otherwise as agreed necessary by SCIS;

---

174 Exhibit 39.1, answer to question 17. This accords with Mr Justice Hope's 1984 view that the committee should provide a forum to which a Minister could take particular issues (Exhibit 2.2.1.2, paragraph 3.7).
175 Ibid. The Hollway Review is discussed below.
176 Exhibit 2.1.3, paragraphs 245-46, 297-302.
177 Exhibit 25.2, paragraph 22.
subject to control and oversight by the Security Committee, provide guidance to the intelligence and security authorities constituting the total national intelligence and security effort, external and internal, including on questions of access to information and distribution of reports that may arise; and

subject to control and oversight by the Security Committee in respect of targets and priorities:

- recommend the national assessment priorities and provide guidance, as necessary, in respect of the national intelligence collection requirements; and

- consider any requests from Departmental Secretaries or heads of statutory authorities or intelligence agencies to have a priority determined. 178

7.8 Although it has no direct authority over any individual agency, SCIS plays a critical part in the control and accountability framework. Its monitoring of the performance of the agencies, principally through its scrutiny of annual reports and budgets, is the essential underpinning of the control which SCOC exerts over priorities and budgets, and of the accountability of the agencies to SCOC. SCIS performs both a screening function, ensuring that proposals going forward to SCOC are balanced by proper analysis and co-ordination, and a signalling function, to ensure that matters of significance are brought to the attention of SCOC.

7.9 SCIS does not intervene in the detailed management of agencies. Dr Keating told the Commission:

Like Security Committee, SCIS is not normally aware of the full details of ASIS's activities. Nor does it seek to be. Its emphasis is on broad policy oversight. It is up to ASIS and other departments and agencies to bring to the attention of SCIS and Security Committee significant issues which it should be aware of. 179

Thus, any significant ASIS proposal would be discussed at SCIS. 180 Conversely, SCIS might draw attention to resource allocation issues within a particular agency, or review an agency's response to requirements placed on it arising from a major event — such as the Gulf War — but it would be up to the responsible Minister and his department to 'draw an inference' and take the action they saw

178 Exhibit 4.6.11.
179 Exhibit 25.2, paragraph 25. See also Mr Costello, T639.
180 T408.
as appropriate. But, while SCIS will deal with issues concerning individual agencies which arise in discussions about annual reports or budget constraints, it will not delve into day-to-day activities.

7.10 In our view, this is as it should be. We have already emphasised (Chapter 6) the importance of maintaining the primacy of the relationship between Minister and Director-General in the management and control of ASIS. There would be no advantage, and some clear disadvantages, in SCIS intruding into management or operational issues.

7.11 One issue which highlighted the limits of SCIS's role was the 'campaign' against ASIS by the disaffected former officers. As we have outlined in Chapter 12, ASIS informed SCIS (via its annual report) of its concern about the threat to security which the actual and threatened media disclosures represented. SCIS in turn reported to SCOC that the potential security threat was a matter of concern. But SCIS was content to leave it to ASIS to determine – and pursue – the necessary action to deal with the threat.

7.12 We agree with the view expressed by SCIS members that the principal responsibility for dealing with this issue lay with ASIS, in consultation with the Minister. But where, as here, there is a threat of significant damage to the national interest, there is in our view an appropriate role for SCIS – and in particular its Chair, as the Prime Minister's representative – to ensure that everything possible is being done within the executive to support the agency and its Minister in determining the best course of action. Earlier experience of other agencies may be relevant and helpful and OSIC, as well as the Attorney-General's Department, should be encouraged to keep a collation of such experience in an accessible form.

7.13 From time to time, the policy co-ordination role of SCIS extends to substantive policy review and development. The 1992 Richardson report (see below) is a good example of this. The Report's assessment of the implications of the post-Cold War international environment for Australia's intelligence requirements enabled SCOC to reach a judgment about appropriate changes in priorities and direction for the various agencies.

7.14 It is, in our view, both appropriate and desirable for SCIS to undertake this policy development role where issues arise affecting the intelligence

---

181 T307-8.
182 T796.
183 Exhibit 12.3.4, answer to question 3; T2545; T2547.
community as a whole.\textsuperscript{184} The cross-section of viewpoints represented means that it is uniquely equipped for this task.\textsuperscript{185}

7.15 SCIS is a forum where inter-agency issues are aired, and agencies have the opportunity to learn from the experience and approach of others. Typically SCIS reaches a collective view about what should be presented to SCOC, but there are occasions when different views are maintained and presented to SCOC. For example, the SCIS advice to SCOC on new resourcing to meet the shortfall in intelligence collection identified in the Hollway Report contained divergent views on the balance of responsibility between ASIS and DFAT.\textsuperscript{186} Clearly there is a balance to be struck between the natural pursuit of individual interest and the requirements of the collective interest, and we agree with Mr Sedgwick that the value of SCIS is likely to be greatest when the objectives of the intelligence community as a whole are paramount in its deliberations.\textsuperscript{187}

\textbf{Control and oversight}

7.16 There is a variety of mechanisms through which SCOC, with the assistance of SCIS, exercises control over ASIS. Some of these operate on a regular basis, such as the annual reviews of performance and the periodic setting of foreign intelligence priorities. Other processes are activated only intermittently. They include reviews of ASIS’s performance in meeting particular collection priorities, and in-depth reassessments of the direction and resourcing of the AIC, and of the role of ASIS within the community.

\textbf{Annual reports and budgets}

7.17 Consideration of annual reports and budgets is probably the most important element of SCOC oversight of ASIS.\textsuperscript{188} This process enables the Committee to assess the performance of ASIS (and the other agencies) against the priorities which the Committee itself sets (see next section), and to recommend changes if necessary. The effectiveness of this oversight naturally depends upon the quality of reporting which SCOC receives from and about ASIS. The key components of this reporting are the annual report of ASIS, part 2 of the ONA annual report and the Finance Report (on the budget and forward estimates of the agencies).

\textsuperscript{184} T305; T330; T639; T795.
\textsuperscript{185} T1214.
\textsuperscript{186} Exhibit 4.6.5, paragraph 12.
\textsuperscript{187} T1214.
7.18 The evidence indicates that the quality of this reporting has been steadily improving, under the close scrutiny of SCIS. Following criticism in previous years, ASIS has moved to a program-based annual report. The reporting of performance against strategic priorities in its 1993-1994 report prompted special commendation from SCIS and from ONA for its 'outcome-oriented approach to evaluation'. Part 2 of the ONA annual report has also been upgraded, following criticism in the Richardson Review that it needed to provide a 'sharper and more helpful overview of ... performance'.

Intelligence priorities

7.19 One of the principal ways in which SCOC gives policy direction to ASIS is through its endorsement of the National Foreign Intelligence Assessment Priorities (NFIAPs). The NFIAPs set national intelligence priorities for agencies involved in foreign intelligence for a period of about two years. They represent the Government’s guidance – both by topic and by country – about what intelligence it requires. The NFIAPs are drafted by ONA, considered and endorsed by the National Intelligence Committee and submitted through SCIS to the Security Committee. The areas where ASIS collection effort should be directed are determined separately, by the National Intelligence Collection Requirements Committee (NICRC) and other tasking mechanisms described in the following chapter, within the assessment framework defined by the NFIAPs.

7.20 The Foreign Intelligence Planning Document (FIPD), endorsed by SCOC in November 1994, will further enhance the policy framework within which ASIS tasking occurs. The development of the FIPD followed the finding of the Richardson Report (see below) that the NFIAPs ‘work well for the purposes for which [they are] intended’, but that they are ‘not an adequate vehicle for setting strategic directions’. The Report therefore recommended, and the Government accepted, that long-range planning needs should be addressed in the development of a FIPD.

7.21 ONA has principal responsibility for the co-ordination and preparation of FIPD. The first FIPD was submitted to SCOC by SCIS and endorsed by SCOC in November 1994. It provides a long-term, strategically-oriented view of

---

188 Exhibit 25.2, paragraph 19.
189 Exhibit 4.1.7, pp. 7-22.
190 Exhibit 4.4.5, paragraph 2(e); T*1086*.
191 Exhibit 4.4.4, Chapter 2, paragraph 52.
192 Exhibit 2.3.1, paragraph 144.
193 Ibid., paragraph 139.
Australia’s foreign intelligence needs, integrating judgments about changes in the international environment with resource planning and programs. The document aims to look ahead over a five-to-seven year period and is to be reviewed on a rolling basis, every three years. The FIPD will provide a broad framework within which future NFIAPs will be developed.

**The Richardson and Hollway reviews**

7.22 In January 1992, following a consideration of agency annual reports for 1990-91, Security Committee commissioned SCIS to review the roles and priorities of the agencies in the light of the significant changes in international circumstances, notably the end of the Cold War. The report of the SCIS review, known as the Richardson Report\(^{194}\) contained a detailed assessment of the structure of the AIC, the arrangements for its management and co-ordination, the priorities for intelligence collection in the post-Cold War period and the respective contributions which the collection agencies could be expected to make. The report concluded, amongst other things, that ASIS’s role was of continuing relevance in the changed international circumstances\(^{195}\). The recommendations in the report were (with exceptions not relevant to our purposes) endorsed by the Security Committee\(^{196}\) and the results of the review were announced in a Prime Ministerial statement to the Parliament on 21 July 1992\(^{197}\).

7.23 The Richardson Report identified certain shortfalls in the foreign intelligence collection effort against priority requirements. The Security Committee commissioned a further report on available options, and their resource implications, for addressing these shortfalls. This report, known as the Hollway Report\(^{198}\) laid particular emphasis on the increasing importance of ASIS’s role as a collector.

**Conclusion**

7.24 In our view, the arrangements for control and oversight of ASIS by SCOC are satisfactory. We are inclined to agree with Dr Keating that it is difficult to see how SCOC’s oversight could, in a practical sense, be any more

---

\(^{194}\) Exhibit 2.3.1. Its principal author was Mr Dennis Richardson of the Department of the Prime Minister and Cabinet.

\(^{195}\) Ibid., paragraph 110.

\(^{196}\) Exhibit 4.6.3

\(^{197}\) Exhibit 1.9

\(^{198}\) Exhibit 2.4. Also known as the Hollway-Kean Report, its authors being Mr DA Hollway, Deputy Secretary, Department of the Prime Minister and Cabinet, and Dr D Kean, Deputy Director-General, Office of National Assessments.
rigorous than it is. The annual reporting process, combining ASIS's self-evaluation with the critical scrutiny of SCIS, ONA and Finance, seems to us to provide a sound basis for the performance by SCOC of its general oversight role. The other mechanisms we have described provide for appropriate policy direction and performance assessment, and we see no reason to recommend any change in the present arrangements, noting however that they depend heavily on the continued effective functioning of SCIS.

**Should ASIS be part of SCIS?**

7.25 The Director-General of ASIS is not a member of SCIS, nor an observer as of right. When matters are under consideration that have a direct bearing on ASIS, the Director-General is invited to attend and participate in the discussion. The present membership of SCIS comprises the Secretary, Department of the Prime Minister and Cabinet (Chair), the Secretary, Department of Defence, the Chief of the Defence Force, the Secretary, Department of Foreign Affairs and Trade, the Secretary, Attorney-General's Department, the Secretary, Department of Finance, the Director-General, ONA and the Director-General of Security.

7.26 The first Hope Report (RCIS) recommended full membership of SCIS for the Head of ASIS, expressing the view that:

> the heads of the Intelligence Agencies should attend the committee as full members. They not only have an interest in what is dealt with but they have important advice to offer as well.\(^{200}\)

The recommendation was not accepted.

7.27 In his second report (RCASIA), Mr Justice Hope recommended that full membership of the Committee be confined to department heads, with agency heads other than the Director-General of ONA, who would be a full member, being observers:

> The Director-General of ASIO, and the Director-General of ASIS, should be entitled to attend meetings of SCIS, but in the formal capacity of observers. They would be able to speak on issues in which they had an interest but would not be full members.\(^{201}\)

This, too, was rejected by Government.

---

199 Exhibit 25.2, paragraph 18.  
200 Exhibit 2.1.3, paragraph 300.  
201 Exhibit 2.2.1.2, paragraph 3.15.
7.28 The arguments advanced against full membership of SCIS for the Director-General of ASIS appear to be the following:

(a) the Committee should be reviewing the budgets and performance of the operating agencies and providing general guidance to them and it is therefore inappropriate for the heads of agencies to be full participants;

(b) the role of SCIS is essentially one of policy co-ordination and advice, and it is therefore inappropriate for an agency which has only a collecting role to be represented, since it would have only a limited contribution to make to the major part of the Committee's work;

(c) at least until recently the position of Director-General of ASIS has been below Secretary level. In any case, it is not a statutory position;

(d) ASIS is co-opted frequently and as a matter of course when matters in which it has a direct interest are to be discussed. Its participation is as full as it needs to be and the arrangement is as efficient as could be devised.

7.29 We accept that there is force in some of these arguments. The first argument, however, would also disqualify the Director-General of Security and the Chief of the Defence Force Staff (CDFS). The second argument is valid in that current members all have responsibility for policy advice, while ASIS has only a policy implementation or collection role. The third is not persuasive, and even less so if the Government accepts our recommendation that ASIS be put on a statutory basis. The fourth argument has some weight, but it implies that the Director-General's legitimate interest in matters concerning the intelligence community begins and ends with ASIS.

7.30 The most significant argument favouring the status quo is that ASIS is purely a collector of intelligence, its tasks defined by an agenda set by others. Full membership of SCIS might suggest that ASIS is somehow a party to the setting of that agenda. It should not, of course, be overlooked that the assessment priorities are set by SCOC, on which the Minister sits, and the collection requirements by NICRC, in which ASIS already participates. We also accept that ASIS's contribution to broader policy co-ordination and development may be more limited than that of agencies which have a more direct policy role, such as ONA.
Against that, we believe there would be considerable value in the Director-General of ASIS being able to participate in broader discussions on the intelligence and security matters which come before SCIS. The Director-General's perspective will often be of assistance to SCIS in these broader discussions. Moreover, exposure to the full range of issues coming before SCIS, and the opportunity to observe the responses of other agencies and departments to particular issues, could only enhance the Director-General's understanding and leadership of ASIS in the particular tasks assigned to it. It would also symbolise ASIS's full membership of the intelligence community and remove any perceived disparity between ASIO and ASIS. This in turn should contribute to improved morale in ASIS and improve the self-assurance of the Service as a participant in Government.

There is an important distinction to be drawn between ASIS and the two intelligence and security agencies in the Defence portfolio, DSD and DIO, neither of which has membership of SCIS. Those agencies report through CDFS and the Secretary of the Department of Defence, each of whom is a member of SCIS. The Director-General of ASIS, on the other hand, does not report through the Secretary of the Department of Foreign Affairs and Trade but directly to the Minister. Whereas CDFS and the Secretary of Defence can adequately represent the interests of DSD and DIO at SCIS, it is not possible for the Director-General of ASIS to be adequately represented on SCIS by the Secretary of DFAT. Nor are we persuaded that the policy input of the Director-General of ONA on foreign intelligence can in any real sense amount to a representation of ASIS at SCIS.

In our view, the benefits of a full relationship between ASIS and SCIS outweigh the arguments against any change and, like Mr Justice Hope in his first report, we recommend that the Director-General of ASIS be added to SCIS as a full member.

National Intelligence Committee

The focus of the National Intelligence Committee (NIC) is on the assessment function, and the work of ONA in particular. It provides an opportunity for policy departments to respond to ONA's assessments to comment on its work program and to identify areas of particular interest. It is chaired by ONA and includes senior representatives from PM&C, DFAT, Defence, Treasury, the Department of Primary Industries and Energy, the Department of Industry, Science and Technology, representatives from ADF, DIO and AFP, and observers from ASIS, ASIO and DSD. The monthly meetings of the Committee discuss ONA's monthly schedule of reports, and now include
reports on the preceding NICRC meeting and on recent developments of significance for intelligence. NIC also has formal responsibility for the development of the NFIAPs.

7.35 NIC was criticised by SCIS, in the Richardson Review, as having become 'somewhat wooden, with little free flowing discussion and bite'. ONA regards this description as still accurate:

probably because most of the committee members are not personally in a position to discuss the substance of ONA's assessments. Where members are able to do so, they may be constrained by the knowledge that others are not. The representation on NIC by a range of policy departments also limits the scope for discussion of issues before the intelligence community. More effective fora for such discussion are SCIS, HIAM or NICRC.

In part 2 of its 1993 Annual Report, ONA confirmed that enlivening NIC had not proved an easy task.

7.36 Despite these reservations, it seems clear that NIC has a distinct and important role to play in ensuring that the output of ONA is meeting the needs of policy departments. So far as ASIS is concerned, NIC is of less direct relevance than NICRC, but ASIS's observer status means that the Service stays informed about areas of major interest to policy departments. This helps to inform the processes of setting collection requirements and tasking. We see no reason to recommend any change to the present arrangements.

Heads of Intelligence Agencies Meeting

7.37 The Heads of Intelligence Agencies Meeting (HIAM) comprises DG-ONA, DG-Security, DG-ASIS, the Directors of DIO and DSD and the relevant Deputy Secretary from DFAT. HIAM is an informal meeting, chaired by agency heads in turn, which meets approximately monthly. ONA regards HIAM as a very valuable forum for building co-operation and avoiding misunderstandings among the intelligence agency heads and DFAT. As a gathering of high-level representatives of both collectors and assessors, HIAM can assist understanding and facilitate action on tasking approved through other mechanisms. Both Mr Miller and Mr Stevenson observed that the meeting acts as a forum for informal

---

202 Exhibit 2.3.1, paragraph 147.
203 Exhibit 28.1, p.6.
204 Exhibit 4.3.6.1, p.61.
205 T369.
206 Exhibit 28.1, p.9.
exchange of ideas before action is pursued at a higher level, such as SCIS or the Minister.  

The presentation of the new Defence Intelligence Assessment Priorities at HIAM was cited as an example of the way the meeting facilitates the communication of information to ASIS.  

7.38 We see benefit in the informal interchange which HIAM allows, provided that its proceedings do not conflict with the formal processes within the framework. Its importance for ASIS would presumably diminish somewhat if, as we have recommended, the Director-General became a full member of SCIS.

---

207 T268, T330.
208 T3046.
Chapter 8
Tasking

Introduction

8.1 Central to the control of ASIS are the procedures by which its collection tasks are defined. Effective external tasking mechanisms are necessary to ensure that ASIS does not itself determine what secret intelligence it collects but acts only in response to government priorities. The effectiveness of the tasking procedures appears to have improved progressively since the first Hope Royal Commission, with the result that tasks are defined more clearly, and guidance as to customer requirements is more specific.

The Hope Royal Commissions

8.2 The first Hope Report emphasised that effective tasking depends on clear specification of customer requirements and on critical assessment by customers of the value of ASIS product. When attempting to assess the value of ASIS output to customers, Mr Justice Hope found it difficult to make a judgment because consumers' assessments had been 'subjective and necessarily generalized'. The Report argued that there 'should be a continuing consumer's review of ASIS intelligence production ... to encourage improvement in quality and to help ASIS in source development and tasking'. The Report therefore recommended the establishment of machinery to facilitate day-to-day criticism and evaluation of the service's reports and continuous review and update of consumer requirements. It also called for greater consultation between ASIS and consumer departments at the desk level.

209 Exhibit 2.1.1, paragraph 108.
210 Ibid., paragraph 109.
211 Ibid., paragraphs 109-10, 631-32.
212 Ibid., paragraph 110.
8.3 The second Hope Royal Commission of 1984 re-emphasised the crucial importance of clear tasking in enabling a secret intelligence service to meet the need of its clients effectively. Mr Justice Hope remained critical of the prevailing situation:

Priorities have been set pragmatically, which has sometimes meant erratically and on a segmented basis. Requirements have been passed on in an unco-ordinated, ad hoc manner.\(^{213}\)

The second Hope Report was more explicit than the first in placing responsibility for the deficiencies on ASIS customers rather than on ASIS itself. The Commission found that, without guidance from customers, the job of selecting priorities had been passed by default on to ASIS representatives abroad.\(^{214}\)

8.4 The Report strongly endorsed the then newly-established National Intelligence Collection Requirements Committee (NICRC) as a way of bringing collectors and assessors together to develop priorities for intelligence requirements.\(^{215}\) It was careful to state, however, that NICRC was not a panacea and that tasking should remain continuous, with ad hoc requests flowing out of informal meetings between ASIS and its customers.\(^{216}\) The Report also recommended the establishment of the National Intelligence Committee (NIC) as a forum for evaluating product and for guidance on targets and sources.\(^{217}\)

8.5 These recommendations were accepted by the Government. By 1992 NICRC was well established as the principal body setting the collection requirements for the intelligence community within the framework of the National Foreign Intelligence Assessment Priorities (NFIAPs), discussed in the previous chapter.

The Richardson and Hollway reviews

8.6 The Richardson Report of May 1992, reviewing nearly a decade of NICRC operation, affirmed the value of the Committee's contribution and recommended that it be assigned two new roles. It proposed that NICRC be given the authority to set mandatory requirements for intelligence collection and that collectors should be required to show the effort they had made in meeting them. In addition, the Report recommended that ASIS and the Defence Signals

\(^{213}\) Exhibit 2.2.2.3, paragraph 3.53.
\(^{214}\) Ibid., paragraph 3.54.
\(^{215}\) Ibid., paragraph 3.56. See also Exhibit 2.5, paragraph 86.
\(^{216}\) Ibid., paragraph 3.58.
\(^{217}\) Ibid., paragraph 3.57.
Directorate (DSD) should report monthly to NICRC on the tasking they had received from customer agencies, so as to eliminate potentially overlapping or conflicting priorities.\textsuperscript{218} The Report also recommended that the Office of National Assessments (ONA) upgrade Part Two of its annual report to provide a sharper and more helpful overview of the intelligence community’s performance, which could better inform decisions about strategic directions.\textsuperscript{219}

8.7 The Hollway Report of November 1992 identified tasking as an issue of management and co-ordination. Although tasking procedures had improved, partly as a result of the Richardson review, there was still a lack of sufficiently clear and precise guidance from customers to the collection agencies.\textsuperscript{220} Hollway called for ‘collegial, well-informed dialogue’ between collectors and customers, to ensure that customers knew what was reasonable – and unreasonable – to expect from collectors. Dialogue could be facilitated if customers were educated about the range of collection capabilities available to them and understood the operational challenges which collectors faced.\textsuperscript{221} ONA should make itself known as a source of advice to departments needing help in registering collection requirements. The contribution of NICRC and NIC to co-ordination of tasking priorities could be enhanced, for example by NICRC ‘sorting out’ different views amongst collection and assessment agencies about the relative value of different forms of intelligence; and by closer co-operation between NICRC (representing collectors and assessors) and NIC (representing ONA and its customers) to make tasking more precise and to promote the giving of earlier notice of collection requirements to relevant agencies.\textsuperscript{222}

8.8 These recommendations of the Richardson and Hollway Reports were accepted by the Government and have become part of tasking procedures and practices. The existing arrangements by which ASIS is tasked are discussed in the following section.

**National Intelligence Collection Requirements Committee**

8.9 NICRC is the highest level body which sets overall collection requirements. The Committee is a meeting place for the main assessment and collection agencies. The Committee is chaired by ONA and includes the Defence

\textsuperscript{218} Exhibit 2.3, paragraphs 150-1.
\textsuperscript{219} Ibid., paragraph 144.
\textsuperscript{220} Exhibit 3.4.5.6.1, paragraph 233.
\textsuperscript{221} Ibid., paragraph 234.
\textsuperscript{222} Ibid., paragraph 238.
Intelligence Organisation (DIO), the Department of Foreign Affairs and Trade (DFAT), the Department of Defence, the Australian Defence Force, ASIS, ASIO and DSD – and the Australian Federal Police and Customs for transnational issues. Other agencies may be co-opted from time to time. NICRC meets monthly unless there is an event which requires an ad hoc meeting.

8.10 NICRC determines the broad priorities on which intelligence collectors, both overt and covert, are expected to focus their collection efforts. Priorities are set within the framework of government guidance provided by the NFIAPs. ONA, in consultation with relevant policy departments, uses the NFIAPs to prepare detailed collection requirements papers on individual countries and on major issues in world affairs. The papers list the most important collection requirements in priority order. They are considered during the monthly meetings of NICRC, where the collectors have the opportunity to ensure that the requirements are clear and appropriate. Meetings also discuss current key topics on which collectors should focus their attention in the coming month. NICRC assigns appropriate agencies to each collection requirement on the basis of ONA recommendations. Adjustments may be made after considering collectors' own appraisal of their capabilities.

8.11 ONA identified the main limitation of requirements papers as being that they do not always provide the best tasking format for the different agencies. While they are suitable for DSD tasking, the requirements papers are less useful for ASIS which 'prefers its tasking to be in the form of a set of questions to which it can pursue answers'. ONA does not, as a result, treat the requirements papers as definitive in all circumstances. It recognises the need for frequent interaction between analysts and collectors to ensure that collectors are responsive to shifting priorities.

8.12 As noted above, the authority of NICRC in setting and co-ordinating requirements for ASIS and other collection agencies has been enhanced in recent years. ONA's view is that NICRC is increasing in 'vitality and effect'. ONA considers that, after some initial hesitation, ASIS has responded well to the new arrangements. The Director-General of ASIS said that the evolution of NICRC was a very positive step forward in systematising the whole requirements

---

223 Exhibit 28.1, p.7.
224 Ibid.
226 Ibid, p.3.
227 T338-9.
process and that mandatory requirements had helped ensure that collectors were more accountable.228

8.13 Some important reservations were, however, expressed about the workings of NICRC. The Secretary of the Department of the Prime Minister and Cabinet, Dr Keating, told the Commission that the requirements laid down by NICRC were often very broad, and so did not always provide a sound basis for decisions on collection options.229 He considered that the accountability provided by the monthly report to NICRC on total tasking was deficient because NICRC requirements were broad enough to allow most tasking to be easily justified. This practice, in Dr Keating’s view, meant that considered judgments based on the whole range of collection options were not being made. Instead, the tendency was for judgments to be left solely to ASIS and individual customers.230

8.14 A senior ASIS Intelligence Officer suggested that effectiveness and accountability would be enhanced if more detailed requirements were determined by a lower-level sub-committee of NICRC which included representatives of collectors who understood the challenges and limitations of secret intelligence.231 A senior DIO officer confirmed that ASIS preferred a far more specific level of tasking than generally appears at NICRC, and that a good deal of DIO’s tasking of ASIS was at a more detailed level.232

8.15 We are satisfied that the collection requirements laid down by NICRC provide the necessary framework to guide ASIS in its strategic planning and general collection activities - and an appropriate framework within which the specific requirements of customers can be advised to ASIS. It is essential that this framework exist, and that the priority requirements be identified, so that ASIS is in a position to satisfy itself that a particular customer requirement is consistent with the overall collection and assessment priorities of the Government. Within that framework, the onus is on ASIS and on individual customers to ensure that specific tasking is clear and precise.

228 T266.
229 Exhibit 25.3, p.4.
230 Ibid.
231 T1063.
232 T3045.
Direct tasking of ASIS

8.16 In addition to the tasking of ASIS through the mechanisms of NICRC, ASIS is tasked directly by customers. Such tasking and associated consultation in support of tasking includes:

(a) written requirements to ASIS;

(b) day-to-day contact between ASIS Intelligence Branch (and other ASIS officers), and officers of customer agencies at a working level. Such discussions frequently give rise to requirements in writing;

(c) discussions at informal contact groups of analysts working on a particular country;

(d) Comment Sheets on previous ASIS reports which include further tasking in the form of follow-up questions; and

(e) requirements which can emerge from operations, e.g. where a source identifies a matter as being worthy of further inquiry.233

Improving customer liaison

8.17 A major part of successful tasking is matching customer requirements with the capabilities of the collection agencies. As the Hollway Report emphasised, this means that customers must be well informed about what the collectors can and cannot do. As the head of DIO acknowledged, this is essential if agencies such as his own are to task ASIS "in a reasonable sense". Knowing that ASIS has "certain people in certain places" enables analysts from assessment agencies to frame their requirements appropriately.234 ASIS collection capabilities can take a long time to establish, and it is important that analysts have an appreciation of the challenges which ASIS faces in the field. Major-General Hartley, Director of DIO, suggested that, in the past, customers may have tasked a number of agencies at the same time in the hope of getting something from at least one, but with limited knowledge of what was really possible.235 This not only duplicates effort, but often results in requirements being incompletely met, with frustrated analysts unable to get the information they really want. With a good understanding of the capabilities of individual

233 Exhibit 20.1.10, pp.4-5.
234 T3050.
235 T3051.
collectors, analysts can direct their requirements to the most appropriate collector.

8.18 If ASIS is to take seriously its characterisation of the agencies as 'customers', it must educate those customers in how to make the best use of its services. Ensuring that customers understand the possibilities and limitations of secret intelligence collection should be a primary ASIS responsibility.

8.19 Success in this educative task will depend on the quality of ASIS's liaison with customers. The liaison function of ASIS is, in the main, the responsibility of the Intelligence Branch of the Operations Division. The Intelligence Branch operates as a clearing house for reporting from Stations overseas, passing it on to customer agencies and receiving feedback from them. The Director of Customer Liaison and desk officers from Intelligence Branch maintain regular personal contact with analysts in the major customer agencies. ASIS liaison provides 'an essential facilitation channel in the tasking process ... with expert advice on ASIS capabilities and limitations and the likelihood of tasking levied on ASIS being satisfactorily achieved'.

**Tasking and customer feedback**

8.20 Customer comment on ASIS reporting is almost as important to the tasking process as precision and realism in the initial definition of a collection requirement. Comment from a customer about whether or not a report was useful can help to focus further tasking of the particular station and source. It also assists ASIS in its evaluation of its performance.

8.21 If the tasking improves, the customer ultimately benefits from the improved reporting. As a senior manager in the Intelligence Branch put it, ASIS customers have an interest in keeping the flow of intelligence alive by nourishing it with good questions and comments. DIO clearly appreciates the importance of good feedback:

> DIO's impression is that where an analyst goes to some trouble in providing comment, ASIS regards that as valuable and this often results in further reporting of relevance to the analyst. Analysts have become aware of this and the quality and rigour of comments and responses have improved accordingly.

---

236 Secretary, Department of Defence, exhibit 35.1, paragraph 6.1.3.
237 T3308.
238 Ibid., paragraph 6.1.4.
8.22 The principal means by which customers communicate their assessment of ASIS output is through comment sheets attached to most ASIS reports. Part A of the comment sheet asks recipients to evaluate a report on the basis of two criteria: the report's value to the analyst; and the credibility of the information it contains. This evaluation is a quantitative one which invites a score of A to D for value and 1 to 4 for credibility. Part B of the comment sheet provides space for supplementary comment and for follow-up questions. Where such comments are made, there are usually follow-up questions placing a further requirement on the Service. Officers take greater note of the comments and follow-up questions on the sheet than the numerical rating.239

8.23 ASIS could enhance the quality of the customer feedback it collects by impressing on policy departments the value which such feedback can add, and by sharpening the focus of its questions. This might involve both some redesign of the comment sheets and the greater cultivation of personal contacts by officers in the Intelligence Branch. The Commission endorses the view expressed in the Foreign Intelligence Planning Document:

ASIS is sometimes too influenced, or is badly influenced, by feedback from assessment agency analysts. They provide most of the comment that ASIS receives through comment sheets that it attaches to its reports. And the comment sheets constitute almost all the routine feedback received by the stations ... Stations should be made less dependent on the comment sheets. ASIS needs to do more to solicit and record comment from policy departments, who are best placed to comment on the 'actionability' of the information, on how it affected outcomes.240

8.24 While we see value in seeking to enhance customer comment on individual reports, we doubt that any system of customer comment can be sufficiently standardised to enable any useful aggregation of statistics. The principal difficulty is the uneven nature of customer response, which was well summarised by Dr Keating:

Customers are often unable or unwilling to provide adequate commentary on intelligence reporting. Lack of time often prevents senior policy makers from providing any commentary at all, let alone commentary that is useful ... Customers often will not have thought carefully about what the criteria should be for judging the value of a secret report ... Critical assessment requires careful thought by customers, and so is time consuming and leads to uneven responses from customers.241

---

239 T3306.
240 Exhibit 4.4.4, paragraph 345.
8.25 ASIS's efforts to improve the quality of its liaison and consultation with customers are to be commended, and should be maintained. One way to facilitate further improvement is through internal restructuring.

8.26 Overall, the Commission believes the processes by which ASIS is tasked are well developed and enhance the accountability and control of ASIS. The conclusions we have reached and the recommendations we make should be seen as refinements and as encouraging further progress in directions that are already being properly pursued.
Chapter 9

Oversight by the Inspector-General of Intelligence and Security

The role first envisaged for the Inspector-General

9.1 The office of Inspector-General of Intelligence and Security (IGIS) was established in February 1987, after the 1984 Hope Royal Commission (RCASIA). In his report on ASIO, Mr Justice Hope had recommended a body with powers to inquire into that organization's compliance with the law; the propriety of its actions in more general terms; and the appropriateness and effectiveness of its internal procedures. In his General Report, he further proposed that the Inspector-General should oversee intelligence agencies other than ASIO to the extent that their activities came within Australian law or could affect the rights of Australian citizens, commenting:

Since the rights or standing of Australian citizens would rarely be involved, this responsibility should not be onerous but it would be valuable in providing an assurance for the Minister and the public, as well as a protection for the services, if allegations of misconduct are made against them.

9.2 Mr Justice Hope emphasised that the role of the Inspector-General would be to assist ministers in meeting their accountability obligations, and not to assist in the management of the intelligence agencies. He wrote in respect of ASIO:

it would be a mistake to interpose an additional officer in such a way as to interfere with or blur the essential line of responsibility from the Director-General [of ASIO] to the Attorney-General and through him to the Parliament. The executive responsibility for decisions in relation to domestic security rests with the Attorney-General and, within statutory limits, the Director-General. ...

---

242 Exhibit 2.2.4, paragraph 16.91.
243 Exhibit 2.2.1.2, paragraph 3.21.
The creation of a new position with power to second guess or take over managerial or administrative decisions would confuse the issue of responsibility and could lead to 'buck-passing' among those concerned.244

9.3 In relation to ASIO, the Inspector-General was to be an independent person with power to maintain a close scrutiny of ASIO's performance of its functions, and to look into complaints, in order to give greater assurance to the Attorney-General, and through him Parliament and the public, that ASIO was acting with propriety and within its charter.245

In his report on ASIS, Mr Justice Hope similarly proposed:

The role of the Inspector-General is not designed to affect or intrude on the line of responsibility from the Director-General to the Minister. Rather it is designed to give the Minister the assistance of an independent watchdog who could, through his inquiries and reports, provide greater assurance to the Minister about the state of affairs in ASIS. In so doing, he would also provide the Minister with a firmer base on which to account to Parliament.246

9.4 Mr Justice Hope laid greater emphasis on the monitoring function of the new office than on the investigation of complaints. Although he saw a need for a means by which members of the public and employees of the intelligence and security agencies could raise complaints about the agencies, and thought it appropriate that the Inspector-General provide that facility, Mr Justice Hope did not propose that it be the main function of the office.247 The balance he sought is captured in his phrase 'an independent person with power to maintain a close scrutiny of ASIO's performance of its functions, and to look into complaints'.248

9.5 Mr Justice Hope recommended that the Inspector-General report to the relevant minister on inquiries. However, where the findings of an inquiry went to the propriety or some other aspect of a ministerial direction to ASIO, the Inspector-General should also provide a copy of the report to the Prime Minister. In addition, the Inspector-General should prepare an annual report, a copy of which should be given to the Leader of the Opposition and an edited version tabled in Parliament.249

244 Exhibit 2.2.4, paragraph 16.83.
245 Ibid., paragraph 16.84.
246 Exhibit 2.2.2.6.
247 Exhibit 2.2.4, paragraph 16.84.
248 Ibid., paragraph 16.84.
249 Exhibit 2.2.4, paragraphs 16.93-16.97.
9.6 The Hope proposal was thus intended to protect the rights of Australian citizens and residents against possible errors or excesses by the intelligence and security agencies and to guard against breaches of Australian law by the agencies. It was not a proposal for a check on the general effectiveness or appropriateness of the agencies' operations. The Inspector-General was not to second-guess or take over managerial or administrative responsibilities, nor to diminish the responsibility of agency heads to their ministers, or ministers to Parliament, for the execution of the agencies' work.

The jurisdiction and powers assigned to the Inspector-General

9.7 The importance which Mr Justice Hope attached to the proposed office of Inspector-General is indicated by the administrative arrangements he recommended. The proposed office should be attached to the Prime Minister's Department and have a statutory base. It should have access to files and other materials held by the agencies it was to oversee, and the power to require answers to questions from their officers, to the extent necessary to carry out its functions. The Inspector-General should be carefully selected, and would hold a personal rather than an institutional office (although a small staff would be needed) for a term of appointment of three to four years, renewable no more than once. Because of the need for wide acceptance of the office, the Government should consult with the Opposition on any proposed appointment to it.  

9.8 The Inspector-General of Intelligence and Security Act 1986 (the IGIS Act) which came into operation on 1 February 1987, closely followed the Hope proposals in these regards. The Act provides for the Inspector-General to oversee those activities of the five intelligence and security agencies (ASIO, ASIS, DSD, DIO and ONA) which have the potential to affect the rights of Australians or to breach Australian law. The extent of the oversight role varies for the different agencies according to the nature of their activities. At its furthest extent, in respect of ASIO, oversight by IGIS applies to:

(a) compliance with Australian law;

(b) compliance with directions or guidelines given by the responsible minister;

(c) the propriety of particular agency activities;

(d) the effectiveness and appropriateness of agency procedures relating to the legality or propriety of activities; and

(e) acts or practices of agencies referred to IGIS by the Human Rights and Equal Opportunity Commission (s.8(1)(a)).

9.9 Inquiries of these types into ASIO may be initiated by IGIS of his or her own motion, by the Minister, or in response to complaints. In addition, the Prime Minister may request inquiries under the headings (a) to (d) above (s.9). There are also two heads of inquiry specific to ASIO, concerned with the rights of Australians upon whom the Organization has reported, and with ministerial directions to ASIO (ss.8(1)(c), 8(1)(d)).

9.10 Since the operations of ASIS are mostly overseas and have very limited potential to affect Australians, ASIS is less open to inquiry by IGIS. A ministerial request is necessary before IGIS may inquire into matters which do not affect Australians, or which do not involve possible breaches of Australian law (s.8(4)). The same condition applies to inquiries into the effectiveness and appropriateness of ASIS's procedures relating to the legality or propriety of its activities (s.8(2)(c)). Ministerial approval is required for an inquiry into any matter concerning ASIS which occurred outside Australia or before the commencement of the Act in 1987 (s.8(8)).

9.11 IGIS's independent power to initiate inquiries into ASIS, in the discharge of the oversight function of the office, is therefore limited to matters affecting Australians or involving possible breaches of Australian law, and occurring in Australia since 1987. Wider inquiries may only be undertaken at the request or with the approval of the Government. As a result, such assurance as the oversight work of IGIS can provide to the public and the Parliament about ASIS does not flow from any power of systematic review of all the Service's activities.

How oversight by the Inspector-General has developed

9.12 The second Hope Royal Commission reported in December 1984 and Cabinet had decided by June 1985 to implement its recommendations on an Inspector-General. The IGIS Act was then drafted and administrative arrangements for the Office were made, in a process coordinated by the Department of the Prime Minister and Cabinet (PM&C) and the Secretaries Committee on Intelligence and Security (SCIS). The legislation was approved by the Security Committee of Cabinet (SCOC) on 30 April 1986 and passed by
Parliament later that year. A Deputy Secretary of PM&C who had been closely involved in the development of the arrangements, Mr Neil McInnes, was appointed as the first Inspector-General in February 1987, following consultation with the Leader of the Opposition.

9.13 Mr McInnes told the Commission that there had been concern within the Australian intelligence community (AIC) about the potential scope of IGIS’s activities and that this was manifest in SCIS’s deliberations on the proposal. The PM&C files support Mr McInnes’ recollection. They record opposition from the heads of intelligence agencies to various proposals which would have implied a wider-ranging role for the Inspector-General. The agencies of the Australian intelligence community also sought to keep open the option of a part-time IGIS, and to limit the staff appointed to support the Inspector-General to one or two research officers and a steno-secretary. A proposal for an assistant to IGIS at Senior Executive Service level was initially rejected, although that position was soon established. The views of the intelligence agencies did not lead to any significant reduction in the scope of activities recommended for IGIS and approved by SCOC. They did, however, signal to Mr McInnes a lack of enthusiasm within the Australian intelligence community for his new office.

9.14 During his three-year term, Mr McInnes found no occasion to test the agencies’ reactions to his office outside the context of inquiries into complaints and monitoring of activities that might affect Australians. In his evidence to this Commission, he summed up his view of the role of IGIS in the following terms:

The only ‘assistance’ Ministers expect from IGIS is to protect the Government by dealing with complaints from the public. And that role, his true role, is more accurately described as protecting the public from the invasion or oppression of rights by intelligence agencies.

9.15 Within that conception of IGIS’s role, Mr McInnes identified some areas in which IGIS ‘need not wait for individual complaints but should act to see that there is no occasion for them’. They were: checking ASIS’s and DSD’s reporting for Australian names; monitoring ASIO’s procurement and use of warrants for telephone interception and entry onto property. Mr McInnes began

---

251 PM&C File 86/075, Part 4, folios 78, 189, 200.
252 Ibid., Part 5, folio 21.
253 Ibid., T853.
254 Ibid., Part 1, folios 2, 66.
255 T854.
256 Exhibit 32.1.2, p.2.
257 Ibid.
regular monitoring of each of these processes, initiating the ASIO process with an own-motion inquiry.258

9.16 Mr McInnes also dealt with 34 complaints during his three-year term. All concerned ASIO, and 11, from a total of 23 persons, were grievances of current or former officers.259 Most of the public complaints were resolved by Mr McInnes’ conclusion after a preliminary inquiry that they had no basis and so advising the complainants. Three led to full inquiries and reports to the Minister. Contrary to expectations when the office was created, staff grievances represented a significant part of its workload from the beginning. Mr McInnes conducted a full inquiry into one of the grievances he received, and an inquiry of his own motion into ASIO’s procedures relating to the redress of staff grievances. As a result of the latter, he proposed various changes to procedures.260

9.17 At the end of his term of office, Mr McInnes suggested that, since the monitoring function had been established and experience had indicated that there would be few serious public complaints, the Government should consider a part-time appointment to replace him.261 However, his successor, Mr Roger Holdich, was appointed from the end of September 1989 on a full-time basis and reappointed in September 1992. On both occasions, the Leader of the Opposition was consulted first.262

9.18 The annual incidence of complaints approximately doubled during Mr Holdich’s first term and a high rate of complaints has continued. A significant proportion of the complaints has been staff grievances, especially from serving and former ASIO officers, but including also the grievances relating to ASIS which came before this Commission.263 Complaints work, including staff grievances, came to dominate IGIS’s work program and Mr Holdich told the Commission that, although he would like to undertake more monitoring work and inquiries of his own motion, the time and resources necessarily devoted to the resolution of complaints has precluded this.264 He estimated that complaints had come to occupy 75-80 per cent of his time in recent years, an increase from about 30 per cent when he was first appointed in 1989.265

258 T860.
259 Exhibit 23.8.1.
260 Ibid.
261 Exhibit 23.4.1.
262 Exhibit 23.4.18.
263 Exhibit 23.6; Exhibit 23.8.1.
264 Exhibit 23.3, paragraph 39; T141.
265 T140.
9.19 The average staffing of the office under Mr Holdich was about 30 per cent higher than it had been under Mr McInnes, and the number of complaints resolved per staff member per year doubled. But the office was still ‘well and truly swamped’ by complaints in the early 1990s, according to the 1992-93 annual report of IGIS.266

9.20 Neither Mr McInnes nor Mr Holdich received any requests from Ministers for inquiries to be undertaken. On each occasion when Mr Holdich has sought the approval of the Minister for Foreign Affairs, to inquire into complaints about ASIS concerning matters that had occurred overseas or before the commencement of the Act, the approval has been given. All these complaints related to employment matters and originated with officers, former officers, or their spouses.

9.21 The amount of time IGIS has devoted in recent years to his function in relation to inquiries into staff grievances has, in our view, distracted him from the general monitoring and oversight functions, and unduly reduced the attention which should have been given to these functions. We regard this as a matter of concern. It is partly for that reason, though principally for other substantive reasons, that we recommend in Chapter 14 that external review of grievances be removed from the jurisdiction of IGIS. One of the effects of that would be to allow IGIS to concentrate most of the energies of the office on the monitoring and oversight functions which we will be recommending be expanded in their coverage.

9.22 We deal in the rest of this chapter with the central role for IGIS envisaged by Mr Justice Hope, the monitoring or oversight role. We deal with IGIS’s role in the resolution of grievances and complaints in Chapter 14.

How the Inspector-General should oversee ASIS

9.23 The office of IGIS was established in a context which emphasised its role in providing assurance to ministers that the intelligence agencies were not encroaching on the rights of Australians or operating in breach of Australian law. Within that context, IGIS now regularly monitors six aspects of the activities of the agencies. Only one aspect of the monitoring is directly associated with ASIS; that concerning its adherence to the rules on retention and communication of information about Australians. Another regular IGIS check –

266 Exhibit 4.10.7, p.1.
that of ASIO's operations under warrant – includes operations undertaken in Australia at ASIS's request.

9.24 Other activities of ASIS which might be monitored are not currently the subject of any systematic external review, and IGIS would be excluded from review of most of them except at the request of the Minister. Neither of the occupants of the office has sought to widen the scope of its activities by, for example, inviting the Minister to request particular inquiries, or by expanding, where possible, the range of routine monitoring of ASIS undertaken under the own-motion power. As already indicated, this may have been the result, in part at least, of the demands placed on IGIS in recent years by the large volume of complaints received.

9.25 It has been accepted since the office was established that IGIS has a role in providing general public reassurance about the operations of the agencies. This was acknowledged by the Attorney-General when he summed up the role of the office in the second reading speech on the IGIS Bill:

We believe that the legislation establishes an office which will, to paraphrase the Royal Commissioner, provide an independent oversight of the agencies' activities, give the public a greater assurance that those activities are proper ones, and clear the agencies, or bring them to task, as the case may be, if allegations of improper conduct are made against them.

9.26 It was not disputed in the evidence that the public has a right to reassurance about the general propriety of the activities of the intelligence agencies. The interests of Australians are affected by activities which are undertaken on their behalf, and which they fund, even when their rights are not directly affected, or the activities do not breach Australian law. The Government is publicly accountable for those activities.

9.27 Nevertheless, it is clear from the Act governing IGIS that the extent of monitoring of ASIS and the nature of the assurance it was to provide, was to be directed not to the full range of ASIS activities but to the limited range which impact directly on Australian citizens or which may involve breaches of Australian law. These are the areas in which IGIS was given the power to initiate inquiries. Part of the reason for this may have been that the control and accountability of ASIS, unlike ASIO, was to be achieved through executive direction rather than legislation – and the associated reason that many of the

267 T183-91.
268 Exhibit 23.3, paragraph 39.
269 Exhibit 3.2.4, p.3706.
activities of ASIS, unlike those of ASIO, are undertaken overseas and have limited direct impact on Australian citizens. In practice therefore, and not surprisingly, routine monitoring of ASIS by IGIS has been directed principally at the issue of retention and use of information on Australians.270

9.28 In his final submission, Mr Holdich proposed some relaxation of the statutory limitations on his power to initiate inquiries. In particular, he argued that:

(a) s.8(4) should be amended to allow inquiry of the Inspector-General’s own motion into the propriety of ASIS activities within Australia which affect non-citizens and non-residents; and

(b) s.8(2)(c) should be amended to allow IGIS to inquire, in response to a complaint or on his/her own initiative, into the effectiveness and appropriateness of ASIS’s procedures relating to the legality or propriety of its activities.271

9.29 We are not persuaded that the restrictions implicit in the need for ministerial approval in some cases, and a ministerial request in others, would in practice prevent the Inspector-General from mounting inquiries he was determined to pursue. We think it unlikely that a Minister would decline to approve an inquiry by IGIS in circumstances where an Inspector-General regarded the case for it as compelling. The need for ministerial approval or request may lead to negotiations on the scope of an inquiry, and the manner of approach to it, in circumstances where the proposed inquiry concerns matters of particular sensitivity. We accept that there could be cases where such negotiation was appropriate and do not see this as being likely to impede the conduct of a necessary inquiry. This is especially so given that IGIS can report to Parliament if authority for an inquiry is sought and refused.

9.30 We accept, however, that there is a difference of emphasis between a requirement for ministerial approval of an inquiry – which the Inspector-General can initiate – and a provision limiting inquiries to those requested by the Minister, which the Inspector-General regards himself as unable to initiate.272 If the present requirements for a ministerial request as the pre-condition for an inquiry were replaced by requirements for ministerial approval, this would remove any implication that IGIS was inhibited in investigating issues of

270 T172.
271 Exhibit 45.3.1, paragraph 20.
272 Exhibit 23.3, paragraph 48; See also T176.
Oversight by the Inspector-General of Intelligence and Security

Concern, while still allowing the Minister to consider how matters of operational sensitivity should be investigated. We therefore recommend that ss.8(2)(c) and 8(4) be amended to make clear that, provided ministerial approval is first obtained, IGIS may inquire into the procedures of ASIS governing the legality and propriety of its activities, and into actions of ASIS within Australia which do not affect Australians and do not involve any possible violation of Australian law.

9.31 As far as ASIS activities abroad are concerned, IGIS initially expressed the view that he should not require ministerial approval before examining activities abroad which affected Australian citizens or permanent residents. This proposition was opposed by the Minister, and was not maintained in the Inspector-General's final submission, which accepted that the pre-condition of ministerial approval could be justified as a means of protecting sensitive operational activities. We agree.

9.32 Mr Holdich argued that the power to conduct a preliminary inquiry should not be confined, as at present, to an inquiry prompted by a complaint. The power should also be available when the Inspector-General is contemplating an inquiry of his own motion. We see merit in this proposal and recommend that the power in this respect be widened.

9.33 The amendments we propose affect DSD as well as ASIS. Our Terms of Reference have not required us to consider the practical implications of applying the changes to DSD, but we expect that the principles of accountability and control which have guided our recommendations on ASIS would apply equally to DSD.

9.34 We agree with Mr Holdich that the degree of assurance to the Minister and the public would be enhanced if IGIS increased the level of monitoring activity by extending the areas over which regular oversight is maintained, within the jurisdictional limits, and by assigning a higher priority and dedicated resources to this function. As Mr Holdich acknowledges, this would require a deliberate emphasis on own motion inquiries, treating them as a non-discretionary aspect of the office's agenda. Such an approach would be consistent with the primacy of the monitoring function envisaged for the Office.

---

273 T164.
274 Exhibit 39.1, answer to question 31.
275 Exhibit 45.3.4, paragraph 85.6.
276 Exhibit 45.3.1, paragraph 21(a).
The development of a systematic plan of monitoring activities in relation to ASIS would, we think, be feasible and is overdue.

Monitoring of ASIS dealings with information on Australians

9.35 As we have pointed out in Chapter 3, ASIS has, since 1988, been subject to Cabinet-approved rules governing its collection, retention and communication of information concerning Australian citizens. We have recommended that those rules be given legislative force. One benefit of this would be to make plain the circumstances in which, and the purposes for which, ASIS is entitled to hold and pass on such information.

9.36 In his 1993-94 annual report, the Inspector-General reported that he had visited ASIS on several occasions to examine the holdings on Australian citizens and permanent residents. This investigation was prompted by the assertion that ASIS improperly held thousands of files and cards on Australian citizens. The Inspector-General found nothing of concern, a conclusion which we have independently confirmed.277

9.37 The Inspector-General indicated in evidence that he regarded further investigation of these holdings as a high priority, to which he would devote any additional resources which might become available for his monitoring role.278 The Inspector-General is conscious that he has so far examined only a very small proportion of ASIS’s holdings on Australians279 and, given sufficient resources, would propose to hold a more systematic inquiry.280

9.38 This regular monitoring provides a valuable assurance and should be continued. The monitoring would be enhanced if ASIS established, for internal use, a list of the categories of information concerning Australians which ASIS staff were permitted to collect and retain. ASIS in practice uses categories similar to those identified in our own investigation281 but a clearly defined list would operate both as a guide and as a discipline for the Service. In particular, it would assist the Inspector-General in assessing whether a particular holding was permitted by the rules or by the legislative provisions which we recommend should replace them.

277 See Chapter 15.
278 T141.
279 T722.
280 T159.
281 T*1015*.
9.39 The Inspector-General's annual reports have also referred to his monitoring of references to Australians in the intelligence reports which ASIS distributes. This process is likewise governed by the 1988 rules. We are satisfied that this monitoring is comprehensive and results in any apparent departures from the rules being identified, and ASIS being called on to provide justification. This monitoring would similarly be enhanced if ASIS were required, in any case where a report was distributed containing information about an Australian, to annotate its own copy of the report with a reference to the provision of the rules - or the proposed legislation - authorising its communication. We recommend accordingly.

**The gap in assurance**

9.40 These various modifications of the legal framework and of the approach to monitoring should enhance the Inspector-General's oversight of ASIS. But the range of ASIS's activities covered will remain quite limited. We accept the necessity for this because we can see no sensible basis on which an agency whose oversight functions are directed - as they should be - to review of and assurance about the legality and propriety of actions undertaken in Australia, or affecting Australian citizens, can ply a similar trade in relation to the operational activity of ASIS.

9.41 We are comforted that there is, in addition to the monitoring by IGIS, a range of other mechanisms for review and assurance to the Minister, Government and Parliament that ASIS is properly performing the functions assigned to it. In particular:

(a) ONA and the tasking and evaluation mechanisms of the AIC provide a check on the tasks ASIS undertakes and the quality of its product;

(b) DFAT supports the Minister's assessment of the risks and benefits of particular operations. The Department's relationship with ASIS helps to keep the Minister informed of the Service's activities and provides a view from outside ASIS on many of them;

(c) SCIS supports the Government's general oversight of ASIS, including through detailed reviews such as that of Richardson;

(d) the Auditor-General currently provides assurance through auditing of the non-exempt accounts. If the Government accepts our recommendations, that assurance will be strengthened by the auditing of the entire ASIS accounts.
9.42 There remains, however, a significant gap in the assurance available to the Minister. The Minister is wholly reliant on the Director-General in the area of compliance by the Service with those parts of the Directive relating to operational control - specifically, the proscription of certain kinds of activity by ASIS in its operations, and the requirements of ministerial approval for specified operational activity. The legislation which we recommend will substantially replace the Directive but it will contain proscriptions, both explicit and implicit. The categories of activity requiring ministerial approval will be the central part of the supplementary directive which we recommend be issued.

9.43 It is not that we have found evidence to suggest that ASIS has failed in the past to adhere assiduously to those parts of the Directive. On the contrary an audit conducted by Commission staff enables us to give the kind of assurance to the Minister which we consider is necessary, on a regular basis, to fill the gap we have identified.
Chapter 10
The Protection of Sources and Methods

What should be protected?

10.1 The proposition that secrecy is crucial to the operations of a secret intelligence service is incontrovertible.\textsuperscript{282} Since the primary function of ASIS is to collect secret foreign intelligence, it necessarily follows that information about its intelligence collection activities – where, how and by whom they are carried out – must remain secret if the activities are to be viable.

10.2 The importance of secrecy is heightened by ASIS’s dependence on human source intelligence. In responding to media disclosures in early 1994, the Minister for Foreign Affairs reminded editors that:

\emph{ASIS relies upon people who, sometimes at considerable risk to their lives and liberties, are willing to provide Australia with the information it needs. These sources of intelligence are a national asset and require protection – indeed, ASIS and the Government have an obligation and a duty to protect Australia’s sources and hold secure information about them. Source protection is the reason for the secrecy that surrounds ASIS \textsuperscript{283}}.

10.3 Disclosure of information about a particular operation directly affects the operation itself and those involved. Such disclosure is also likely to have indirect effects which are detrimental to the operational effectiveness of ASIS.

10.4 There are also adverse consequences of a non-operational kind. Both ASIS and the Minister refer to the damage which may be caused to Australia’s foreign relations by the disclosure of an ASIS operation.\textsuperscript{284} ASIS is also

\textsuperscript{282} Exhibit 20.1, paragraph 2.1.
\textsuperscript{283} Exhibit 12.9.1; Exhibit 12.10.1; see also T46.
\textsuperscript{284} Senate \emph{Hansard} 23 November 1988, p.2613 (Exhibit 12.1, tab 1); Exhibit 20.1.18, paragraph 5.
concerned about the loss of public and parliamentary confidence ‘among those who know little of the Service and never learn of its services and value to the nation’. If the disclosure is made by an officer or former officer of the Service, there may be an adverse impact on staff morale.

10.5 In our view, there are two fundamental considerations which create the need for secrecy and which determine the scope of the protection it requires. The first is the need to maintain the operational effectiveness of ASIS. The second is the need to protect the individuals who take part in ASIS operations, ASIS officers as well as their sources. The Minister would rank with these the need to avoid damage to foreign relations. We recognise, of course, that disclosure of an operation or alleged operation can cause acute diplomatic embarrassment, but arguably this is not as compelling a consideration as the first two. In any case, the secrecy required in order to protect operations and individuals should be sufficient to ensure that diplomatic embarrassment is avoided.

10.6 Media witnesses who gave evidence regarding the D Notice system generally accepted the necessity of protecting operations and individuals. They acknowledged the continuing acceptance by their organisations of the rationale for the D Notice system, that there is a public interest in the non-disclosure of certain classes of information. There were varying views as to how those classes should be defined in relation to ASIS, but there was consensus that – except in quite exceptional circumstances – information should not be published which would put individuals at risk. Most were prepared to accept a wider proposition that there is a public interest in the collection of foreign intelligence which necessarily depends upon the secrecy of the activity and that – subject again to exceptional circumstances – the non-disclosure of current operations was therefore justified.

10.7 What, then, is to be protected? It follows from what we have said that the focus of protection must be to prevent disclosure of information about what ASIS is doing, or planning to do, and where. Such disclosure may be direct – for example, by reference to a particular operation or by identification of an ASIS officer as engaged in intelligence collection in a particular place – or it may be indirect. Indirect disclosure may take a number of different forms, including:

---
285 Exhibit 20.1.18, paragraph 5.
286 Exhibit 20.1, paragraph 8.4.
287 Exhibit 12.1, tab 1.
(a) a reference to a past operation, from which the existence of a current operation can be inferred;

(b) disclosure of locations in which ASIS works;

(c) disclosure of details of the ASIS expenditure budget; and

(d) disclosure of information about ASIS reporting, which can reveal how, where and from whom the information was obtained.

Direct and indirect disclosures of these various kinds may put individuals at risk, as well as threatening present and future operations.

10.8 Whether a particular disclosure causes damage to ASIS, or puts individuals at risk, will depend on its content. A direct disclosure of a current operation will certainly be prejudicial to the work of ASIS because of its effect on the operation. Indirect disclosures, however, may or may not cause significant damage, depending on the nature of the disclosure. The same is true of disclosures about management matters. For example, the disclosure of changes in ASIS deployments would have far more serious potential consequences for ASIS than the disclosure of its total staffing complement. Either of these would be likely to be more damaging than the publication of a new grievance procedure. The more authoritative the source, the more damaging the disclosure is likely to be. What might be no more than mere gossip will carry weight if attributed to an officer or former officer. In the same way, an untrue statement by an officer or former officer is potentially very damaging, because of its apparent authenticity.

10.9 Having identified the interests which require protection, the more difficult task is to determine how much secrecy is necessary to achieve the required degree of protection. A number of competing considerations must be weighed up. On the one hand, ASIS emphasises that the need to defend the Service and its operation from penetration and compromise by hostile intelligence and security agencies entails a high degree of protection of information:

ASIS knows ... that there is nothing about a target intelligence or security agency and its personnel that is not of some significance ... Every item of information about ASIS and its personnel that leaks or is extracted from the Service is potentially if not actually damaging, and if not now then at a future time. The significance of each item of information may not be apparent at the time it is leaked or obtained, and may only be fully appreciated when seen as part of the
larger picture. Information of no great present significance may assume crucial significance in light of later developments or information.\footnote{Exhibit 22.1.2, paragraph 3.}

Taken to its logical conclusion, this line of argument would prevent disclosure of any information about ASIS at all. We do not understand the Service to intend that result.

10.10 On the other hand, there are powerful reasons for ensuring that the extent of secrecy is no greater than is truly necessary. First, and most importantly, there is a competing public interest in the free flow of information and opinion relating to Government, and in the public discussion and criticism which it facilitates. It is vital for the process of good government and good administration that this should occur. Striking the balance between these competing interests is of the essence both of the voluntary D Notice system\footnote{See chapter 11.} and of the law regarding unauthorised publication.\footnote{See chapter 13.} Secondly, the principles of accountability require that information about ASIS be disclosed to the Government and, as we have said in Chapters 4 and 5, to the Opposition and the Parliament, subject to adequate safeguards. Thirdly, there is the more general problem for ASIS that secrecy tends to breed suspicion in the public mind. ASIS has suffered from this in the treatment its alleged activities have received in the media and from commentators who, through no fault of their own, lack even a basic understanding of what ASIS does and does not do, or of how it accounts for itself. Chapter 15, on the public face of ASIS, looks at better ways of satisfying public interest while maintaining an acceptable level of protection for information.

10.11 Fourthly, the unnecessary withholding of information from staff can itself be detrimental to the functioning of the organisation. Finally, there must be some avenue for ASIS staff to disclose information about ASIS which demonstrates illegality or serious maladministration. This we discuss in Chapter 13, in the context of whistleblower protection.

10.12 Clearly, the scope and limits of legitimate secrecy cannot be defined with precision. But once it is recognised that there are limits to secrecy – and the Service has recognised this – energies can be concentrated on protecting what is most important. Provided that the key interests – the safeguarding of operations and the protection of individuals – are kept firmly in view, there is every
prospect that the limits will be defined appropriately and will be accepted as legitimate by the media and by the community at large.

The mechanics of protection

10.13 The existing safeguards against disclosure of sensitive ASIS information fall into two categories. The first comprises the systems and procedures internal to ASIS which are designed to keep information secure within ASIS itself. The second category comprises external constraints directed at preventing publication of sensitive information. These external systems – the voluntary D Notice system, civil remedies to restrain publication and criminal remedies to punish publication – are discussed in Chapters 11 to 13. In this chapter we are concerned with the internal arrangements.

10.14 On the evidence, the most serious potential threat to the security of information arises from unresolved grievances of ASIS staff. The view of ASIS about how to deal with this threat appears to have changed, at least in its emphasis, in the course of the Inquiry. At the beginning of the Inquiry ASIS contended that the solution to this threat lay in strengthening the external constraints:

It is the absence of effective, enforceable sanctions, legal or otherwise, against those who knowingly make unauthorised disclosures of classified information into the public domain, that represents the greatest threat to the security of the Service, the broader intelligence community and ultimately the nation.291

10.15 In a later submission, however, the Director-General placed greater emphasis on the critical importance of ASIS resolving grievances or complaints when they arise, so as to prevent them from developing into major issues. He referred to:

the realisation that no legislation, rules, regulations or undertakings can prevent a determined current or former ASIS officer from making unauthorised disclosures if this is the path they choose. It shows that we must do all we can to attempt to reduce the possibility of unauthorised disclosures, and the first step in that chain is to handle grievances and complaints more effectively when they first arise.292

10.16 The Director-General identified various ways in which this issue should be tackled, including a greater acceptance by managers of their

291 Exhibit 20.1.18, paragraph 9.
292 Exhibit 20.1.18.1, paragraph 3.
responsibilities towards their staff, changes in ASIS management culture and improved training for managers and supervisors. In our view, the focus on the internal dimension rather than the external sanctions is the correct one, and we commend the Director-General for his commitment to addressing these issues of management culture and attitude. We are firmly of the view that the internal health of the organisation is the single most important element in the protection of that information which must remain secret.

10.17 There are two related points. The first is that the imperative to avoid unresolved grievances applies with equal force to the management of the sources upon whom ASIS depends and the handling of ASIS staff at and after the point of their separation from the Service. As to the first of these, the Service clearly recognises that the maintenance of a relationship of trust with its sources is essential not only as a pre-condition to the flow of intelligence but in order to prevent discontent. All the evidence suggests that these relationships are handled with great care. Secondly, the Service has acknowledged the importance of dealing sympathetically with staff who are separating from the Service. One aspect of this is career transition management. More generally, we agree with the Service’s submission that the issue of separation must be handled in a way which is sensitive, and which provides practical assistance if possible and a point of continuing contact with the Service after separation. In a case where potential difficulties are clearly apparent at the point of separation, we would see a role for the Service to take the initiative in maintaining contact with the departing officer.

10.18 It is appropriate at this stage to refer to a submission with which we have been pressed from time to time during the Inquiry. The submission of the Service was that it was necessary for the proper satisfaction of our third term of reference to identify any sources within or outside ASIS of information relating to the Service which appeared in the media. We do not agree, and we have rejected applications made for that purpose. If we had mounted such an investigation and had identified serving officers as the sources, or if journalists had been prepared to name them, we would have learned nothing helpful for the purposes of this aspect of our Inquiry. We have elsewhere expressed the view that those of the former officers who did so were not justified in making their disclosures to the media. That disapprobation would apply with no less force to others.

293 Exhibit 45.2.4, paragraph 2.12; Exhibit 45.2.5, paragraph 3.3.5.
10.19 The disciplinary action which might have been open to the Service would be irrelevant to the objects of this Inquiry. Further, it might well be argued that such action would have been to little purpose in the case of serving or former officers. We agree with the view expressed by Mr David McKnight:

The most likely source of leakages at present are aggrieved and disgruntled officers or ex-officers. In my view, the most secure organisation is one which is humane, well run and internally fair and exhibits an *esprit de corps* based on these features, not on authoritarian controls. Any conclusion from this Inquiry that a more punitive approach to 'leaks' will solve the problem will simply fail. 294

10.20 We have dealt above with the various mechanical means of protecting sources and methods. Side by side with those is probably the most effective method of protecting the Service against deliberate disclosures of confidential information from the Service to the media, which is to preserve a high state of morale based upon a fair and open system of management. To aim to establish a system of that kind is not to lend any support to the view, which rightly troubled the Director-General, that in any organisation which deals with highly classified national security information 'you can deal with your personal grievance and bring the organisation to heel by leaking national security information'. 295 Any attitude of that kind must be firmly discouraged, and is not affirmed by the resolution of particular cases.

---

294 Exhibit 46.1, p.5.
295 T*955*.  

112
Chapter 11

The D Notice System

The present system

11.1 The D Notice system is a mechanism for voluntary self-restraint by the media on the publication of sensitive defence, security and intelligence information. The foundation of the system is an acceptance by media organisations – at editorial level as well as management level – that there is a public interest in the non-disclosure of certain categories of information. The D Notices define the categories.296

11.2 The Australian D Notice system was established in 1952. It was modelled closely on the corresponding British system which itself originated in 1912.297 Although in its early years the existence of the D Notice system was itself secret,298 it has been a matter of public knowledge – and intermittent controversy – since the early 1970s.

11.3 The D Notices are issued under the authority of the Defence, Press and Broadcasting Committee (the D Notice Committee). The Committee comprises media representatives and government nominees. It is chaired by the Minister for Defence, whose department is responsible for administrative support to the Committee. The Committee has not met since 1982. At that time, it comprised 16 media representatives – covering both editorial and management – and four Defence representatives.299

296 'D' stands for Defence, reflecting the origin of the notices in the first World War as a means of protecting defence-related information.
298 In November 1967, the Prime Minister, Mr Holt, answered a question in Parliament on D Notices. He described the system in general terms but declined to name the members of the D Notice committee or to specify the number or content of the Notices.
299 Exhibit 11.1.1.
11.4 A D Notice is in the nature of a request to editors. It is not an instruction or a prohibition. As the most recent (1982) D Notice booklet says:

The system is an entirely voluntary one, offering advice and guidance only. Non-observance of a request contained in a Notice carries no penalties. In the end, it is for an editor to decide whether to publish an item of information, having regard to national security requirements.\textsuperscript{300}

11.5 Originally there were seven Notices but this was reduced to four in 1974. The four Notices covered defence equipment and communications; air capabilities; the whereabouts of the Petrovs; and ciphering and monitoring activities. A fifth Notice – on ASIS operations and personnel – was issued in 1977, following the Government's decision to acknowledge publicly the existence of the Service.

11.6 In 1982 the Committee again reviewed the Notices, reducing them to the present four which cover:

(a) the capabilities of the Australian Defence Force, including aircraft, ships, weapons and other equipment (D Notice No. 1);

(b) the whereabouts of Mr and Mrs Vladimir Petrov (D Notice No. 2);

(c) signals intelligence and communications security (D Notice No. 3); and

(d) ASIS (D Notice No. 4).

**Revitalising the system**

11.7 The D Notice system has largely fallen into disuse. Although an ASIS-related program was anticipated, the ASIS D Notice was not drawn to the attention of the ABC before it broadcast the *Four Corners* program of February 1994.\textsuperscript{301} When the Minister drew the attention of individual editors to the D Notice after various ASIS-related publications in 1993 and 1994, the editors concerned – all from leading daily newspapers – confessed to ignorance either

\textsuperscript{300} Ibid.

\textsuperscript{301} Though ABC witnesses gave evidence that the terms of the D Notice had been considered before the program was broadcast.
that the system was still operating,\textsuperscript{302} or of the existence or content of the ASIS D Notice itself.\textsuperscript{303} The description of the system as moribund\textsuperscript{304} seems apt.

11.8 The clear view of the media is that the D Notice system should be revived, not buried. We took evidence from a number of senior representatives of the print and electronic media,\textsuperscript{305} all of whom supported the continuation of the D Notice system. Significantly, no media representative argued for the abolition of the system as an unreasonable restraint on publication, although one editor considered that the media would look more sceptically at a reactivation of the D Notice system in the post-Cold War period.\textsuperscript{306} Rather, the prevailing concern was to oppose the suggestion, given some speculative coverage in the media, that the system be made compulsory and sanctions imposed for breach. No such suggestion was advanced in the course of our proceedings.

11.9 As we pointed out in Chapter 11, the media witnesses acknowledged the continuing acceptance by their organisations of the rationale for the D Notice system. It is not seriously contested that there is a public interest in the non-disclosure of information which would endanger individuals. Most witnesses accepted that the non-disclosure of current operations was also justified on grounds of prejudice to the operations,\textsuperscript{307} with the important proviso that there might be an overriding public interest justifying the disclosure of, for example, illegality or serious impropriety, even if to do so would involve disclosing a current operation.\textsuperscript{308}

11.10 ASIS, on the other hand, submitted that the voluntary system suffered from fundamental problems, and should be replaced by a voluntary ‘code of conduct’. According to the Service:

\begin{quote}
The current D Notice [system] is inadequate because it relies on voluntary media restraint, which no longer exists. Changes in Australian society since the 1950s have led to debate as to how principles of public participation and independence of the media can be reconciled with secrecy required for the sake of the national
\end{quote}

\textsuperscript{302} Mr Kelly, T*690*.
\textsuperscript{303} Exhibits 12.5.3 and 12.6.3; cf. Mr Kohler, T*818-19*; Ms Grattan, T*867*, T*898-9*.
\textsuperscript{304} Mr Ayers, Exhibit 35.1, p.2.
\textsuperscript{305} Those who appeared before the Commission were: Mr David Hill, Managing Director, and Mr Chris Anderson, Managing Editor, Australian Broadcasting Corporation; Mr Peter Harvey, Director of News, Canberra Bureau, Nine Network; Mr Paul Kelly, Editor-in-Chief, The Australian; Mr Dennis Grant, Bureau Chief for Channel Seven; Mr Alan Kohler, Editor, The Age; and Ms Michelle Grattan, Editor and Mr Jack Waterford, Deputy Editor, The Canberra Times.
\textsuperscript{306} Mr Kelly, T*693*.
\textsuperscript{307} But see the evidence of Mr Hill, T*635-37*.
\textsuperscript{308} T*874*. 

115
interest. This debate has engendered increasing disagreement on what constitutes the national interest. The media organisations have shown by their actions that they will decide what the public interest is in any given situation without assistance from those affected. The media organisation's perception of the national interest appears to coincide with its own journalistic interests.309

ASIS also pointed to differences in the interpretation of the ASIS D Notice by different organisations and what it argued was inadequate verification by media organisations of the content of stories proposed to be published and inadequate assessment of compliance (or otherwise) with the D Notice.

11.11 The essential elements of the code of conduct proposed by ASIS were:

(a) a summary of information on the role, functions, oversight and accountability of ASIS;

(b) a statement of the Government’s commitment to the protection of intelligence assets and sources;

(c) an explanation of the potential of ASIS-related material to identify staff and sources; and

(d) the identification of points of contact for the media to seek advice on the content of proposed stories on ASIS.

This code would no longer define specific matters which should not be published, that being the function of a specific legislative prohibition against the identification of ASIS staff and sources.310

11.12 In Chapter 13, we have recommended the enactment of a specific legislative prohibition, directed (like s.92 of the ASIO Act) at the identification of individuals. We are not, however, persuaded that the voluntary D Notice system should thereupon be abandoned. In the first place, the scope of the D Notice is considerably wider than that of the proposed legislative provision. Most importantly, it deals with the disclosure of information about operations independently of disclosures which identify individuals. Secondly, and more generally, we see an important role, both symbolic and practical, for a voluntary system. The hallmark of the system is that compliance by the media is by consent and not by coercion. In accepting the D Notices, the media are

309 Exhibit 45.2.5, paragraph 3.2.5.3.1.3.
310 Ibid, paragraphs 3.2.5.2.3, 3.2.5.3.4.6, 3.2.4.3.
acknowledging that, in the field of security and intelligence as in others, the right to publish is not absolute and that there are competing public interests:

the essence of the exercise [is] to get the media themselves to reflect upon the balance between the national interest and their right to publish ... which would be harder to do if you established a link between their right to publish and the government's right to punish.311

Provided that sufficient information and assistance is available to enable editors to make judgments about when a D Notice is applicable, the voluntary system should be more effective than a penal provision in preventing publication.

11.13 A voluntary system is also peculiarly appropriate to the role of the media as a vehicle of public accountability for government. We share the view advanced by some of the media that it is important for the process of good government and good administration that there be some light shed on government administration when it goes wrong.312 Provided that the D Notices are designed so as to provide real guidance, and their concept and application are accepted by the media, their existence should ensure that the interests of defence and security are generally given proper consideration in any decision whether or not to publish. The non-coercive nature of the system means that the final decision about what should and should not be published rests with editors, not with governments.

11.14 We recognise that the system is not working satisfactorily at present. There is very limited awareness of the existence of an ASIS D Notice, let alone of its precise terms; the rationale for the specific proscriptions is not understood; and there is insufficient information in the hands of journalists and editors to enable them to assess whether particular publications would or would not breach the D Notice. The result is that, amongst the individual articles and broadcasts which we have examined in detail, there are to be found some clear (though unintentional) breaches of the D Notice. But we believe that the revival of the system along the lines we propose will reduce – although not remove altogether – the risk of such breaches occurring.

11.15 The D Notice system will never provide complete protection. The option of recourse to legal sanctions will always need to be retained. In the next chapter, we examine the civil remedies against media disclosures of information relating to ASIS. In Chapter 13, we discuss the existing, and proposed, criminal

311 T818, H. White, Defence Department
312 Ms Grattan, T*924*; See also Mr Harvey, T*677*; submission from the Age, 18 November 1994.
provisions applicable to such disclosures. Given the apparent reluctance of Governments to activate legal process, either civil or criminal, against journalists, we see the D Notice system as an important mechanism through which Government and media can seek to deal constructively with these complex issues.

A new Notice and a new committee

11.16 In December 1993, the Defence Department initiated a review of the D Notice system. This was partly prompted by a review of the British Notices completed in 1993 but the immediate stimulus was twofold - a contact between the Minister for Defence and a Melbourne newspaper about D Notice No. 3 (concerning DSD) and an expectation that *Four Corners* would disclose information relating to ASIS operations. The preliminary conclusion of the review was that the system should be maintained and revitalised, and that each of the Notices required revision.

11.17 ASIS agreed to redraft its Notice to give 'more focus to the question of the rationale underlying the Notice'. A redrafted ASIS D Notice was submitted to the Minister in February 1994. Both the review process, and the redrafting of the ASIS Notice, were interrupted by the establishment of this Commission. The evidence of media witnesses provided an opportunity for an examination of the content of the present D Notice in the context of actual publication decisions. We consider that the content of the present ASIS D Notice requires examination, as discussed in the next section.

11.18 The D Notice Committee should be re-established and given the task of carrying out a review of the content of the D Notices. The basic structure of the former Committee, with its mixture of media and Government representatives, is appropriate for this task. The media representatives should be drawn from as wide a cross-section as possible, including representation from specialist periodicals. Although in its original conception the D Notice Committee was a forum in which Government dealt with newspaper owners, we endorse the modern emphasis on representation from the editorial side. After all, the key decisions from day to day about whether or not publication is permitted under the terms of a D Notice rest with editors, not owners. On the Government side,
consideration should be given to widening the official representation beyond the Defence portfolio. It seems to us desirable that individual Ministers should participate when D Notices relating to their portfolios are being debated or finalised. This should have the result that the process, and the agreement reached through it, have and are seen to have full Government authority.

11.19 We do not see the D Notice Committee as having a continuing role once agreement is reached about the content of the Notices. Its inactivity since the last revision of the Notices in 1982 underlines the point. In the event of a major review in the future, the Committee could be reconvened. There should, however, be a permanent secretariat to the Committee, which should function on a full-time basis at least until the form of the new Notices is settled. The secretariat should probably be located, as at present, in the Department of Defence, especially if the Minister for Defence continues to chair the Committee. The Department of Prime Minister and Cabinet or the Attorney-General's Department would be suitable alternative locations, but we see no need for a change in the existing arrangement. There is little enthusiasm from other agencies to take on the role.317

11.20 We would see the secretariat's ongoing functions as including the publication, distribution and promotion of the D Notices, communication with editors, monitoring changes in ownership and changes of editor, and ensuring that new appointees are informed of the system. The secretariat should also be available to give advice on request about the functioning of the system, although advice on particular issues arising under one of the D Notices should be provided by the relevant agency. The secretariat would also have a role in monitoring publications on topics to which the D Notices related, but it would again rely heavily on the agencies themselves to keep it informed of relevant publications. It should report to the Government periodically on the results of this monitoring, but the responsibility for responding to particular publications would once again rest with the individual agencies. Whether a Minister became involved in direct contact with a media organisation on a D Notice issue would continue to depend on a case-by-case assessment.

**Reviewing the ASIS D Notice**

11.21 The current (1982) version of the ASIS D Notice opens with a short description of the functions of the Service and a reminder of the importance of

---

317 T819.
secrecy of its activities. The operative part of the Notice is a request to editors not to publish or broadcast information which would lead to:

(a) the identification of individuals employed by the Director-General of ASIS; or

(b) the disclosure of current or projected foreign intelligence activity of ASIS.

The Notice provides some limited further assistance on the question of identification:

Identification does not depend simply upon a name but also upon the publication of an ASIS member's whereabouts or other identifying characteristics. Publication of the name of a person believed to be a former member of ASIS can by association lead to the identification of current members.

11.22 Any review of the D Notice will need to address each of its constituent elements:

(a) a rationale for secrecy;

(b) the defined non-publication area;

(c) assistance to editors in applying the Notice.

We deal with each of these in turn.

11.23 As to the first, the advantage of a clearly-stated rationale is that it reminds editors and journalists that there are sound reasons for restraint in publication. In the case of ASIS, it is a reminder of the need to protect the Service's sources and the well-being of people overseas who are working in Australia's interests. The achievement of this purpose would be enhanced if the D Notice rationale included, or was accompanied by, a fuller account of what ASIS does and why it is important in the national interest — along the lines of the public booklet which the Director-General has been developing.318 This would help to establish the context in which publication decisions are to be made, rather than the D Notice existing — as it does at present — in a vacuum.

11.24 The re-draft prepared by ASIS in early 1994 contains a section of this kind. The draft draws attention to the 'real risk of harm' to which the

318 See Chapter 15.
identification of ASIS staff or sources may expose them or their families. It also points to the prejudice to operations which can flow from the disclosure of identities, emphasising the necessity for intelligence operations to be pursued in conditions of secrecy. As they stand in the draft, these assertions are made in fairly bald terms. We would expect that before such assertions were accepted by media representatives on the reconstituted committee, there would need to be some fuller explanation provided, perhaps with the assistance of some hypothetical examples.

11.25 Defining the non-publication area will be the most controversial part of any review. Not surprisingly, media witnesses expressed their opposition to any widening of the operative part of the ASIS D Notice. The 1994 ASIS draft proposes certain extensions, directed at ensuring the non-publication of information which would lead to:

(a) the identification of the families of ‘individuals employed by the Director-General, ASIS’;

(b) the disclosure of the whereabouts of such individuals or their families;

(c) the identification of visiting foreign intelligence liaison officials; and

(d) the disclosure of past operational activity of ASIS.

11.26 Of these, only the last involves a change of real substance. The first and second are simply an elaboration of the long-established ban on the identification of serving officers. They are consistent with the scope of the legislative prohibition we recommend. See paragraph 13.56. We would add two comments. First, neither the existing Notice nor the ASIS redraft brings former officers within the non-publication area unless their identification would lead to the identification of current officers. Consistently with our recommendation for legislative protection, we consider that the D Notice should extend to former officers and sources. Secondly, the phrase ‘individuals employed by the Director-General, ASIS’, carried over from the existing Notice, is not appropriate to cover – as it is obviously intended to do – the sources of the Service who may or may not be properly characterised as ‘employed’ by the Director-General. The third extension, concerning visiting officials, relies on the same rationale, the
The D Notice System

ASIS Inquiry 1995

protection of individuals, and would in practice be likely to have a very limited operation.

11.27 The proposed extension to past operations is, however, a significant one. According to the rationale set out in the ASIS re-draft, the justification for a specific prohibition directed at past operations is that publicity 'may deny the opportunity for fuller exploitation of a capability or technique'. To this we would add that publicity about a past operation may also tend to identify, and so put at risk, former officers and former sources who participated in the operation. Evidence was given that certain of the articles published about ASIS in early 1994 had had repercussions of this kind, and it seems to us to be understandable that this can occur.

11.28 The effect of the existing Notice is that information about a past ASIS operation may be published unless it would lead to the identification of serving officers or to the disclosure of a current or projected operation. Provided that the non-publication area defined in the D Notice is extended to former officers and sources, as suggested in paragraph 11.26 above, we would regard the extent of the prohibition on disclosure of past operations as being sufficient, albeit that it is an indirect rather than a direct prohibition. That is, information should not be published about a past operation if (but only if) that publication would tend to identify either a serving or a former officer or source or would disclose a current or projected operation. The explanatory section of the D Notice should make quite explicit that past operations are, in this indirect sense, within the ambit of the Notice.

11.29 The rationale advanced by ASIS does not persuade us that a blanket prohibition on the disclosure of information about past operations is justified. While we can conceive of circumstances where publication of information about an operational capability or technique would impede its future operational use or otherwise prejudice current operations, we would have thought this would be a relatively rare occurrence. At the other end of the scale, there are operational techniques, which are now a matter of notoriety, and public reference to them cannot sensibly be said to inhibit their future use. This is the kind of issue to which the D Notice itself could usefully draw attention, urging the need for caution.

11.30 Whatever may be decided about the ambit of the proscription, it is essential that the Notice contain some fuller explanation of the kinds of considerations which need to be borne in mind by editors in deciding whether or not the publication of a particular piece of information will contravene the terms
of the Notice. There was considerable discussion during the evidence of media witnesses about the difficulties associated with assessing the sensitivity of particular pieces of information. It was acknowledged by most that there was considerable complexity associated with determining whether, for example:

(a) the publication of a statement purporting to describe a past operation would, if that operation were in fact still current, tend to disclose that operation;

(b) the identification (by name or otherwise) of a former officer as having carried out operations in the past in a particular place would tend to lead to the identification of his/her successors at the relevant station; or

(c) the disclosure of a past operation would expose to present risk those officers or sources who had been involved in that operation.

11.31 The revised Notice should give as much guidance as possible on how these linkages can be made. It might, for example, usefully give some illustrative examples. In addition, the Notice should encourage editors and their staff to seek advice, either via the proposed D Notice secretariat or direct from ASIS, about a publication under consideration and the applicability of the Notice.

**ASIS media liaison officer**

11.32 Whatever the precise text of the ASIS D Notice, its application involves the making of what are agreed on all sides to be complex judgments. Most witnesses conceded that media organisations are necessarily less well placed than Government, or the Service in particular, to make those judgments.\(^{320}\) In this context, there was much discussion of the concept of an ASIS media liaison officer who, amongst other functions, would be available to media organisations to provide advice regarding the sensitivity of particular pieces of information. Understandable scepticism was expressed about this proposal, because it was thought that such contact might simply alert the Government to an impending publication and provoke an injunction application, and because – at least initially – there would be doubts about the reliability of the advice provided. There was also a natural suspicion that the advice would tend to be self-serving.

\(^{320}\) See for example, Mr Kelly, T*711*.
Nevertheless, the majority of media opinion was supportive of the notion, provided that it was left to media organisations to decide whether or not to avail themselves of the service. The solicitor for the *Age*, Mr Bartlett, likened the proposal to his regular recourse to advice from the Office of the Victorian Director of Public Prosecutions about whether publication of material regarding a criminal trial would be prejudicial.\textsuperscript{321} ASIS also expressed support for the creation of a media liaison position, in the expectation that the officer's advice would be 'likely to provide a brake for the more outlandish stories'.\textsuperscript{322}

We recommend that ASIS establish such an office for this advisory purpose (amongst others). We say more about the functions of such an office in Chapter 15. The selection of the right person to hold the office would, of course, be critical, as the success of it would depend very much on the ability of the person to establish credibility with media organisations. That credibility would depend on the officer establishing over time that advice given was not misleading. Media representatives understand that there will be times when the officer can do more than offer 'no comment'. But, where advice can be given, credibility will be earned if it can be established progressively, by example, that advice or information given is truthful and factually well-based. Once credibility is achieved, the office will be likely to contribute significantly to a generally constructive relationship between ASIS and the media. In the present context, it has the potential to help make the D Notice system more effective. It need hardly be added that, were contact with that office in the D Notice context to be seen to lead to injunctive action, credibility would be likely to be impaired and this would undermine the operation of the D Notice system. We discuss this problem in Chapter 15.

\textsuperscript{321} T*824*, *827*.
\textsuperscript{322} Exhibit 45.2.5, paragraph 3.2.5.7.3.
Chapter 12

Civil Remedies to Prevent Unauthorised Disclosures

Background

12.1 During 1993 and the early part of 1994, the print and electronic media carried a number of stories relating to ASIS. Some of these referred to operational activities, past and present, by particular individuals in particular places. They thus disclosed information (or what purported to be information) of a kind which should ordinarily be protected.323

12.2 The only remedy of any real potency against unauthorised disclosures is the injunction to restrain publication. There are other remedies available after a disclosure has occurred, including damages, an account of profits and an order for destruction or delivery of documents, but by then the damage to the public interest has occurred. It is damage which cannot be compensated in monetary terms.

12.3 The critical thing, therefore, is to prevent the disclosure before it occurs. But unless there is advance warning of the disclosure, the injunction remedy is useless. It is rare for the Government to have sufficient warning to justify an application for a restraining order. Publishers and broadcasters do not ordinarily give formal advance notice of publication of secret material. Even where some notice is given, it will not usually identify with any precision what is to be published. Government needs to know enough about the proposed publication to enable it to decide whether the damage likely to be caused by publication warrants its acting to restrain publication and being seen accordingly as a censor.

323 See Chapter 10.
12.4 On occasion, armed with the requisite knowledge, the Government has successfully taken injunctive action. In one case, the application was based on a promotional leaflet describing the contents of a forthcoming book. In another case, the High Court granted an interim injunction to restrain publication of a magazine on the basis of a reported conversation with its editor about its proposed content, and in related proceedings in the Federal Court the Commonwealth obtained on subpoena the manuscript of a forthcoming book, the contents of which were subsequently negotiated with the authors to delete sensitive material.

12.5 In all but one case, the disclosures about ASIS during 1993 and 1994 occurred without warning. The Government was, as a result, unable to take any preventive action. In the case of the Four Corners program which triggered this Inquiry, the Government, and the Service, had warning that the ABC was proposing to broadcast an ASIS-related program although the precise timing and content were unknown.

12.6 In this chapter we examine the legal remedies and procedures currently available to the Government to prevent the disclosure of sensitive information. We first outline the present state of the law. We then review the unusual circumstances leading up to the Four Corners program, before considering whether any reform of the law is indicated.

The existing remedies

12.7 Of the available causes of action, breach of confidence and breach of contract are likely to be of most assistance. As to the first, the relevant equitable principle is that:

the court will "restrain the publication of confidential information improperly or surreptitiously obtained or of information imparted in confidence which ought not to be divulged" (Lord Ashburnon v. Pape [1913] 2 Ch. 469, at 475, per Swinfen Eady L.J.). In conformity with this principle, employees who had access to confidential information in the possession of their employers have been restrained from divulging information to third parties in breach of duty and, if they have already divulged the information, the third parties themselves have been restrained from making disclosure or making use of the information.

If the intending publisher is an employee or former employee of the Commonwealth, there may be a breach of the fiduciary duty not to disclose, without authority, information acquired in the course of the employment.328

12.8 The claim in contract will ordinarily be available only against an employee or former employee of the Commonwealth. Its basis would be a claim to restrain a breach by the (former) employee of a contractual obligation such as an undertaking not to disclose information acquired in the course of the employment or an undertaking not to publish without pre-publication clearance.329 Legal advisers to both the CIA and SIS regard the obligation to seek pre-publication authorisation as the starting point for injunctive action against an employee or former employee.

12.9 Where the intending publisher is a former ASIS employee, the contract of employment will of course have come to an end. The secrecy agreement which ASIS employees are now required to sign is, however, a separate, collateral contract, under which the ASIS employee agrees never to make an unauthorised disclosure. This collateral contract survives the expiry of the employment contract itself.

12.10 The key issue for the Commonwealth, as a prospective plaintiff, is whether it can demonstrate to the court that the anticipated disclosure will include material damaging to the public interest to the requisite degree. This is so whether the obligation of confidence sought to be enforced is grounded in equitable principle or in contract. An Australian court will not restrain publication at the suit of the Commonwealth unless it can be demonstrated that there will be damage to the public interest 'because national security, relations with foreign countries or the ordinary business of government will be prejudiced'.330 The court may be called on to consider whether the public

327 Commonwealth v. John Fairfax and Sons Limited (1980) 147 CLR 39 at 50 per Mason, J.
328 In Snepp v. United States (1980) 444 U.S. 507, the United States Supreme Court held that a former CIA employee had breached a fiduciary obligation by publishing a book about Agency activities without pre-publication clearance. The proceeds of the breach were, accordingly, impressed with a constructive trust for the benefit of the Government. A claim based on fiduciary obligation was advanced by the British Government in the Spycatcher case - see Attorney-General (UK) v. Heinemann Publishers Australia Pty Ltd (1988) 165 CLR 30.
329 Exhibit 11.2.2. The standard ASIS secrecy agreement now in use includes undertakings of both kinds.
330 Fairfax (supra) at 52.
interest in publication overrides the risk of damage if the information is disclosed.331

12.11 In Commonwealth v. Fairfax, Mason J. enunciated principles which will govern the court's approach to the question of detriment:

It can scarcely be a relevant detriment to the government that publication of material concerning its actions will merely expose it to public discussion and criticism. It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to a government when the only vice of that information is that it enables the public to discuss, review and criticize government action.

Accordingly, the court will determine the government's claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected.

The court will not prevent the publication of information which merely throws light on the past workings of government, even if it be not public property, so long as it does not prejudice the community in other respects. Then disclosure will itself serve the public interest in keeping the community informed and in promoting discussion of public affairs. If, however, it appears that disclosure will be inimical to the public interest because national security, relations with foreign countries or the ordinary business of government will be prejudiced, disclosure will be restrained. There will be cases in which the conflicting considerations will be finely balanced, where it is difficult to decide whether the public's interest in knowing and in expressing its opinion, outweighs the need to protect confidentiality.332

These principles were publicly endorsed by the Minister for Foreign Affairs in 1988.333

12.12 The Commonwealth may also have a cause of action in breach of copyright. In the Fairfax case, it was the only basis on which the High Court was prepared to grant an injunction. But the significant limitation on the utility of copyright in relation to the protection of confidential information is that it protects only the form of the copyright work, not the information or ideas contained in it. Thus, if the purpose is to restrain disclosure of information contained in a document, rather than the publication of the documents as such, an injunction based on copyright will be of no practical use because the information can be published in a different form. As a matter of policy, the Commonwealth has not, in recent times, relied on copyright when its real claim

331 Ibid., see also Attorney-General (UK) v. Heinemann (supra) at 45.
332 147 CLR at 52.
333 Senate Hansard, 23 November 1988, p.2614.
is that publication of the information in a document will damage the public interest.\textsuperscript{334}

12.13 It may be possible to demonstrate that the anticipated disclosure will, if it occurs, constitute a breach of the criminal law – for example, of ss.70 or 79 of the \textit{Crimes Act 1914}.\textsuperscript{335} On the present state of the law, however, a threatened breach of the criminal law would not be sufficient for the Commonwealth to obtain an injunction. In \textit{Fairfax}, Mason J. noted that the issue of an injunction to restrain a threatened breach of criminal law was exceptional, confined in practice to cases where an offence was frequently repeated, in disregard of an inadequate penalty, and to cases of emergency. His Honour concluded that s.79 was not designed to provide a civil remedy to protect the government's right to confidential information.\textsuperscript{336} We consider below the proposal by the Gibbs Committee on Review of Commonwealth Criminal Law that the Crimes Act be amended to provide specifically for the grant of an injunction in respect of a threatened breach of the relevant criminal provisions.

12.14 The defence of public interest, also known as the defence of iniquity, applies to disclosure of confidential information.\textsuperscript{337} It is probably also available when the claim is brought in copyright.\textsuperscript{338} According to Mason J in \textit{Fairfax}, the defence is limited in scope:

\begin{quote}
\textit{It makes legitimate the publication of confidential information ... so as to protect the community from destruction, damage or harm. It has been acknowledged that the defence applies to disclosures of things done in breach of national security, in breach of the law (including fraud) and to disclosure of matters which involve danger to the public.}\textsuperscript{339}
\end{quote}

It is not possible to characterise with precision the degree of wrongdoing the disclosure of which would be sufficient to attract the defence in a particular case. Clearly, the matter disclosed must be of a serious nature.\textsuperscript{340}

\textsuperscript{334} Exhibit 13.3, p.2. \textit{Unauthorized Disclosure of Government Information}, Attorney-General's Department, 30 October 1991. We acknowledge the assistance we have derived from this paper, and from a written commentary on this issue prepared at our request by its author, Mr B. Leader, Deputy Government Solicitor (Litigation).

\textsuperscript{335} See Chapter 13.

\textsuperscript{336} At 491.

\textsuperscript{337} \textit{Fairfax} at 56-57. See also \textit{Attorney-General v. Observer Limited} [1990] 1 AC 109.

\textsuperscript{338} \textit{Fairfax} at 57.

\textsuperscript{339} Ibid.

\textsuperscript{340} Beloff \textit{v. Presdram} (1973) 1 All ER 241, 260; \textit{A v. Hayden} (1984) 156 CLR 532 at 545-56.
Proposals for law reform

12.15 In the light of the *Four Corners* experience, we have considered whether the law requires modification to reduce or remove the impediment to injunctive action which the Government's lack of knowledge about content often creates. There are two principal ways in which this could be done. First, the substantive law could be altered to remove or modify the obligation to demonstrate a likelihood of damage to the national interest in the event of publication. Secondly, the procedural steps available to the Commonwealth could be strengthened to facilitate access to documents or other information likely to reveal content. We deal with these possibilities in turn.

Substantive law

12.16 The Gibbs Committee has recommended the amendment of the Crimes Act to create specific offences for disclosure of intelligence and security information. The Committee further recommended that there be a provision enabling the Commonwealth to obtain an injunction where there is a threatened breach of one of the criminal provisions.

12.17 We support this recommendation, but with a qualification. The Committee proposed that disclosures by officers or former officers of the intelligence and security services be punishable without proof of damage. It recommended that the availability of the civil remedy of an injunction be subject to the same requirements of proof of damage as would apply in a prosecution. This would seem to mean that, in the case of an officer or former officer of ASIS, the Commonwealth as applicant would need only to show the threatened disclosure of information 'relating to intelligence or security', without the need to show that its publication would be damaging. This would represent a very significant change in the law, beneficial to the Commonwealth.

12.18 In Chapter 13, however, we have recommended that the requirement to prove damage should be dispensed with only where the offence alleged to have been committed by the officer or former officer is the disclosure of information identifying current or former officers, sources or operations of ASIS. If this recommendation regarding the criminal provisions were accepted, it would have the effect of narrowing any benefit which the companion injunction provision confers on the Commonwealth. That is, in a proceeding for injunction

---

341 Exhibit 14.4.
342 Ibid, paragraph 31.39.
343 Ibid.
to restrain a threatened breach of the criminal provisions, the Commonwealth would be required to adduce proof of the damage which the apprehended disclosure was likely to cause, except where the defendant to the civil proceeding was an officer or former officer and the threatened disclosure concerned individuals or operations. While not having to prove damage in those particular circumstances, the Commonwealth would nevertheless need sufficient evidence to demonstrate that the threatened disclosure was likely to identify individuals or operations. It is evidence of that very kind which, under present circumstances, is required to prove the threat of detriment but which is so often lacking.

12.19 Whichever formulation of the criminal provisions is adopted, proof of likely damage will remain a pre-requisite for injunctive relief against anyone other than an officer or former officer, including media organisations and commercial publishers. Neither the Service nor the Minister suggested that there should be any change to the law in this regard and we, for our part, see no reason to recommend a change.

12.20 A separate issue concerns the publication of what purports to be information about ASIS but which is in fact untrue. Such a publication can be damaging to the Service or to individuals, especially if the source is authoritative. At present, the publication of false information would not be either a breach of confidence or a breach of contract because, by definition, it would not be a publication of information obtained in confidence or derived by the defendant in the course of his/her employment with the Commonwealth. In the case of a threatened disclosure by an officer or former officer, this problem will disappear if the Gibbs Committee recommendations are accepted. Since the disclosure of false information by an officer or former officer will be an offence, injunctive relief will be available to restrain the commission of that offence.

12.21 We are not otherwise persuaded that this problem is of significant magnitude to justify any change in the law. We think it somewhat unlikely that the Commonwealth would know in advance that false information was to be published. In any case, the disclosures about ASIS in 1993 and 1994 suggest that false information would almost certainly be intermingled with one or more true statements. Moreover, false information about ASIS would in most – perhaps all – cases be coloured by knowledge gained in the course of employment or otherwise in confidence, in order to give it plausibility. A description of a fictitious operation, for example, is likely to be couched in terms drawn from true operations, derived from actual experience. It follows that in most cases the disclosure can be dealt with adequately under the present law.
12.22 The Government's concern will continue to focus on preventing publication of information in the two key categories, relating to individuals and to operations respectively. Those are the categories where the likelihood of damage flowing from disclosure is most obvious. In our view, there must be a greater readiness on the part of the Government and the Service, when they have notice of a possible disclosure of such information, to make a direct approach to the intending publisher for the purpose of identifying what is sensitive and seeking to negotiate undertakings not to publish the sensitive information. An approach to the ABC in early 1994 might have been worthwhile, at least in modifying the content of the *Four Corners* program. An approach based on early contact and negotiation has clear advantages over litigation, and is consistent with the way in which we see a revitalised D Notice system working.

**Procedural mechanisms**

12.23 Court rules in the various Australian jurisdictions make provision for applications for preliminary discovery. A prospective plaintiff (A) can apply for pre-action discovery against a prospective defendant (B) for the purpose of enabling A to determine whether to commence a proceeding against B. A must demonstrate that B is likely to be in possession of relevant information, and that all other reasonable inquiries have been made. In circumstances such as those preceding *Four Corners*, this procedure would have enabled the Commonwealth to make application for discovery by the ABC of any documents in its possession or under its control relevant to a potential claim by the Commonwealth for breach of confidence or breach of contract. If such an application had been made in early February 1994, and had succeeded, the ABC would have been required to produce the material it had gathered in preparation for the program.

12.24 There is no evidence that consideration was given to the use of this procedure. This was presumably because of a concern that such an application, which must be made on summons, would have alerted the ABC to the Government's awareness of the program and might have prompted an early screening of the program. Even the making of such an application ex parte would not solve that difficulty, since the order for discovery must necessarily be served on the other party. The obligation to comply with the order does not, of course, inhibit publication in any way. In any case, the privilege against self-

---

344 See for example Federal Court Rules 0.15A r.6.; Rules of the Supreme Court of Victoria, Rule 32.05.
345 Exhibits 12.4.2, 12.4.3, 12.4.4.
346 T2527.
incrimination might be invoked as a ground for resisting the production of documents.

12.25 ASIS submitted that the court rules should be amended to give the Commonwealth an entitlement in ‘national security cases’ to interrogate potential defendants about what they possess. This would have the advantage of extending the scope of the existing rules to non-documentary information. The Service was pessimistic about its proposal, because of the improbability of uniformity being achieved in all Australian jurisdictions. The problem of uniformity would largely disappear if, as is proposed, jurisdiction were conferred on the Federal Court in proceedings brought by the Commonwealth. But an order for interrogatories, like an order for discovery, would not prevent publication and might in fact precipitate it. Once again, the provision of answers to interrogatories might be resisted on the ground of tendency to incriminate.

12.26 Finally, we were invited to consider the ex parte order for entry and inspection of premises. Developed in the intellectual property field, this remedy is obtained without notice to the defendant and before any writ is issued. Sometimes known as an Anton Piller order, it permits a plaintiff to enter a defendant’s premises, to search for evidence of infringement of intellectual property rights and to seize and retain infringing material.

12.27 Such orders have been made in cases involving breach of confidence. The pre-conditions for the grant of such an order are, however, quite strict:

First there must be an extremely strong prima facie case. Secondly, the damage, potential or actual, must be very serious for the applicant. Thirdly, there must be clear evidence that the defendants have in their possession incriminating documents or things, and that there is a real possibility that they may destroy such material before any application inter partes can be made.

12.28 There are two obstacles to the utilisation of such a procedure. The first is the one already referred to, of alerting the prospective defendant who may, even after seizure of the documents, proceed to publish. Secondly, the requirement of ‘an extremely strong prima facie case’ may be difficult to satisfy. In any case, the Anton Piller order, like the Mareva injunction, has been

347 E.g. in respect of a subsequent charge under the Crimes Act (see 12.13 above).
348 Exhibit 45.2.5, paragraph 3.2.2.2.
351 Anton Piller (supra) at 167.
fashioned by the courts as a means of preserving the status quo – in the case of Anton Piller by preventing the destruction of evidence relevant to the plaintiff's case. It is not designed to supply the plaintiff with information about the defendant’s state of knowledge or intentions. In an appropriately serious case such an order could be sought by the Commonwealth, and we see no reason to recommend any statutory alteration of the conditions of its availability.

12.29 The Commonwealth always has the option of commencing proceedings for injunction and issuing a subpoena requiring the intending publisher to produce relevant documents. The obstacle here is that, if the subpoena can be characterised as a 'fishing' expedition, designed to elicit documents out of which an otherwise indistinct cause of action can be constructed, it is liable to be set aside. In other words, the subpoena approach will only assist if the Commonwealth already has sufficient information in its possession to justify the commencement of the proceedings.

Conclusion

12.30 It is apparent that the various procedural steps available to the Commonwealth are not designed to give it the advantage which it needs in seeking to restrain publication. That advantage depends on advance knowledge being obtained without notice to the intending publisher. It is, of course, conceivable that if an application for pre-action discovery were made, the intending publisher might elect to withhold publication and provide the documents sought, so as to enable a court determination of the Commonwealth's claim. But this would, we think, be a rather rare occurrence.

12.31 We recognise the significant obstacles which stand in the way of civil action by the Commonwealth to prevent unauthorised disclosures. We are not, however, persuaded that any change to the law or procedure is required, beyond that which will flow from the adoption of the Gibbs Committee recommendations (modified as we recommend). While new and more stringent remedies could be developed, that is not a course which either the Minister or the Service has urged us to follow. There are circumstances where the public interest compels action to suppress publication but they are, or should be, rare. We would not recommend the introduction of a new remedy in the absence of compelling reasons for doing so.

---

352 See, for example, Commissioner for Railways v. Small (1938) 38 SR 564 at 575.
Chapter 13
Criminal Sanctions Against Publication

The existing provisions: Crimes Act ss.70 and 79

13.1 The provisions of Commonwealth criminal law applicable to disclosure of information about ASIS operations, sources and methods are ss.70 and 79 of the Crimes Act 1914 (Cth).353 These are general provisions on the disclosure of government information. Section 70 of the Crimes Act creates a general offence of disclosure by Commonwealth officers, or former Commonwealth officers, of any information which they have a duty not to disclose. It provides:

70(1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he is authorised to publish or communicate it, any fact or document which comes to his knowledge, or into his possession, by virtue of his being a Commonwealth officer, and which it his duty not to disclose, shall be guilty of an offence.

(2) A person who, having been a Commonwealth officer, publishes or communicates, without lawful authority or excuse (proof whereof shall lie upon him), any fact or document which came to his knowledge, or into his possession, by virtue of having been a Commonwealth officer, and which at the time he ceased to be a Commonwealth officer, it was his duty not to disclose, shall be guilty of an offence.

The penalty for an offence against section 70 is two years imprisonment.

13.2 Section 79 similarly relies on the notion of a ‘duty to treat as secret’. The relevant provisions are as follows:

353 This chapter draws upon a report prepared by the Attorney-General's Department in October 1993 entitled The protection of official information (Exhibit 14.1). Referred to in this chapter as the Attorney-General's Department response, it was part of a Government response to the recommendations contained in the final report of the Gibbs Committee Review of Commonwealth Criminal Law (Exhibit 14.4).
79(l) For the purposes of this section, ... information is prescribed information in relation to a person if the person has it in his possession or control and: ...
(b) it has been entrusted to the person by a Commonwealth officer or a person holding office under the Queen or he has made or obtained it owing to his position as a person:
(i) who is or has been a Commonwealth officer;
(ii) who holds or has held office under the Queen;
(iii) who holds or has held a contract made on behalf of the Queen or the Commonwealth; ...
(v) acting with the permission of a Minister;
and, by reason of its nature or the circumstances under which it was entrusted to him or it was made or obtained by him or for any other reason, it is his duty to treat it as secret; ...

(2) If a person for a purpose intended to be prejudicial to the safety or defence of the Commonwealth or a part of the Queen's dominions:
(a) communicates ... prescribed information to a person other than:
(i) a person to whom he is authorised to communicate it; or
(ii) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his duty to communicate it;
 or permits a person, other than a person referred to in sub-paragraph (i) or (ii) to have access to it; ... he shall be guilty of an indictable offence.

The penalty for an offence against s.79(2) is imprisonment for seven years.

13.3 Disclosure by an ASIS officer, or former officer, of information about ASIS activities would seem to fall squarely within these provisions, subject in the case of s.79 to proof of purpose. The general duty imposed on public servants by regulation 35 of the Public Service Regulations (not to disclose any information except in the course of official duty) does not apply to ASIS officers. The existence of a duty on the part of an ASIS officer – both during and after employment with ASIS – not to disclose ASIS information is nevertheless readily apparent from the terms of the secrecy agreement, which forms part of the employment contract between each officer and the Director-General and from the secrecy acknowledgment signed by an officer on departure from ASIS.

Criticisms of the existing provisions

13.4 The provisions of sections 70 and 79 were reviewed by the Gibbs Committee on Review of Commonwealth Criminal Law (the Gibbs Committee). This was the first time there had been a thoroughgoing review of the provisions,
although they had been much criticised. In 1979 the Senate Standing Committee on Constitutional and Legal Affairs recommended that urgent consideration be given to reforming section 70 ‘so as to limit the categories of information that it is an offence to disclose and to establish procedural safeguards for any person who may face prosecution under that section’. In 1983 the Human Rights Commission suggested that section 70 could be inconsistent with Article 19 of the International Covenant on Civil and Political Rights, which protects the right to freedom of expression. In accordance with that Covenant, it recommended that the operation of section 70 be limited to restrictions which were necessary for the respect of the rights and reputations of others, and for the protection of national security, public order or public health or morals.\textsuperscript{356}

13.5 The Gibbs Committee identified three basic principles which, the Committee believed, would be generally accepted in any consideration of restrictions on disclosure of official information. The first was that ‘it is unacceptable in our democratic society that there should be a restraint on the publication of information relating to Government when the only vice of that information is that it enables the public to discuss, review, and criticize Government action’ (Commonwealth v. John Fairfax & Sons Ltd (1980) 147 CLR 39, 52 per Mason J). The second was that it is undesirable that the sanctions and machinery of the criminal law should be applied in relation to the unauthorised disclosure of all forms of official information and this should be avoided if possible. Thirdly, there are some descriptions of official information that should be protected by the criminal law from unauthorised disclosure.\textsuperscript{357} The Committee also accepted a broader principle that:

\begin{quote}
in a modern democratic society, the public should have access to as much information as to the workings and activities of Government and its servants as is compatible with the effective functioning of that Government.\textsuperscript{358}
\end{quote}

13.6 Applying these principles, the Gibbs Committee criticised the breadth of the existing provisions:

The combined effect of sections 70 and 79 is that the unauthorised disclosure of most information held by the Commonwealth Government and its agencies is subject to the sanctions of the criminal law. No distinction is drawn for the purposes of these provisions between information the disclosure of which may

\textsuperscript{356} Exhibit 14.4, paragraph 26.1.
\textsuperscript{357} Ibid., paragraph 31.1.
\textsuperscript{358} Ibid., paragraph 31.2.
cause real harm to the public interest and information the disclosure of which may cause no harm whatsoever to the public interest.359

The Committee concluded that 'the catch-all provisions of existing law are wrong in principle and additionally ... are seriously defective from the point of view of effective law enforcement'.360

13.7 The ASIS perception is that the provisions are ineffective, both because of difficulties of proof and, associated with that to some extent, because of a reluctance on the part of Government to prosecute. The former Director-General, Mr Furner, described the Crimes Act provisions as 'this terrible Damoclean sword ... which never seems to leave its silken thread'.361 He referred to 'an inbred reluctance to invoke the Crimes Act in cases of apparent threats to national security'.362 The explanation for this, according to the Service, is that:

leaving aside the politics of Crimes Act prosecutions, the relevant provisions of that statute are insufficiently distinct to allow for rigour and confidence in mounting a prosecution against those who make unauthorised disclosures about ASIS.363

13.8 Historically, it has been rare for governments to resort to the Crimes Act to punish unauthorised disclosures. Despite the apparent breadth of sections 70 and 79, there have been very few reported prosecutions under those provisions.364 One of the obstacles to prosecution has been the apparent belief that it was necessary to prove intent to cause harm on the part of the officer making the disclosure. The Minister said he had been advised on a number of occasions about the difficulties of establishing the necessary degree of intent in criminal prosecutions under the Crimes Act.365

13.9 The element of intent only arises, however, under s.79. Section 70 contains no such requirement. Clearly, if the prosecution is required to prove that the person making the disclosure did so 'for a purpose intended to be prejudicial to the safety or defence of the Commonwealth', this presents problems of proof. For this reason, it would be expected that the first recourse in any consideration of prosecution would be to s.70.

359 Ibid., paragraph 25.12.
360 Ibid., paragraph 31.4.
361 T*42*.
362 T2765.
363 Exhibit 20.1.17, paragraphs 17 & 18.
364 Exhibit 14.1, paragraph 2.10. See also the cases there cited.
365 T2533.
13.10 The Minister identified, as a further inhibition on prosecution, the risk that prosecution action will prompt further publication:

Free speech, penalising people, jailing, fining people for merely exercising a whistleblowing function, and so the argument will go. It runs the risk of flushing out further publications by people who are discontented with this.\(^{366}\)

This consideration will exist whatever legislative regime is in place, and is likely to become more significant in the event of any strengthening of criminal sanctions.

**The Gibbs Committee recommendations**

13.11 The central recommendation of the Gibbs Committee was that criminal sanctions should apply only if the information discussed fell into one of a number of specific categories. These categories should be ‘no more widely stated than is strictly required for the effective functioning of Government’.\(^{367}\) The relevant category for present purposes was ‘information relating to security or intelligence’. The Committee recommended that disclosure of such information by an officer or ex-officer of one of the intelligence and security services should be an offence without the requirement to prove damage. Publication by any other person would not be an offence unless it were proved that the disclosure was damaging, that is, unless the disclosure:

(a) caused damage to the work of, or of any part of, the security and intelligence services; or

(b) was of information that was such that its unauthorised disclosure would have been likely to cause such damage.\(^{368}\)

13.12 The Committee’s recommendation that damage should not be an element of the offence where the disclosure was made by an officer or ex-officer was justified in the following terms:

Undoubtedly, a member of the intelligence or security services stands in a special position and it is not unreasonable, in the opinion of the Review Committee, that he or she should be subject to a lifelong duty of secrecy as regards information obtained by virtue of his or her position. Subject to the very important proviso that satisfactory procedures are established by which complaints or allegations by such a person as to illegality, misconduct or

---

366 T2533.
367 Exhibit 14.4, paragraph 31.5.
368 Draft Bill, sub-clause 85DB(3).
improper activities of those services or persons employed in them are received, investigated and dealt with ... the Review Committee is satisfied that disclosures by such persons should be prohibited by criminal sanctions without proof of harm. 369

13.13 The Attorney-General's Department response supported this conclusion:

If it were necessary to prove that the disclosure of information by a member of the intelligence or security services had caused damage, it may then be necessary to either confirm the validity of the information, or to reveal further secret information. Unauthorised disclosures by such individuals are also harmful to the public interest because they diminish confidence in the ability of the service to carry out its duties properly. 370

13.14 The category of protected information was recommended to extend to statements made by officers of the services which purported to be of information relating to the services, or were intended to be taken as such. 371 This was in recognition that, given the constraints of the conventional 'neither confirm nor deny' policy, disclosures of misinformation by an officer can also be harmful.

13.15 In our view, the essence of the Gibbs Committee's recommendations – the replacement of wide provisions of general application with offences referable to disclosure of defined categories of information – is desirable both in principle and in practice, and should be implemented. Some of the specific recommendations, however, require closer examination.

A whistleblower scheme

13.16 The recommendation that proof of damage not be required in a case of a disclosure by an officer or former officer was subject to the proviso that there be satisfactory procedures for complaints or allegations to be investigated and dealt with. To this end, the Committee recommended that a scheme be established by law for 'whistle-blowers'. The proposed scheme would apply to a Commonwealth officer who believed that he/she had evidence of illegality, gross mismanagement, gross waste of funds or 'a substantial or specific danger to public health or safety'. 372 Under the scheme, an ASIS officer in possession of such information could, without risk of criminal liability, disclose it either to a

---

370 Exhibit 14.1, paragraph 4.27.
371 Exhibit 14.4, Part VI, paragraph 85DB(1)(d).
372 Exhibit 14.4, paragraph 32.35 and paragraph 32.50.
designated complaints officer of the Service or to IGIS. The Attorney-General’s Department response supported these recommendations.\(^{373}\)

13.17 We have no hesitation in supporting the principle that there should be protection from criminal liability and from disciplinary sanctions for disclosures of this special character. Such a scheme should be established regardless of whether, or in what way, the Crimes Act may be amended. As the Gibbs Committee recommended, the IGIS Act should be amended to empower IGIS to inquire into allegations of the requisite kind against any of the intelligence and security agencies,\(^{374}\) and to confer immunity from prosecution or disciplinary action on a person disclosing information to IGIS in support of such allegations.\(^{375}\) Allegations of this special character are to be clearly distinguished from employment-related grievances which at present are within IGIS’s jurisdiction\(^{376}\) but which we recommend in Chapter 14 should be transferred to the jurisdiction of the Administrative Appeals Tribunal. If this change is implemented, it will need to be clearly stated that once a complainant has invoked the Tribunal’s jurisdiction, the jurisdiction of IGIS in relation to the subject-matter of the complaint is permanently excluded.

13.18 We have not seen it as our function to investigate possible schemes for whistleblower protection. The recommendations of the Gibbs Committee took account of relevant statute law in the United States and a variety of Australian proposals.\(^{377}\) The Senate subsequently established a Select Committee on Public Interest Whistleblowing, which reported in August 1994. It is sufficient for us to say that we regard the scheme proposed by the Gibbs Committee as appropriate, with one significant qualification. The protection which the scheme affords should, in our view, be extended to a disclosure by a former officer, or by a source or former source, of one of the services who believes that he/she has evidence of the requisite kind.

---

\(^{373}\) Exhibit 14.1, paragraphs 6.8-6.19.

\(^{374}\) Exhibit 14.4, paragraph 32.12. IGIS already has power under s.8(2)(a) of the IGIS Act to inquire into complaints regarding ASIS’s compliance with Australian law and with ministerial guidelines.

\(^{375}\) cf. the existing immunity from civil action - IGIS Act s.33(2).

\(^{376}\) IGIS Act, ss.8(6), 11(5).

Proof of damage

13.19 Like the Gibbs Committee, we see the task of defining appropriate criminal provisions in this area as one of finding the right balance between competing public interests, between protecting intelligence-gathering activities on the one hand and maximising disclosure of information about the workings of government on the other. In failing to distinguish between damaging and non-damaging disclosures, the existing Crimes Act provisions are too heavily weighted against disclosure.

13.20 Clearly, however, officers and former officers of the intelligence and security services are in a rather special position. The question is whether the character of their work, and the sensitive nature of the information with which they are entrusted during that employment, justifies criminal liability without proof of damage when that information is disclosed. We have referred already to the considerations advanced in support of this Gibbs recommendation, namely:

(a) the officer's lifelong duty of secrecy;
(b) the loss of public confidence in the Service if an officer or former officer makes disclosures; and
(c) the likely need to disclose secret information in court in order to prove damage.

13.21 As to the first of these, the obligation of secrecy is imposed on an ASIS officer as a matter of civil law, by virtue of his/her contract with the Service and the equitable obligation of confidence. We accept that it is a lifelong duty, the observance of which is essential to the effectiveness of what ASIS does, but it is a very serious thing for any breach of that civil law obligation to attract a criminal penalty regardless of whether damage is caused – for example, if the information disclosed is of an administrative kind entirely lacking in operational significance. We have not ignored the argument that any breach of the secrecy obligation has a tendency to damage ASIS because of its effects on internal morale and reputation of ASIS with its liaison partners. But in the end we are not persuaded that the existence of the duty of secrecy by itself justifies a criminal sanction for any breach.

13.22 In our view, the balance of interest favours taking the risk of harm being done simply because an officer is making a disclosure, rather than the detriment which would flow from the creation of criminal liability for an officer.
who discloses problems with Service administration which are not in themselves damaging.

13.23 As to the second consideration, it is impossible to assess whether public confidence is affected by the mere fact of a disclosure, apart altogether from the impact of the information disclosed. Assuming that changes in public confidence are capable of detection, we would doubt whether individual disclosures – especially harmless ones – would produce any measurable change. This is not, in our view, an argument which would justify the step of imposing criminal liability without proof of damage.

13.24 The problem of disclosing secret information in court in order to prove damage is more significant. But this problem will arise in other prosecutions concerning intelligence-related information – whenever the defendant is someone other than an officer or former officer – and it is therefore not by itself a ground for treating officers and former officers differently. In any case, a solution is to be found in taking the necessary evidence in camera, an approach which ASIS informed the Gibbs Committee it would generally be prepared to accept.378 Such a procedure would necessarily involve the disclosure of sensitive information to the jury, but risk of any wider disclosure would be minimised by the combination of the judge’s order closing the court and prohibiting publication of the evidence – breach of which would be a contempt of court if not a criminal offence in itself379 – and the prohibition on secondary disclosures (see paragraphs 13.43-51), the effect of which could readily be explained to the jury.

13.25 An alternative solution, adopted in New Zealand, would be to remove the question of damage from the jury. Under the Crimes Act 1961 (NZ), the question whether a communication was likely to prejudice the security or defence of New Zealand is reserved for determination by the judge, who may receive evidence on the question in addition to that heard by the jury. We agree with the view of the Gibbs Committee that the removal of such a significant element of the case against an accused from determination by the jury should not be considered except as a last resort.380

13.26 Our chief concern is with the extent of the criminal liability which the Gibbs proposal would create. It would render an ASIS officer or former officer criminally liable – without proof of damage – for the disclosure of ‘any

---

378 Exhibit 14.4, paragraph 30.13.
379 Crimes Act s.85B.
information relating to security or intelligence'. Thus, there would be liability not only for disclosures of sensitive operational information, which are damaging to the work of the Service, but also for disclosures of an innocuous kind, for example concerned with administrative or management issues.

13.27 The chain of events which started with the *Four Corners* program demonstrates that judgments about what is and is not damaging are often complex. The disclosure of a piece of information, which may not have appeared to be damaging at the time, may be followed by (and may itself lead to) other disclosures, the cumulative effect of which is damaging. Additionally, the 'mosaic' theory advanced by the Service means that any piece of information about the Service is, in the wrong hands, potentially damaging. This is, however, a difficult argument to evaluate and, taken to its extreme, it would prevent disclosure of any information about ASIS.

13.28 As we said in Chapter 11, disclosures of various types can be damaging to ASIS, depending on the circumstances. We accept that disclosures about operational matters will often – but not always – be damaging to the work of ASIS. Disclosures about management matters may or may not be damaging, depending on their content. But if no damage can be demonstrated as flowing from a particular disclosure, does that nevertheless justify subjecting the officer or former officer to criminal penalty? Such a result might offend against the first of the three principles identified and adopted by the Gibbs Committee (see paragraph 13.5 above).

13.29 In our view, the solution lies in confining liability without proof of damage to those disclosures which, by their nature, are most likely to cause damage. This could be done by defining certain narrower categories within the general category of 'information relating to security or intelligence'. This possibility was explored by the Gibbs Committee, in the context of disclosures by persons other than officers or former officers of the intelligence and security services, whose guilt would depend on some form of damage.\(^\text{381}\) The ASIS submission to the Committee on this point said:

A list of "specific forms of information relating to ... intelligence" presents some difficulty for ASIS because such a list could itself disclose classified information. An unclassified list could include "any information purportedly:
(a) identifying current or former officers, sources or contacts of ASIS;
(b) identifying current or former places of operation of ASIS; or

---

(c) describing specific intelligence operations of ASIS by such persons and/or at such places".382

13.30 In the event, the Gibbs Committee did not proceed with this approach,383 but recommended instead that proof of damage be required in relation to all non-officer disclosures. Whilst agreeing with that conclusion, we consider that the approach can be usefully adapted to the different purpose of narrowing the scope of liability-without-damage for officers and former officers.

13.31 The ASIS list set out above is a useful starting-point. It concentrates on those categories of information which we have identified as most obviously in need of protection because of the damage which their disclosure is likely to cause.384 It is no coincidence that the categories in this list are similar to those in the ASIS D Notice. They also reflect what the Minister has said is the focus of the Government's concern:

The Government's concern is not and never has been with the publication of material about the Australian Secret Intelligence Service (ASIS) as such. Much more specifically, the concern has been about the publication of information which identifies former or current officers of ASIS or their contacts, which identifies current or former places of overseas operation of ASIS, or which falsely describes specific intelligence activities involving those officers or those places.385

13.32 The first of the categories proposed by ASIS – the identification of individuals – is addressed later in this chapter, where we recommend a specific provision in the legislation for ASIS, corresponding to a provision in the ASIO Act. The second and third categories focus on specific operational information. They require some modification. In our view, it would be appropriate that any disclosure by a serving or former ASIS officer of a current or projected operation or of current or projected ASIS operational locations should constitute an offence without proof of damage. The probability of damage in such cases is high, as reflected in the equivalent D Notice provisions. On the other hand, as we have discussed in Chapter 11, disclosures about past operations or past locations may or may not be damaging, depending on the circumstances. In those cases, proof of damage should be required.

13.33 It follows that we do not agree with the Gibbs Committee that proof of damage should be dispensed with in any case where the information is disclosed

382 Ibid, paragraph 30.16.
383 Ibid, paragraph 31.32.
384 See chapter 11.
385 Senate Hansard, 23 November 1988, p.2613, at Exhibit 12.1, tab 1.
by an officer or former officer. Instead we recommend that proof of damage be an element of the offence arising from disclosure of information relating to intelligence and security, except where the person making the disclosure is an officer or former officer and the information disclosed:

(a) identifies or purports to identify current or projected places of operation of ASIS; or

(b) describes or purports to describe current or projected intelligence operations of ASIS.

Where the exception applied, the offence would be committed when information of the requisite kind – including false information – was disclosed. No proof of damage would be necessary. Nor would it be when the disclosure involved the identification of current or former officers or sources.

13.34 At the same time, we recommend that the proposed definition of 'damage' be widened, to include a case where an individual (e.g. a source in a foreign country) was put at risk by the disclosure, even though it might not be possible to demonstrate that this had had any direct adverse effect on the work of the Service. This expansion of the definition will ensure that the scope of the criminal provisions corresponds with the nature of the interests to be protected. As we have seen, those interests are individual as well as operational.

**Defence of prior publication**

13.35 The Gibbs Committee recommended that it should be a defence in a prosecution for unauthorised disclosure for the defendant to satisfy the court that:

(a) the information in question had previously been published;

(b) the defendant had reasonable grounds to believe that the second publication was not damaging; and

(c) the defendant was not in any way involved in the prior publication.\(^{386}\)

Importantly for present purposes, however, the Committee recommended against this defence being available in relation to an unauthorised disclosure of intelligence and security information by a member or former member of the

\(^{386}\) Exhibit 14.4, paragraph 31.35.
intelligence and security services, if the information disclosed had been available to the person because of his or her position as a member of such a service. The denial of this defence was said to be justified by 'the very special position' of a member of such a service. The Attorney-General's Department response endorsed the Committee's recommendations.\footnote{Exhibit 14.1, paragraphs 4.50, 4.52.}

13.36 Once again, we have come to a different view. As we have already indicated, we do not accept that the position of members or former members of ASIS is such that they should automatically be placed in a less advantageous position than other persons making unauthorised disclosures. In our view, the defence of prior publication should be available to a member or former member in any case where damage is an element of the offence, that is, where the information disclosed falls outside the categories proposed in paragraph 13.33. In such a case, the elements of the defence, as defined by the Gibbs Committee, mean that it will only be available if it was reasonable for the officer to believe that no damage to the work of ASIS would be caused and where the officer was innocent of involvement in the original publication. If the officer is able to satisfy those requirements, we see no reason in principle why the defence should not be available.

**Defence of public interest**

13.37 In an action for breach of confidence brought against a person who has made an unauthorised disclosure of information, it is a defence if the defendant can establish that the disclosure was required in the public interest.\footnote{See Attorney-General v. Observer Limited [1991] A.C. 109 at 259, 264 and 282; Commonwealth v. John Fairfax & Sons Limited (1980) 147 CLR 39 at 56-7; A v. Hayden (1984) 156 CLR 532 at 544-6.} The Gibbs Committee doubted whether an equivalent defence was available in a prosecution under either ss.70 or 79 of the Crimes Act, but, in view of its recommendations about whistleblower protection, did not consider it necessary to make provision for a defence of public interest specifically in that form.\footnote{Exhibit 14.4, paragraph 32.2.} The Attorney-General's Department response endorsed the Committee's view, arguing that:

> There should not be a general public interest defence in the criminal law on protecting official information. It is acknowledged that persons who illegally disclose information may be motivated by a perceived benefit to the public. Yet this will be true for a number of crimes. It is not appropriate to make the application of the criminal law depend upon the ultimate motives of the offender. Rather, it should be based upon the nature of the act and the damage
which it may cause. Questions of motive should be relevant only with respect to sentencing.\textsuperscript{390}

13.38 The Department’s comment appears to misunderstand the nature of the defence under consideration. If the defence were dependent on a wholly subjective test – whether the defendant honestly believed that publication was necessary in the public interest – it would have a far wider operation than could reasonably be justified. In civil law, the defence is not made out unless the defendant establishes the facts on which the allegations (of criminal activity or misconduct) are based, sufficient to satisfy the court that in all the circumstances it was in the public interest for the defendant to make the disclosure of confidential information about which the plaintiff complains.\textsuperscript{391} Disclosure must be required in the public interest, not merely believed to be required.\textsuperscript{392}

13.39 Here again, our conclusions diverge from those of the Committee. We have already indicated our support for the Committee’s recommendations on whistleblower protection. But we do not regard the establishment of such a scheme as concluding the question about a public interest defence. On the contrary, allowance must be made for the possibility that a person, having information of the kind to which the whistleblower scheme will apply, concerning for example serious illegality or gross mismanagement, will disclose that information publicly. Such disclosure might be made in ignorance of the existence of the whistleblower scheme; it might be made by a person who was concerned that an investigation by the Ombudsman or (in the case of ASIS) the Inspector-General would not be sufficiently rigorous; or it might reflect dissatisfaction with an investigation which the Ombudsman or IGIS had already carried out.

13.40 We think that a defendant, in those circumstances, should be entitled to call in aid a defence of public interest. We do not consider that the establishment of such a defence would be likely to encourage a rash of disclosures since, ex hypothesi, the person making the disclosure will be running the risk of conviction. We recommend that it be a defence to a charge under the new provisions if:

(a) the defendant believed that the disclosure to which the charge relates was necessary in the public interest; and

\textsuperscript{390} Exhibit 14.1, paragraph 6.5.
\textsuperscript{391} \textit{A v. Hayden} (supra) at 546, 545.
\textsuperscript{392} \textit{Attorney-General v. Observer Limited} (supra) at 282.
(b) there were reasonable grounds for the defendant to hold that belief at the time the disclosure was made.

The defendant would bear the onus of establishing both these elements on the balance of probabilities. The requirement to show reasonable grounds ensures that liability is not dependent upon 'the ultimate motives of the offender'.

13.41 Failure to report the matter in question to the whistleblower agency in the first place should not be a bar to reliance on this defence, although we would expect that recourse to the agency would be the first step in most cases. Not only is public disclosure generally seen as a last resort, but a defendant who had not given the whistleblower agency an opportunity to investigate before the matter was raised publicly would find it much more difficult to establish in court that it was necessary in the public interest to make a public disclosure.

13.42 We deal next with the issue of secondary disclosure. If, contrary to the recommendation we there make, the offence recommended by the Gibbs Committee is created, the defence of public interest should apply to it. The offence can be committed by persons other than Commonwealth officers and contractors, and in those circumstances the existence of the whistleblower scheme is irrelevant.

**Secondary disclosures**

13.43 'Secondary' disclosures are made by those who gain access to government information as a result of an unlawful 'primary' disclosure. Section 70 of the Crimes Act does not directly apply to secondary disclosures, such as where an officer or former officer has wrongly disclosed sensitive information to an individual who subsequently publishes it. The secondary publisher may be liable as an accessory to the primary offence. In this regard, Crimes Act s.5(1) provides:

5(1) Any person who aids, abets, counsels or procures, or by act or omission is in any way directly or indirectly knowingly concerned in, or party to, the commission of any offence against any law of the Commonwealth or a Territory, whether passed before or after the commencement of this Act, shall be deemed to have committed that offence and shall be punishable accordingly.

13.44 In certain circumstances, this provision could enable the prosecution of a person who came to an arrangement with a Commonwealth officer for that officer to disclose information unlawfully. For example, it could apply to a journalist who published information about ASIS, knowing that it had been communicated to him or her by an ASIS officer without authority. But a
subsequent recipient who published the illegally-disclosed information would escape liability, having had no involvement in the original offence. Moreover, in the absence of evidence as to which officer was responsible for the primary disclosure, it would be difficult to mount a successful prosecution of the third party, even where the third party had obtained the information by coming to an arrangement with a Commonwealth officer.

13.45 According to the Gibbs Committee, this represents a limitation on the operation of the law:

A prosecution of a subsequent publisher of [protected] information for breaches of sections 70, 79 or 5 of the Crimes Act will ordinarily not succeed without proof of the identity of the officer who made the disclosure, the channel of communication to that publisher or at least the circumstances under which the publisher received the information in question.\(^{393}\)

The Attorney-General's Department response commented:

This is unsatisfactory, if only because the application of the criminal law will be highly arbitrary. If, for example, a third party has acquired official information to which he or she should not have had access, and deliberately discloses that information in circumstances which he or she knows will cause damage to the public interest, prosecution may be avoided provided that the circumstances in which the third party acquired the information are unclear. However, if the circumstances of the primary disclosure can be established, then the third party would be liable. Indeed, under the current law he or she would be liable irrespective of the potential harm caused by the subsequent disclosure.\(^{394}\)

13.46 The Gibbs Committee recommended that Australian legislation should broadly follow s.S of the Official Secrets Act 1989 (UK) in creating an offence of secondary disclosure.\(^{395}\) The Committee recommended that the offence created should apply to a person who knows, or has reasonable grounds to believe, that the information in question:

(a) had been disclosed (whether to him/her or another) by a Commonwealth officer without authority or had been unlawfully obtained from such an officer; or

(b) had been entrusted to him/her in confidence by such officer on terms requiring it to be held in confidence; or

\(^{393}\) Exhibit 14.4, paragraph 25.42.

\(^{394}\) Exhibit 14.1, paragraph 5.6.

\(^{395}\) Exhibit 14.4, paragraphs 31.41-2.
had been disclosed (whether to him/her or another) without lawful authority by a person to whom it had been entrusted in confidence.

The Committee further recommended that, in addition to these matters, the prosecution would be required to prove that:

(d) the defendant disclosed the information without authority;

(e) the disclosure was damaging; and

(f) the defendant knew, or had reasonable cause to believe, that it was damaging.\(^{396}\)

13.47 In supporting this recommendation, the Attorney-General's Department response commented:

It must be emphasised that the secondary disclosure provision will only cover official information which it is important to protect. This means that criminal sanctions will only be imposed on third parties in circumstances where they have disclosed information which is genuinely secret. Further, they will only apply where the third party knows, or has reasonable grounds to believe, that the information is secret and that its disclosure would cause the relevant form of damage.\(^{397}\)

13.48 The proposed provision would cover the case of disclosure of information by an ASIS officer (but not a former officer) to a journalist where the journalist was well aware that this was an unauthorised disclosure. Criminal liability would depend on whether the disclosure was in fact damaging and whether the journalist knew, or had reasonable cause to believe, that it was damaging.

13.49 The policy question is whether, if the voluntary D Notice system is revitalised as we recommend, a criminal offence of secondary disclosure is also necessary. The contents of some media reporting on ASIS throughout 1993 and 1994 clearly fell within the current D Notice. Its publication represented a failure of the D Notice system. In part, this was a function of ignorance of the system\(^{398}\) and in part, according to the Director-General,\(^{399}\) it was a function of journalistic attitude. It could certainly be argued that some of this reporting was damaging

---

\(^{396}\) Ibid., paragraph 31.44. The Committee's draft Bill did not include an express requirement that it be a damaging disclosure - see clause 85DF cf. clause 85DB(2).

\(^{397}\) Exhibit 14.1, paragraph 5.9.

\(^{398}\) T*690*, *710*.

\(^{399}\) T*982*.
to the work of ASIS and, further, that the journalists had reasonable cause to believe that it was damaging. Assuming that the sources of the information were, to the journalists' knowledge, ASIS officers, the offence would be made out if – but only if – ASIS could establish the fact of damage and that such damage could reasonably have been anticipated.

13.50 Standing alone, this draft provision imposes what we regard as appropriate limits on the exposure of a journalist, or other secondary publisher, to criminal liability. But the provision cannot be considered in isolation. Because in its practical operation it will apply – or be perceived as applying – most often to journalists, it must be considered in the context of our recommendations for the reactivation of the D Notice system and a review of the ASIS D Notice.

13.51 Although the existing s.5(1) potentially applies to journalists, the proposed new secondary disclosure offence is both an extension and a refinement of the present law. In particular, it would apply to a journalist who had no involvement in the primary disclosure. If enacted it would be seen by the media – with some justification, in our view – as effectively replacing the voluntary D Notice system with a system based on criminal sanctions. Media witnesses made clear their opposition to such a course. If this offence were created it would, in all likelihood, destroy the voluntary system. Accordingly, we recommend that the Government not proceed with the proposed offence of secondary disclosure at least until it has been established beyond reasonable doubt that the D Notice system is incapable of being made effective.

Identification of individuals: a mirror provision to ASIO Act s.92?

13.52 Section 92 of the ASIO Act 1979 prohibits the publication of:

any matter stating, or from which it could reasonably be inferred, that a person having a particular name or otherwise identified, or a person residing at a particular address, is an officer ... employee or agent of the Organization or is in any way connected with such an officer, employee or agent or, subject to subsection (1)(B), is a former officer ... employee or agent of the Organization or is in any way connected with such a former officer, employee or agent.  

400 See for example the submissions from the Age, 18 November 1994 (Exhibit 12.5.6); and from the Australian, 29 November 1994; (Exhibit 12.10.5).

401 ASIO Act, s.92.
The prohibition does not apply in relation to action taken in respect of a former officer, employee or agent who has consented in writing to the taking of that action or who has caused or permitted the publication to occur.402

13.53 ASIO has found s.92 to be an effective deterrent, although it does not offer a universal guarantee.403 ASIO's conclusion that it is a deterrent is based principally on the fact that there has been very little publication.404 On one occasion ASIO drew the attention of Four Corners to the provision, and its terms were complied with in the broadcast program.405 The author of a recent book on ASIO, however, advised ASIO that he was identifying a large number of officers and former officers, knowing that he was infringing s.92.406

13.54 ASIS has submitted that a like prohibition should apply to the identification of ASIS officers and sources.407 This has been a prime concern of the Service from the beginning of the Inquiry, and a key factor in its decision to seek legislative coverage.408

13.55 The proposal was taken up with media representatives during their evidence before the Commission. A number of media representatives were firmly opposed to the proposal. Mr Kohler and Mr Bartlett of the Age said they considered the D Notice system to be sufficient to prevent disclosure. They argued that there had been few, if any, instances of the names of ASIS officers being revealed and that any limitations in D Notices did not flow from the system itself but from the Government's failure to disseminate information about it.409 Mr Hill from the ABC told the Commission that the ABC would 'oppose any further restriction on the reporting of ASIS, whatever form that may take'.410 Other media witnesses were more receptive to the suggestion. Mr Grant from Channel Seven thought it would be acceptable.411 Mr Harvey of Channel Nine generally favoured a voluntary rather than a proscriptive approach to the protection of ASIS security, but believed that a ban on the disclosure of the

402 Ibid., s.92(1B)
403 Exhibit 34.1.2, p.2.
404 T*317*.
405 T*318.9*.
406 T*318*.
407 Exhibit 20.1.17, paragraph 124; T*958*.
408 See paragraph 3.4.
409 T*840*.
410 T*614*.
411 T*756*.
identity of ASIS officers would make little difference to his organisation 'in practical terms' because it did so little reportage on ASIS.412

13.56 An equivalent provision to s.92 of the ASIO Act would enhance the protection afforded to present and former officers and sources against disclosure of their identities. It would also strengthen the assurance which the Service can give to sources about such protection. We are satisfied that the importance of such protection to the effective functioning of the Service, and to the security of the individuals concerned, is sufficient to justify criminal liability without proof of damage should a disclosure occur. It is, moreover, difficult to see any basis for denying to ASIS officers and sources the protection afforded to their ASIO counterparts. We recommend accordingly.

Secrecy provisions in ASIS legislation

13.57 Elsewhere in this report we recommend the introduction of legislation for ASIS. We believe it should contain specific offences concerning the communication of information by ASIS officers or otherwise relating to ASIS. We envisage that, if and when the Crimes Act is amended along the lines recommended, that part of the ASIS legislation would be repealed. It is, in our view, desirable that there be a single code dealing with unauthorised disclosures and that, to the extent that special provisions are necessary in relation to the intelligence and security services, those provisions should be included in that code, rather than in separate legislation.

412 T*673*. 
Chapter 14

Complaints and Grievances: External Review

Inquiries into complaints and grievances

14.1 When Mr Justice Hope proposed that a new office of Inspector-General be established, he apparently expected that such complaints as were received would originate primarily from the public. He propounded a model of inquiry into complaints based on informal fact-gathering and rejected the model of a quasi-judicial tribunal:

Often ... an aggrieved person may believe, but will not know, that ASIO has acted in a particular way. The submission by the Australian Labor Party noted:

... fishing expeditions into ASIO's activities should not be permitted: nor should a person be able, by virtue of some review Tribunal, to, in effect, deliver a requisition compelling ASIO to disclose whether he was or was not a 'target'.

These considerations suggest that any inquiry should be more like those carried out in other areas by an Ombudsman ... In this area a quasi-judicial inquiry of the kind that the Security Appeals Tribunal is well suited to carry out seems inappropriate. The emphasis will be on ascertaining the facts and circumstances by direct inquiry rather than on calling on ASIO to justify an acknowledged action or opinion on its part.¹⁴¹³

14.2 This reasoning applies more readily to complaints from the public than to employee grievances. An aggrieved staff member could be expected to seek exactly what Mr Justice Hope had considered unlikely – that the agency be required to justify an action it had taken. The original conception was that there would be other avenues for review of the grievances of staff and that IGIS should normally respond to staff grievances by suggesting that a staff member should pursue the grievance procedure within the organisation. The Inspector-General

¹⁴¹³ Exhibit 2.2.4, paragraph 17.72 (RCASIA, Report on ASIO, AGPS, 1984).
would not ordinarily inquire into particular cases but would be available to ensure that the procedures operated as intended, and fairly.414

14.3 Our discussion in this chapter maintains the distinction between public complaints and employee grievances. We describe as a ‘grievance’ a matter raised by an employee or former employee of an agency which is related to his or her employment. We use the term ‘complaint’ for any other matter raised with IGIS concerning the activities of an agency.

The power to inquire

14.4 IGIS may inquire into complaints about:

(a) compliance by ASIS with Australian law;
(b) its compliance with directions or guidelines given by the Minister;
(c) the propriety of particular activities of ASIS; and
(d) an act or practice of ASIS referred to IGIS by the Human Rights and Equal Opportunity Commission.415

IGIS also has the power to inquire into a grievance of an employee of ASIO or ASIS which ‘directly relates’ to the promotion, termination of appointment, discipline or remuneration of the employee or otherwise to the employment.416

14.5 The power of inquiry is subject to important qualifications. First, the Minister’s approval is required before IGIS can inquire into a matter which occurred outside Australia or before the commencement of the Act on 1 February 1987.417 Secondly, a ministerial request is necessary before IGIS can inquire into matters which do not affect Australians or involve possible breaches of Australian law.418

14.6 The power to inquire into grievances is subject to additional restrictions. Under the Act, IGIS is prevented from inquiring into the grievance of an employee of either agency if satisfied that:

---

414 Ibid., paragraph 14.73.
415 s.8(2)(a).
416 s.8(6).
417 s.8(8).
418 s.8(4). This restriction applies to inquiries into complaints but not grievances.
(a) the procedures of the agency relating to redress of grievances are adequate and effective;

(b) the aggrieved employee has not pursued those procedures as far as practicable; or

(c) the matter to which the grievance relates is not of sufficient seriousness or sensitivity to justify an inquiry.419

14.7 IGIS also has a discretion not to inquire into a complaint, or to discontinue an inquiry, if satisfied that:

(a) the complainant became aware of the action more than 12 months before the complaint was made;

(b) the complaint is frivolous, or vexatious, or was not made in good faith; or

(c) having regard to all the circumstances of the case, an inquiry, or continuation of an inquiry, is not warranted.

The value of inquiries into complaints and grievances

14.8 The value of IGIS's function of investigating complaints lies in the protection it offers to the rights of Australians and in the contribution it makes to the accountability of ASIS. The investigation of public complaints about ASIS by an independent statutory officer contributes to accountability by increasing the likelihood that any aspect of ASIS's activities which should be investigated will come to attention and be dealt with. In addition, the inquiries provide IGIS with an insight into the operations of ASIS and an 'information base'420 which enhance the quality of the monitoring undertaken as part of IGIS's broader role of independent oversight.

14.9 Inquiries into staff grievances, on the other hand, will usually be directed to the way in which ASIS treats its employees, rather than to its performance of its primary functions. This generally narrows the contribution which such inquiries can make to the accountability of the Service or to IGIS's understanding of its operations. The external review of grievances is of more benefit to the individuals involved and to the agencies themselves than to broader public accountability.

419 s.11(5).
420 Exhibit 45.3.4, paragraph 74.4.
The experience of complaints and grievances

14.10 Inquiries into complaints and grievances have made greater demands on IGIS than was anticipated by Mr Justice Hope. These inquiries have come to occupy 75 to 80 per cent of the time of IGIS.\textsuperscript{421} Staff grievances have accounted for much of this effort. As a result, IGIS has not been able to carry out as much systematic monitoring of the intelligence and security agencies as we believe was intended and is desirable.

14.11 In the first four years of IGIS's existence, between four and six complaints from the public were lodged per year. The only issue of substance arising from them concerned the arrangements for security assessments.\textsuperscript{422} Six formal grievances from ASIO officers were also lodged in this period and there were several informal approaches by ASIO staff. These led to an inquiry of IGIS's own motion into ASIO's procedures for dealing with staff grievances.

14.12 Beginning in 1990-91, the annual rate of receipt of complaints from the public approximately trebled. Ten were received in 1990-91, 19 in 1991-92, 21 in 1992-93, and 12 in 1993-94. There was also an upsurge in grievances in 1990-91 and 1991-92. Eight were received in the first of these years (6 ASIO; 2 ASIS) and nine in the second (6 ASIO; 3 ASIS). The introduction in ASIO's grievance procedures in 1991 of a review panel with an external representative removed IGIS's jurisdiction over grievances of serving officers of the Organisation, although some continued to be lodged by ex-employees. Two additional grievances were received in 1992-93 (both ASIO) and four in 1993-94 (2 ASIO, 2 ASIS).

14.13 Mr Holdich's inquiries into complaints dealt with several issues of apparent significance. Matters he investigated in response to complaints included security assessment procedures (for the second time), ASIO's compliance with the Archives Act, community interviewing by ASIO, communication of information on individuals by ASIO, and whether ASIO had maintained a file on a member of Parliament, had knowledge of the Hilton and Yagoona bombings which should have been communicated to the police, or had interfered with arrangements for the publication of a book. According to the annual reports, IGIS was dealing, on average, with about four inquiries of this level of significance during each year between 1990-91 and 1993-94. Many of the inquiries took more than a year to complete.

\textsuperscript{421} T140.

14.14 Several grievances also appear to have involved substantial issues, and many were difficult to resolve. Of the six inquiries which Mr Holdich considered to have been the most difficult in the experience of his office, four were into grievances.\(^{423}\) On average, inquiries into grievances have taken about three times as long as those into complaints, a further indication of the relative difficulty of the two types of activity.

14.15 The great majority of complaints concerned ASIO. All but nine of the 83 received to the end of June 1994, including all the complaints before 1991-92, were about ASIO. None of IGIS's substantial inquiries about ASIS up to May 1994 had been into complaints.\(^{424}\) Only two complaints about another agency – DSD – have been discussed in the annual reports, both referred by the Human Rights and Equal Opportunity Commission and concerning alleged discriminatory employment practices.

14.16 The sudden increase in complaints and grievances in 1990-91 created a significant backlog in inquiry work which has increased in each year since. Until 1990, most inquiries had been completed in the year in which they began, but this changed dramatically in 1990-91. IGIS entered that year with three inquiries incomplete, received a further 20 complaints and grievances during the year, and reported on only seven. The backlog of inquiries at the beginning of July 1991 thus increased to 16. It was 17 a year later, had increased to 23 by July 1993, and to 28 by July 1994.\(^{425}\) The development of the backlog is illustrated in Figure 14.1.

14.17 The burgeoning arrears of work contributed to increasingly lengthy delays in the completion of inquiries. In the four years to 1989-90, 19 inquiries (63 per cent) were completed in 3 months or less and only five (17 per cent) took longer than six months to resolve. In the four years from 1990-91, 35 inquiries (44 per cent) were completed in three months or less, but 32 (40 per cent) took longer than six months. The average duration of completed inquiries into complaints in the first four-year period was 1.8 months; in the second period it was 4.7 months. For inquiries into grievances, the comparable averages were 12.3 months and 13.3 months respectively.

\(^{423}\) Exhibit 23.6.

\(^{424}\) T162-63; A complaint lodged by the wife of an ASIS officer was investigated jointly with the officer's grievance.

\(^{425}\) There was also one inquiry into a grievance which had been resolved in 1992-93, when the Attorney-General had agreed to support the payment of compensation to a former ASIO officer, but had been reopened in 1993-94 when the Minister for Finance refused to approve the necessary act-of-grace payment.
14.18 Considerably greater delays occurred in the inquiries that had not been completed by 30 June 1994. The average duration of the inquiries that made up the backlog at that date was 15.1 months for complaints and 20.6 months for grievances. As at 30 June 1994, there were 15 inquiries into complaints and grievances which were more than 12 months old. We consider delays of this order unacceptable.

[Figure 14.1]

Complaints and Grievances

14.19 It is important that we record the efforts made by Mr Holdich and his staff since the middle of 1994 to reduce the backlog of cases and to manage inquiries more efficiently. Of the 15 long-standing inquiries referred to in the previous paragraph, unfinished as at 30 June 1994, 7 have now been concluded. It is evident that inquiries which have been undertaken since that date are being conducted with considerably greater dispatch than in the past. This is apparently attributable to a number of factors. Case management procedures have been adopted, which provide for the setting of timetables and clearer definition of the key issues. A case manager has been appointed, whose task it is to assist the Inspector-General in planning case management strategies and to
monitor the progress of inquiries continuously. Some additional staffing assistance has also been provided. We commend the Inspector-General for the initiative he has shown in addressing the problem of delay.

14.20 Nevertheless, at the date of writing – nine months later – the size of the arrears is still such that a significant backlog of inquiry work will persist for some time unless special measures are taken to reduce it. The flow of work is not abating. During the first part of 1994-95, complaints from the public continued at about the same rate as in previous years, and several new inquiries into ASIS grievances were commenced. Mr Holdich told us that he would need another half dozen staff to eliminate the backlog quickly. This estimate is consistent with past completion rates. The staffing of the office at the end of June 1994 was six. In the concluding section of this chapter we consider the resource implications of reducing the backlog.

### Public complaints

14.21 The inquisitorial model of inquiry for which the IGIS Act provides is well-suited to the task of dealing with complaints from the public. Once an issue is raised, it is for the Inspector-General to investigate it by gathering such oral and documentary evidence as he judges necessary. We can see no advantage in making this a more formal process, less still in converting it into any kind of adversarial proceeding before a tribunal. We agree with the Inspector-General that such a proceeding would be inappropriate to the task and to the subject-matter of inquiry, and could prove to be counterproductive, both for the complainant and for the agency.

14.22 Complainants and agencies have generally accepted the conclusions reached by IGIS after these inquiries, almost all of which have concerned complaints about ASIO. Since IGIS will ordinarily be unable to supply the complainant with any detail of the inquiries undertaken, continued success in the discharge of this function will depend upon the office maintaining credibility in the eyes of the public. Any perception that the office lacked independence from the agencies would jeopardise that credibility, as would any significant delay in the completion of an inquiry.

---

426 T2858.
427 T147.
428 Exhibit 45.3.4, paragraph 74.4.
429 Exhibit 23.3, paragraph 22.
14.23 As we have seen, IGIS's powers to investigate ASIS in response to complaints are restricted in several ways. The restrictions apply equally to the discharge of the oversight function. In Chapter 9 we have recommended some amendments to the IGIS Act to permit certain inquiries to be undertaken with ministerial approval, rather than being dependent on a ministerial request.

14.24 Mr Holdich drew attention to the requirement for ministerial approval under s.8(8) for an inquiry into a matter which occurred before the commencement of the Act on 1 February 1987. Noting that complaints had often involved a sequence of linked events beginning before that date, he argued that his statutory discretion to decide whether or not to inquire into such a complaint might be sufficient, without any need for ministerial approval. For our part, we see it as highly improbable that ministerial approval would be declined in the circumstances described by the Inspector-General, where a complaint or grievance concerned a chain of events stretching back before 1 February 1987. We recommend no change.

14.25 Both the Inspector-General and the Service made submissions concerning the procedures by which IGIS conducts inquiries. Since the procedures apply whether the inquiry is into a complaint or a grievance, we defer our consideration of those submissions until later in this chapter.

**Inquiries into grievances**

14.26 It appears that IGIS was given the function of inquiring into grievances of the staff of ASIO and ASIS because there was no other avenue of external review available to those employees. When ASIO attempted to have IGIS excluded from inquiring into grievances of its employees, the then Secretary, PM&C, responded:

As a general principle ... employees of all Government organisations should have access to an external review mechanism where they have serious grievances against management.431

14.27 This principle was not, however, embodied in the IGIS legislation. Instead, the external review for which the IGIS Act provided was of a temporary and transitional kind. It was intended that the function of IGIS in relation to employee grievances would diminish or disappear once the internal procedures

---

430 Exhibit 45.3.4, paragraph 85.7.
431 Exhibit 15.2.3.
of the agencies for dealing with grievances were assessed as satisfactory. The original Hope recommendation was that the emphasis should be on an appropriate and effective internal system of review of grievances and that review by the Inspector-General of an employee grievance should be at his discretion 'if he felt that those procedures were not operating properly or effectively'. The original drafting instructions for the IGIS Bill treated the adequacy of the internal grievance procedures as a matter to be considered by the Inspector-General in deciding whether or not to entertain an employee complaint. In the event, s.11(5)(a) made clear that once the internal procedures were adjudged as satisfactory, IGIS would be excluded.

14.28 In May 1993, IGIS received written advice from the Attorney-General’s Department that an ASIS employee could still approach the Inspector-General with a grievance under s.8(6), notwithstanding that the Inspector-General had previously endorsed the ASIS grievance procedures as adequate and effective. According to the advice, the Inspector-General must be satisfied at the time the grievance is lodged that the procedures are adequate and effective. IGIS has interpreted this advice as meaning that he should consider on a case-by-case basis whether the procedures are adequate and effective, having regard to the way in which they are administered.

14.29 Between October 1993 and May 1994, there was a lengthy exchange of correspondence between the Inspector-General and the Director-General about the adequacy and effectiveness of the ASIS grievance procedures. Ultimately the Inspector-General advised that his concerns had been met by changes made to the grievance procedures and that he regarded them as adequate and effective, 'subject of course to the necessity for that question to be re-assessed at the time of the lodging of any complaint under s.8(6)'.

14.30 The effect of s.11(5)(a) is that, if the Inspector-General continued to be satisfied with the ASIS grievance procedures, there would be no avenue for external review of grievances. Apparently recognising this, the Inspector-General is taking what we regard as a generous view of the 1993 advice he received. There have been three inquiries into grievances of current or former

---

432 This was confirmed by Mr McInnes who was in PM&C when the legislation was negotiated - Exhibit 32.1, pp.3-4; T854; T877.
433 Exhibit 2.2.2.7, paras 8.63-4.
434 Exhibit 15.2.1, p.19.
435 Exhibit 20.1.20, p.23; Exhibit 23.1, paragraph 7.
436 Exhibit 20.1.20.
437 Ibid., [p.36]; T753.
ASIS officers which IGIS has commenced since giving clearance to the ASIS grievance procedures in May 1994. As we understand the approach, IGIS has considered as a threshold question whether the ASIS procedures were adequate and effective in the particular case. Where he has concluded that they were not, he has regarded himself as unconstrained by s.11(5)(a). This process has not, apparently, involved any systematic re-examination of the procedures as such or any identification of their deficiencies.

14.31 In our view, there should continue to be an avenue for external review of grievances relating to ASIS. The fundamental principle is the one already identified, that aggrieved employees of Government organisations should have access to an independent review process. External review has the additional benefit that it provides an opportunity for the identification of flaws in the internal review processes. But even if the internal review processes are appropriate, and operate effectively, employees should have access to external review. It is in the interests of the individual and of the organisation that an employee should be able to challenge the outcome of the internal review. As the Director-General acknowledged:

where, for the best reasons, [after] an application of what we think are good procedures, if people are unhappy, they do need some other external [avenue of review].438

14.32 It follows that we see no place for a provision such as s.11(5)(a). ASIS employees should have access, as of right, to a mechanism for external review of grievances, irrespective of the state of ASIS's internal grievance procedures. We regard it as most desirable that the Inspector-General should continue to monitor the adequacy and effectiveness of those procedures,439 and to advise ASIS of any deficiencies which are identified. This can only promote the interests of ASIS officers and of the Service itself, and lessen the need for external review. But, whatever the Inspector-General's opinion may be from time to time, there should be guaranteed access to external review.

14.33 The key issue is whether the function of reviewing grievances should remain with IGIS. On the basis of our close examination of four of the Inspector-General's inquiries into grievances of former ASIS employees, we have come firmly to the view that it should not. We set out our reasons in the next section.

438 T119.
439 Which he can do of his own motion or at the Minister's request - s.8(2)(b).
The experience with ASIS grievances

14.34 We have reviewed the Inspector-General’s conduct of his inquiries into four separate grievances lodged by officers or former officers of ASIS. That examination has led us to conclude that the informal, inquisitorial model of inquiries which the Act establishes is quite unsuitable for the review of employee grievances.

14.35 The chief deficiency of the inquisitorial approach is that it permits, indeed encourages, open-ended inquiries. The Act imposes no limits either on the scope of a grievance, other than that it must directly relate to the employment, or on the manner in which it is investigated. As a result, two of the four inquiries ranged very widely indeed.

14.36 The extensive delays in the completion of the inquiries were partly a function of the range of issues raised by the complainants and partly of the Inspector-General’s failure to impose any limits on his own investigations. A further contributing factor was the procedural requirements imposed on the Inspector-General by the legislation. The Act provides that:

(a) IGIS shall not make a report containing opinions that are critical of an agency unless IGIS has given –

  (i) the head of the agency reasonable opportunity to appear and make submissions (s.17(4));

  (ii) the responsible Minister a reasonable opportunity to discuss the proposed report with him (s.17(9));

(b) any person whom IGIS proposes to criticise must be given an opportunity to appear and make submissions (s.17(5));

(c) on completing an inquiry, IGIS must prepare a draft report setting out his conclusions and recommendations and give a copy of the draft report to the head of the agency. If the head of the agency makes comments on the draft report, those comments must – so far as relevant – be included in the final report (s.21(1) and (2)).

We understand the reasoning behind these provisions. There are, of course, sound reasons of principle for providing an opportunity to respond to criticism. But the process of preparing draft reports, seeking comment and then modifying the report as necessary in the light of the comment can add considerably to the time it takes to complete an inquiry.
There is another difficulty. In several of the cases, these processes, involving proposed reports and draft reports, resulted in modification of the Inspector-General’s view in the light of comments from the Service. This is likely, if known to a complainant, to give an impression that the Inspector-General is insufficiently independent of the Service. In our view, the practice of soliciting comment on a draft report, and then deciding whether or not to incorporate it in the final report, is less effective than a procedure which allows all those involved to make submissions to a tribunal before it prepares a final report. This requires that all should understand what the issues are, and address them.

**The need for determinative power**

The Inspector-General has no power of determination. He is not empowered to give binding rulings, but is limited to forming conclusions and making recommendations. The indirect objective of each inquiry is to further the objects of the Act, in particular to assist Ministers in the oversight and review of legality, propriety and human rights issues (s.4). The direct objective of the inquiry is to produce, for the Minister and the Director-General, a report setting out IGIS’s conclusions and recommendations (s.22(1)). It is important to note that the report goes to the Minister and the agency. The complainant receives ‘a written response’ (s.23(1)). The written response received by the complainant is often a very truncated version of the full report given to the Minister and the agency, which again can create a perception of imbalance.

What emerges more clearly than anything else from our examination of the ASIS grievances is the need for an external review body which is demonstrably independent of government and, above all, which has the power to make a final determination binding on all parties. It is vital that the determination should be, and be seen to be, the end of the matter. To this end, it must be clearly understood from the beginning of the review process that the decision will be final and binding.

Finality in this sense is necessary to exclude the possibility of any re-examination of a grievance within government, as can occur when a Minister has to decide whether to accept a recommendation from IGIS. Finality of decision should also dispel any belief on the part of aggrieved individuals that there is some further avenue of appeal beyond the review body. Finality means certainty for both the individual and the agency, and it should minimise the risk of disaffection continuing and ultimately spreading to the public arena.
14.41 In our view, there is a persuasive case for moving to an adjudicative model for the review of grievances. The elements of this model would include:

(a) a requirement for clear definition of the grievance;

(b) a preliminary hearing directed at identifying the issues;\(^{440}\)

(c) the imposition of a timetable for the provision of relevant documentary material by the complainant and by ASIS;

(d) the presentation of oral evidence by the complainant and by the Service;

(e) power in the tribunal to call its own evidence;\(^{441}\)

(f) the making of submissions by the complainant and the Service, with the opportunity for each to comment on the submission of the other; and

(g) final determination of the grievance by the tribunal, with power to award compensation.

14.42 So structured, we think the model would be of great benefit to both the individual and the Service. It would promote early crystallisation of the key issues, underline the independence of the reviewer from both complainant and government and, above all, avoid the delay in resolution which can itself be so destructive. The essential feature of the model is that the parties would be brought together in the same forum, with each having the opportunity to respond directly to the other's case before the tribunal made its decision.

14.43 Great care will need to be taken to ensure that the position of the complainant in such proceedings is adequately protected. Otherwise, the obvious inequalities in access to information and in financial resources are likely to produce significant unfairness. The imbalance in information is, of course, a characteristic of proceedings against government and can largely be rectified by strict insistence on the provision by the agency of all relevant documents. The tribunal's ability to enforce this obligation would be enhanced if the tribunal were able, in appropriate cases, to be assisted by its own counsel.

\(^{440}\) cf ASIO Act s.58(4).

\(^{441}\) cf ASIO Act, s.58(11).
14.44 The financial imbalance is more difficult to correct, particularly as it affects legal representation. Unless the right to legal representation were excluded altogether, or confined to the most exceptional circumstances, it must be assumed that the agency would almost always be represented. Most complainants, by contrast, would be unable to afford legal representation for a hearing of any duration.

14.45 For a complainant to be unrepresented in circumstances where the agency was represented would, in most instances, be unacceptable. The solution, in our view, is for the right to legal representation to be excluded absolutely and for provision to be made for the tribunal to appoint counsel assisting, where the tribunal considers the nature and/or complexity of the case warrants it. Counsel's function would be to gather and present the evidence, including by examining all witnesses, and this should ensure that evidence on both sides was properly tested. If no counsel were appointed, the tribunal itself would take the evidence from the complainant and from the agency. The absence of other legal representatives would help preserve procedural informality. As with the Security Appeals Tribunal, there should, in any case, be a requirement for the tribunal to conduct its proceedings with as much expedition and as little formality and technicality as possible.\textsuperscript{442}

14.46 We recognise that a blanket exclusion of legal representation is very unusual. It is not, however, unprecedented. The legislation establishing the Merit Protection and Review Agency makes no provision for representation of persons appearing before the Agency to give evidence or produce documents.\textsuperscript{443} Under s.17(6) of the IGIS Act the Inspector-General can approve representation 'by another person' in the limited circumstances where the Act requires that an opportunity be given to the head of an agency or another person to appear and make submissions. In none of the cases we examined was such approval given.

14.47 If, contrary to our view, legal representation were to be permitted, steps would need to be taken to reduce the inequality between complainant and agency. First, provision could be made for legal assistance to be granted by the Attorney-General in a case of hardship, equivalent to the procedure established for the Security Appeals Tribunal.\textsuperscript{444} Secondly, as we have said, the tribunal should be enjoined to minimise formality and technicality. Thirdly, the tribunal

\textsuperscript{442} cf ASIO Act s.67(1)(b).
\textsuperscript{443} Merit Protection (Australian Government Employees) Act 1984, Part II, Division 7.
\textsuperscript{444} cf ASIO Act s.72.
should be required to take whatever steps it regarded as necessary to protect the interests of an unrepresented applicant.

**A new review body?**

14.48 If, as we recommend, an adjudicative model is accepted, we are firmly of the view that the Inspector-General should not be the adjudicator. The function of reviewing employee grievances should be removed altogether from the jurisdiction of IGIS.

14.49 There are four principal reasons for this view. First, previous experience indicates that grievance inquiries are a very serious distraction from the Inspector-General's primary function of monitoring the activities of the agencies. Given the typically pressing nature of such inquiries, this distraction, and the diversion of resources which it entails, are difficult to resist. Secondly, the adjudicative function is fundamentally different from the investigative approach which IGIS will continue to adopt in his oversight role and in his investigation of public complaints. The former requires independence and detachment, while the latter necessarily involves close and regular contact with the agencies. The methodology is also quite different, the former requiring the evaluation of evidence presented by others, the latter involving the active gathering of evidence. We think that to require the Inspector-General to perform functions of both types virtually simultaneously would be likely to lead to institutional schizophrenia, with neither function being performed successfully as a result.

14.50 Thirdly, the different roles require different qualifications. While the qualities of integrity, independence of mind and capacity for rigorous inquiry identified by Mr Justice Hope as selection criteria would be relevant to both, it would be necessary for anyone performing the adjudicative role to have knowledge of, or experience in, quasi-judicial review. Such qualifications would not be necessary for the discharge of the inquisitorial function. Fourthly, it is inevitable that IGIS will be in close contact with ASIS management in the performance of his monitoring function and will from time to time – we would hope more often than not – be providing management with a healthy report card. In the eyes of an employee or former employee raising a grievance for external adjudication, this may give rise to a perception of bias which could weigh against acceptance of the independence and finality of the adjudication.

14.51 The adjudicative function should, in our view, be conferred on an appropriate tribunal. The obvious candidate is the proposed Security Appeals Division of the Administrative Appeals Tribunal (AAT).
reviewing security assessments made by ASIO, formerly carried out by the Security Appeals Tribunal established under the ASIO Act, will be transferred to that Division under legislation currently before the Parliament.\textsuperscript{445} Like its predecessor, the Security Appeals Division will develop a specialist expertise in security matters and will be required to be familiar with public sector employment policies and practices, and with the operation of ASIO. It would be a natural extension of the Tribunal's review function in relation to security assessments for it to have the jurisdiction to review grievances of employees of ASIS and ASIO.

14.52 The review of Government decisions on the merits is the defining characteristic of the Administrative Appeals Tribunal. The Tribunal's standing, its expertise in matters concerning Government, and the authority which its decisions carry are all factors conducive to finality. In addition, the AAT is a large enough tribunal to be able to cope with fluctuations in workload, without experiencing the problems which IGIS faced with the upsurge of grievances in the early 1990s.

14.53 The Tribunal's review of a grievance should be on the same basis as a conventional proceeding in that Tribunal when a government decision is under review. That is, there should be a complete re-hearing of the matter, with the Tribunal exercising all the powers of the relevant decision maker in the agency. Its task should be to review the employee's grievance, as defined by the employee for the purpose of the internal grievance review which will have taken place first. In the case of ASIS, the internal grievance panel has recommendatory power only, the final decision resting with the Director-General.

14.54 The basis of the Tribunal's review would therefore be the employee's application for a review of the Director-General's decision at the conclusion of the internal grievance process. Review of that decision would necessarily involve an examination of the matters raised in the grievance process. The issue having been thus broadly defined for the Tribunal, we would expect it to take control of the proceeding and, so far as necessary, be ready to seek its own evidence in addition to that placed before it by the parties. Given the sensitivity of the role, we recommend that the Tribunal be constituted for this purpose by a presidential member.

14.55 Both the Service and the Inspector-General submitted that jurisdiction over employee grievances should be conferred on an independent review body.

\textsuperscript{445} Law and Justice Legislation Amendment Bill (No. 3) 1994, clause 3.
The submissions were importantly different, however, from each other and from what we recommend. The Service proposed that IGIS retain the function of inquiring into grievances and that this be supplemented by ASIS or a complainant having access to a security tribunal, presided over by a judge, for a review of any recommendations, conclusions or findings of IGIS. The Inspector-General submitted that inquiry powers in relation to employee grievances should be divided, with the Inspector-General being given responsibility for investigation and conciliation or mediation of those grievances, with determinative powers being given to an independent tribunal. Both the Service and IGIS saw the proposed Security Appeals Division of the AAT as an appropriate body for those parts of their respective models involving a tribunal.

14.56 As we have said, we consider that IGIS's role in relation to employee grievances should cease altogether, other than the monitoring functions related to internal procedures. Given the importance which is attached on all sides to expedition and finality in relation to review of individual grievances, we regard it as appropriate that there be two stages only, one internal and one external. If the internal processes fail, the external review should provide the kind of decisiveness which the Director-General clearly envisaged when he said:

if they're dealing in a strictly judicial situation, where they come into a courtroom situation - a tribunal - present their case, the other side presents its [case], the person - a magistrate, a judge, whatever - makes the decision, bang, that's it. The IGIS process has been a lot more informal.

14.57 We think it important that former, as well as current, employees of ASIS should have an avenue for review of grievances. If the subject matter of the grievance is related to employment with ASIS, it should not matter that the person has ceased to be employed. Indeed, the fact of termination, or the circumstances in which it occurred, may well give rise to a grievance. It is obviously in the interests of the Service that there be an avenue for review. It is not appropriate for an internal grievance committee, even one with external representation as in the case of ASIO, to entertain complaints from former staff. Strictly speaking, the Inspector-General's jurisdiction over grievances under s.8(6) was confined to the grievances of current employees. The Inspector-General has, nevertheless, conducted inquiries into the grievances of a number of former ASIS employees, apparently by treating them as public complaints under s.8(2)(a).

446 Exhibit 45.2.6, paragraph 4.2.8.4.
447 Exhibit 45.3.4, paragraph 77.1.
448 T119.
14.58 It should, we think, continue to be a pre-condition to external review in the case of an employee that the internal grievance procedures have been exhausted. Provision should be made, in terms equivalent to s.11(5)(b) of the IGIS Act, for access to the AAT to be unavailable unless and until an employee has pursued the grievance through the internal processes. The Tribunal could be given power to relieve a complainant from this obligation if it could be demonstrated that, for special reasons, the pursuit of a grievance within the Service was impracticable. Likewise, there should be an equivalent provision to s.11(5)(c), empowering the Tribunal to decline to entertain an application for review of a grievance if satisfied that the subject matter is not of sufficient seriousness or sensitivity to justify examination. This would be a matter upon which counsel assisting the Tribunal, if appointed, could advise.
15.1 The public face of ASIS is the face presented in the media. Perhaps more accurately it is the face drawn by the media, since a degree of artifice is often involved in order to supply by invention the facts which a firm policy of secrecy conceals. The portrait is seldom other than unflattering. There are several reasons for this. First of all, many media organisations are sceptical about the need for an agency such as ASIS and are therefore predisposed to denigrate it on principle. Secondly, unfavourable media attitudes reflect community responses in Australia, where there is a strong tradition of dislike of spying and of doing things in an apparently underhanded or unfair way. Thirdly, it is almost inevitable that there should be mutual suspicion and even hostility between the media, which trade in the free flow of information and opinion, and a service which is dedicated to secrecy.

15.2 There is, at the same time, something of an irony here since both journalists and intelligence officers are deeply involved in the business of wrestling secrets from those who have no wish to part with them; and cultivate and rely on sources of information whose anonymity they take great care to protect. Indeed, it might be suggested that there are other similarities. The derisive attitude of journalists towards ASIS is mirrored by the condescension which many people bestow upon journalists; and the soiled trench coat is often said to be the standard uniform of both journalists and spies, the former being distinguished only by their inky fingers and, according to Charles Dickens, their reptilian characteristics.\[449\]

15.3 There are therefore, or there ought to be, some affinities between a journalist and an Intelligence Officer which experience, however, does not reveal. Of the reasons for discord which we have suggested above, we are

\[\text{449 In The Pickwick Papers.}\]
inclined to think that the journalistic judgment that our society has no need for an agency of this kind is the most influential. That assumption, added to ignorance of what ASIS actually does and how its members work and behave operationally, naturally produces a view of ASIS which owes much to the fiction of Le Carré and Fleming and to the persistent myth that ASIS is an uncontrolled and unaccountable body which pursues its own objectives without the restraints which executive and parliamentary structures impose upon other agencies of government.

15.4 In this chapter, we examine how this image of ASIS is shaped by the approach which ASIS and the media adopt to each other. We then consider ways in which ASIS might develop its relationship with the media, so that what is presented to the Australian public more closely resembles the true position.

The ASIS approach: the blanket of secrecy

15.5 Historically, secret intelligence agencies adopted an approach of total secrecy. This meant that not only were their sources, methods and intelligence product kept secret, but their very existence was concealed from public knowledge. Although the establishment of the CIA in 1947 was a matter of public – and legislative – record, the British Secret Intelligence Service remained unavowed until 1992. Following the British example, the establishment of ASIS in 1952 was kept secret.

15.6 The fiction of non-existence proved to be unsustainable in the long term. In 1977, Mr Justice Hope concluded that secrecy concerning ASIS’s existence was neither necessary nor desirable.450 Citing ASIO and the CIA as demonstrating that intelligence services could carry out secret operations while being publicly declared, Mr Justice Hope recommended that the existence of ASIS be publicly acknowledged. The Government did so in October 1977, in a Prime Ministerial statement to Parliament.451 The Prime Minister added, however, that:

ASIS’s capacity to serve Australia’s national interest will continue to depend on its activities being fully protected by secrecy. The Government will therefore adhere strictly to the practice of refusing to provide details of ASIS’s activities nor will it be prepared to enter into any discussion on the Service.

15.7 Since 1977, ASIS has adhered to this policy of strict secrecy. According to the Minister, it has worked to secure its operations by seeking to avoid any

450 Exhibit 2.1, paragraphs 301-303.
public reference to itself or its activities.\textsuperscript{452} The Service's guiding assumption has been that 'there is no such thing as good publicity for an intelligence service'.\textsuperscript{453} The rationale advanced by the Service, and endorsed by the Minister,\textsuperscript{454} is that:

People are willing to work with ASIS, to provide it with the information it is seeking, often at some risk to themselves, because they trust the Service to be discreet, to be reticent, to be able to keep secrets. Agencies of foreign governments are willing to work with ASIS and, through it, to share confidences with the Australian government because they trust in our discretion and security. An intelligence service that courts publicity, promotes an active public image and is regularly in the public eye is not one that is likely to win the trust of those with whom it needs to deal if it is to succeed at its appointed tasks.\textsuperscript{455}

15.8 Consistently with this policy, ASIS has had virtually no contact with the public or the media. Where contact with the media is considered by ASIS or the government to be absolutely necessary, it is handled by the Minister's office. The Minister is responsible for responding to media stories about ASIS and for making public statements about the Service. The Director-General does not take calls from the media.\textsuperscript{456} The Department of Foreign Affairs and Trade (DFAT) handles public (and some official) inquiries addressed to ASIS. ASIS has no programs of public information and as little as possible about the Service is released into the public domain. The only publicly acknowledged ASIS officer is the Director-General.

15.9 The standard response to media stories has been for the Minister to state that the government neither confirms nor denies the statement being made about the Service. The practice has thus become known as 'neither confirm nor deny' (NCND). The reasoning is obvious enough: to confirm an accurate allegation would convert mere assertion into official fact, while to deny an untruthful allegation would imply confirmation of any subsequent allegation which was not denied. We examine the NCND policy more closely below. What is significant here is the uninformative and unresponsive attitude which NCND epitomises.

15.10 Both the Service and the Minister acknowledge that non-engagement with the media has its costs:

\textsuperscript{452} Exhibit 39.1, paragraph 60.
\textsuperscript{453} Exhibit 14.3, paragraph 1.
\textsuperscript{454} Exhibit 39.1, paragraph 60.
\textsuperscript{455} Ibid.
\textsuperscript{456} T50.
not the least being that the overwhelming majority of the material about ASIS in the public domain originates from those opposed to ASIS and has gone unchallenged and uncontested. The amount of material about ASIS in the public domain is currently substantial. Overwhelmingly it is negative and critical about the Service and much of it is wildly inaccurate. It has been demonstrated to the media that ASIS is an easy and safe target - it does not fight back and anything, no matter how outrageous, may be said about it with impunity.457

15.11 Staff morale is adversely affected when persistent public criticism, and uninformed comment, go unanswered. According to the Director-General:

people felt frustrated and angered by the various allegations that have been made about the Service. I think anyone from within the Service knows that they are without a foundation in almost all cases, or, where there is a germ of truth, that has been distorted. But there is a sense that people feel they're a hard-working, dedicated group of people serving the national interest and they are being consistently maligned in the media, without any response on the part of the government. And, as I said, this has caused frustration and I think it probably has damaged morale in some respects.458

15.12 The Service recognises that a wholly passive stance with the media is no longer adequate. With the Minister's support, the Director-General has been working towards the development of a more positive media policy. Some elements of this will be examined further below.

The media approach: 'a good story'

15.13 In a media-dominated world where information and entertainment become one and the same, and where the quest for ratings and circulation dominates, secret services are a good story.459 From the 'Boys' Own' tales of spies and adventure on the Northwest Frontier to the more modern and sophisticated development of the genre in the novels of Le Carré and Ian Fleming and the movies they inspired, security and intelligence agencies have been invested with an aura of romance, thrills and adventure. The exploits of James Bond present a shadowy world of violence and intrigue which many find fascinating. The CIA is given credit, at least in popular reports, for the exercise of power and influence on a formidable scale. Sometimes the more exaggerated criticisms of the maligned activities of such agencies even serve to enhance their image.460

457 Exhibit 14.3, paragraph 3.
458 T55; see also the evidence of SWA, T969.
459 'The operations of spies is great media'; Mr Hill, T*637*.
460 T950, 1133, 2041.
Such an image may help ASIS recruit staff, but it also makes the Service a ready media target. The intrigue which secrecy generates can, however, attract the very attention which the Service and its sources, aim to avoid. It was readily acknowledged by the media witnesses who appeared before the Commission that ASIS makes a good story precisely because it is shrouded in secrecy. Mr Kohler believes journalists are 'fascinated by secret organisations'. According to Mr Hill, the scarcity of information about ASIS was 'what makes these exceptional stories like the *Four Corners* one so interesting'. Ms Grattan and Mr Kelly agreed that the newsworthiness of stories about ASIS was heightened by the secrecy surrounding the Service. The case for publication by journalists would be weaker if more information were available in public statements.

That said, ASIS has not in fact been the subject of a great deal of media coverage since its formation. With one or two exceptions, there is little sustained interest in ASIS amongst Australian journalists. The two periods of significant media focus on ASIS (following the 1983 Sheraton Hotel incident and during the months preceding the present Inquiry) have resulted from internal problems of the Service spilling into the public arena, rather than from the efforts of the media to uncover information on ASIS.

When stories are published, however, the combination of understandable ignorance, romantic speculation and deep-seated suspicion produces some surprising results. Perhaps the most surprising is that journalists and editors appear to suspend the operation of their ordinary critical faculties when faced with a story about ASIS. Some examples will serve to demonstrate the point.

**The ASIS assassin**

In March 1994, an article was published in the mass-circulation women's magazine *New Idea* entitled 'Confessions of a Spy'. It purported to describe the exploits of one Wendi Holland, who claimed to have been employed by ASIS between 1969 and 1989. The promise of the article's sub-heading – 'I killed more than ten people' – was immediately realised in the lurid language of the opening paragraph:

---

461 T*837* Mr Kohler is the Editor of the *Age.*  
462 T*644* Mr Hill was then Managing Director of the ABC.  
463 T*899* Ms Grattan is the Editor of the *Canberra Times*; Mr Kelly, the Editor-in-Chief, the *Australian.*  
464 T*714*.
Australian trained assassin and spy Wendi Holland pulls a thin-bladed knife out from its wooden scabbard and slices the air in front of her jugular vein. ‘This’ she announces with a cold edge to her voice, ‘is how I slitted his throat. He died very quickly.’

Ms Holland described her training at a secret property near Canberra where she was taught ‘to inflict wounds so the victims would die quickly’. She claimed to have carried out more than ten assassinations on orders from ASIS. A less dramatic version of Ms Holland’s story had appeared in the *Women’s Weekly* of November 1993. The assassination claim had first surfaced in a Melbourne radio interview in December 1993, which was republished in the *Canberra Times*. It was subsequently repeated in separate media interviews with the ABC in June 1994 and the *Sunday Telegraph* in July 1994.

15.18 It is remarkable that this story should have been given any currency at all, particularly by such serious-minded media as the ABC and the *Canberra Times*. As one newspaper admitted, it was ‘the most fantastic story’. Even making allowances for the lack of information about what ASIS does and does not do, it must, on any rational view, have seemed highly probable that the exploits to which she laid claim were wholly unsound.

15.19 Ms Holland maintained her story in evidence to the Inquiry. Despite repeated requests, however, she failed to produce any of the diaries and other documents which she claimed would corroborate her assertions of ASIS service. ASIS has no record of any contact with Ms Holland. We are satisfied that there is no truth in her claims to have been employed by ASIS, let alone in her stories of carrying out assassinations on ASIS’s instructions. Nothing she said persuaded us that there was the slightest substance in her story. She received substantial payments for each of the magazine articles and it is difficult for us to say whether she believes what she is reported to have said – and, indeed, what she told us – or whether she has invented the whole episode. Whatever the answer to that question, Ms Holland’s description of her adventures with ASIS is quite untrue.

---

465 Exhibit 12.2, tab 11.
466 Ibid., tab 15A.
467 Ibid, tab 25AA.
468 Ibid, tab 28.
469 Ibid, tab 28.
470 T603.
The CIA assassin

15.20 We have already referred to the claim made on the February 1994 *Four Corners* program by a former ASIS officer that a CIA officer had offered to murder an Australian diplomat. In the transcript of the interview conducted in preparation for the *Four Corners* program, the reporter exhibited considerable reluctance to accept what the former officer said about this offer:

> A lot of people watching this may have difficulty accepting that the climate in Cairo got to such a stage that friendly intelligence services were offering to kill Australian Foreign Affairs officials to help you do your job ... A lot of people would find it absolutely incredible that things had got as bad as you describe ... I don't think you've still described for me adequately just exactly why things were as bad as they were. Give me a bit of the emotion ...

15.21 We are not surprised at the journalist's evident scepticism about this highly improbable story. What is surprising is that he apparently ignored his professional instincts and gave the story a public airing.

The ASIS fire

15.22 In the early hours of 26 November 1994, a fire broke out in the administration and finance sections of ASIS headquarters. All fire warning and safety systems worked properly and the fire was promptly located by ASIS guards who were on duty at the time. Damage was limited to one wing, although there was smoke damage to adjacent areas. Several offices were destroyed, with extensive collateral damage throughout the whole wing. Total documentary losses were confined to part of the contents of one two-door compactus, located in the office of the archives and records disposal unit. The limited file material which was destroyed contained either old material of no current relevance or work in progress, the supporting material for which was held elsewhere.

15.23 Press reports of the fire instantly assumed – without any factual basis for doing so – that the fire had destroyed a large number of documents directly relevant to the Inquiry. The *Australian* of 29 November claimed that 'hundreds of top secret documents' relevant to the Inquiry had been destroyed:

> The fire has erased highly sensitive ASIS files and archives that detailed the activities and operations of the troubled spy agency over the past decade.

---

471 Paragraph 28.12.
472 Exhibit 12.4.2.
The blaze is a big blow to the Government's Inquiry into the accountability and management of ASIS because it destroyed many of the records needed to adequately assess the organisation's performance ...

It was rumoured yesterday that the fire also destroyed thousands of files that the Service was alleged to have kept on Australian citizens.

15.24 The Herald Sun of 29 November carried the same fanciful story, this time asserting that 'thousands of sensitive files' had been destroyed. The inference that this was a 'wonderfully convenient' fire proved irresistible, even to a journalist of the standing of P.P. McGuinness:

[ASIS] has, it seems, resorted to the time-honoured 'the dog ate my homework' defence to stymie the Inquiry at present under way into its treatment of its own agents – in this case, it has simply burnt the inconvenient files (purely accidentally, you understand).473

15.25 It was not the function of this Inquiry to investigate the causes of the fire. It can, however, be said categorically that the fire did not affect in any way the production of documents to the Inquiry by ASIS. By the time of the fire, the process of collecting evidence was almost concluded, and all outstanding requests for ASIS documents have been met. Moreover, an inspection by Commissioner Samuels and Inquiry staff on 30 November 1994 established that the area where operational and personnel files are kept was not near the fire area and was totally unaffected.

'Tens of thousands of files'

15.26 The collection, retention and communication by ASIS of information concerning Australian citizens or permanent residents is a controversial issue. It is hardly surprising that this should be so. Where an organisation operates almost entirely in secret, there is ample room for speculation over what interest the organisation may be taking in the activities of Australians. Such speculation is traditionally – and understandably – more closely associated with ASIO. But ASIS is by no means immune.

15.27 Wide currency has been given to an assertion that ASIS secretly holds tens of thousands of files on Australian citizens. This assertion owes its genesis to the following passage from the Four Corners program of 21 February 1994:

REPORTEER: Most Australian Government files like these are subject to strict privacy legislation but perhaps the most concerning aspect for all Australians

should be that ASIS secretly holds tens of thousands of files on Australian citizens, a database completely outside privacy laws.

OFFICER ONE: Those things are never scrutinised. A lot of information that goes onto those cards will just be hearsay.

OFFICER TWO: If ASIS provided information to ASIO which led to the refusal of a visa or a job my understanding is that the individual would not be told that on the facts and grounds. He would not realise that the information came from ASIS. That's my understanding.

REPORTER: So information could be held, of a deleterious nature, on an Australian citizen, inside ASIS?

OFFICER TWO: Yes.

REPORTER: And they wouldn't know anything about it?

OFFICER TWO: No ... No comeback at all.474

15.28 As disclosed in his 1993-94 annual report, the Inspector-General visited ASIS on several occasions during that year to examine the Service's holdings on Australian citizens or permanent residents. He did this, he said, because:

an ex-officer of the Service told me that ASIS holds thousands of files and cards on Australian citizens; that the files and cards recorded information and gossip of a personal nature and that this was freely available to ASIS officers and was made available on request to foreign intelligence services.475

15.29 After examining relevant cards and files, the Inspector-General concluded that the rights of Australians were not abused in any way. We note in passing that the publication of these conclusions in the Inspector-General's annual report received no publicity of which we are aware. Indeed, that report, which ought to have reassured the public that ASIS was, in this respect, operating within proper bounds, appears to have done nothing to inhibit speculation about these holdings at the time of the fire. As we have already seen, at least one of the reports of the fire suggested that it had destroyed 'thousands of files ... on Australian citizens'.

15.30 Given the public attention which this assertion has attracted, we decided to conduct our own review of holdings by ASIS on Australian citizens. For that purpose, Commission staff examined a sample of close to 10 per cent of all holdings by ASIS on Australian citizens, the sample having been randomly selected by Commission staff. The holdings fall into four general categories:

(a) persons 'listed' or briefed by ASIS;

(b) persons of operational interest;

474 Exhibit 12.1, tab 41; see also Sunday Telegraph, 16 January 1994, Exhibit 12.2, tab 19.

(c) staff; and

(d) persons of security interest.

We deal with each of these categories in turn.

**Listings**

15.31 Numerically, the most substantial holdings are those relating to the 'listing' of persons for whom entitlement is sought for access to briefing on ASIS and to its secret intelligence reporting. These are people who are employed by other Government agencies – particularly assessment agencies, policy advising agencies, and law enforcement agencies – whose jobs require knowledge of ASIS and its product. The holdings are not in the form of files but rather card references. There are files to do with listing, but they are generally, and sensibly, created for each department or agency so that records are held together of those officers of the department or agency who are entitled to receive ASIS material.

15.32 There is no doubt that it is appropriate for ASIS to engage in a process of clearing people for the purposes of listing, and appropriate for them to hold material which records those who are listed. Other than advice about listing to the individual and to the department or agency concerned, no material held for this purpose is passed outside ASIS. There is thus nothing improper in the holdings ASIS has for this purpose.

**Persons of operational interest**

15.33 There are also holdings in ASIS on Australian persons whom ASIS thinks are, or could become, of operational interest. That is to say, these are people who ASIS feels may be able to assist them in the performance of ASIS functions. Particularly in the early days of ASIS, these would often be people who were known to be travelling to parts of the world of interest to ASIS and whom ASIS might contact on return to see whether anything of interest had been observed. They may be people whose professions or language skills are such that there is potential for them to gain access to persons in positions of influence in other countries, or potential for them in other ways to gain worthwhile intelligence material.

15.34 Clearly, the interest ASIS has in such people is a positive interest, and one which is directed at the discharge of the Service's intelligence collection function. Based on our sample, the bulk of persons in this category have only a very limited reference on card. In general, and certainly in more recent periods, a file would only be created on such a person where ASIS determined to
approach them to seek a working relationship with them. Such files, and there are few, are then held in the Operations Division registry and very closely held indeed. Thus there is no publication, except within ASIS, of the information that a person is a potential contact and where that potential is activated, knowledge within ASIS is restricted to those who need to know.

15.35 Our sample showed no evidence of any material adverse to a person being recorded in this process. We conclude that it is legitimate and appropriate for ASIS to collect and hold information of this character on Australian persons in pursuit of its assigned functions and that the interests, including the privacy interests, of Australian citizens are not infringed by the careful processes which are followed.

Staff

15.36 The next largest category established by our sample comprised holdings relating to ASIS staff, former staff or potential staff. In most of these cases, holdings would appear on files created for the purpose. The material held on those files is, based on our sample, material of a kind it would be legitimate and normal practice for any employer to hold in relation to staff or potential staff, allowing for the fact that ASIS (because of its particular functions) requires more extensive security checking and revalidation than would most other employers.

15.37 Material on those files is for ASIS purposes and our sample found no evidence of publication of any of this material outside ASIS. We conclude that there is nothing improper in the holdings ASIS has of information on Australians for this staffing purpose.

Persons of security interest

15.38 The final and smallest category, and the category potentially most relevant to the assertions which have been made, is holdings on those Australian persons considered by ASIS to be of security interest. This is not a category defined by ASIS. Rather, it is our general description of the holdings relating to security concerns of various kinds, either for Australia or for ASIS itself. Examples of the former concern involvement of Australians in organised crime, including drug trafficking, in terrorist activities or in activities which appear to threaten the safety of other Australians. In these instances, information is generally passed to those Australian authorities (in particular the Australian Federal Police and ASIO) who have responsibilities that are relevant. Examples of security concerns for ASIS itself included threats to identify ASIS officers,
threats to the security of ASIS premises, cases where people pose as ASIS officers, and publication of material relating to intelligence and security in the media.

15.39 In some cases (such as threats to the security of ASIS premises), material was passed to other agencies with relevant responsibilities. On occasions, where threatened publication of sensitive material was involved, legal advice would be sought from the Attorney-General's Department. Otherwise, the holdings in this category are not published and are securely retained within ASIS.

15.40 Holdings in this category are essentially of a factual kind. No examples were seen in our sample of recording of personal information or the personal characteristics of an individual as perceived by ASIS staff. The holdings on media publications were, for the most part, simply copies of the articles or transcripts of electronic reporting. As already indicated, in some of those cases legal advice was sought. But beyond that, the material was not published outside ASIS nor could material on the files sampled in any way be described as containing personal details or material impacting adversely on the individuals or affecting their privacy.

15.41 Most of these holdings take the form of references on general files rather than specific files relating to individuals. Based on the Commission's sample, it is estimated that there have been some 2,300 such file references or files created since ASIS came into existence in 1952. Of this total there have been some 850 such references or files created since 1 January 1980.

15.42 No evidence was found of any systematic exercise of collection of information by ASIS on any individual or group. Rather, the character of this material is reactive, involving the drawing together and recording of information externally generated which has a bearing, as ASIS perceives it, on its security or on Australia's security interests. We conclude, therefore, that material in this final category, like the material in the other categories referred to earlier, is being held by ASIS for reasons directly associated with its functions, and that the material is being held in appropriately secure fashion and could not fairly be said to infringe the privacy rights of Australian citizens.

15.43 It follows that we consider the assertion made on the *Four Corners* program, and the flavour given in the subsequently repeated assertions, to be without any credible foundation.

15.44 We add that the regular monitoring by IGIS of ASIS's holdings and their dissemination of information on Australian citizens provides a valuable
check and discipline and should be continued. It represents a safeguard which will help ensure that ASIS does not collect, hold or disseminate information that is not related legitimately to its functions or to security.

**The need for verification**

15.45 The publication of wholly or substantially false stories points to the need for improved avenues for checking the veracity of information. We recognise that there are limits on the capacity of editors to satisfy themselves that their journalists' sources are reliable. At the same time, we were unimpressed by the degree of rigour apparently applied to the assessment of the reliability of sources for such obviously sensitive stories as these. Although editors may reserve the right to insist on their journalists disclosing their sources, calling on them to do so is the exception rather than the rule. Largely, editors rely on the experience of the journalist and on general assurances.476

15.46 While we accept that independent checking by a senior editor of the sources for a journalist's work is not realistic as a general proposition,477 we would have thought that stories about security and intelligence merited special attention. This is so both because of the risks of harm being caused by such stories and because of the acknowledged lack of information in the hands of media organisations to enable them to make judgments, about ASIS in general and about the consequences of publishing particular allegations. Greater rigour in internal processes will be enhanced by making available to media organisations more authoritative advice and information on intelligence matters. We have addressed this in Chapter 11 in the context of the D Notice system. The idea of an ASIS media liaison officer is considered further below.

**Alternative approaches to media relations**

15.47 The problems of sensationalised and inaccurate reporting are not unique to ASIS. Other security and intelligence agencies have had to confront similar problems, and have in recent years begun to respond by adopting a more activist approach. The comparisons are instructive.

15.48 ASIO has re-fashioned its approach to the media and public relations. Recognising that there is 'a great deal of legend and myth about ASIO', the Director-General has determined that ASIO should be 'a little more transparent

---

476 Mr Kelly, T*701-02*, T*717*, T*729*; Ms Grattan, T*892*, T*904*, T*917*; Mr Kohler, T*837*, T*845*, T*850*, T*852*.

477 T*852*. 

185
than it has been in the past'. ASIO is developing a public communications strategy, the elements of which include:

(a) the Director-General making himself available, on a selective basis, to the media;

(b) annual appearances before Senate Estimates Committees and their successors, Legislation Committees, since 1993;

(c) describing publicly what ASIO does, including in the public annual report, while not commenting on sensitive operational matters;

(d) adopting a policy of selective denial of allegations against ASIO;

(e) the appointment of a media liaison officer, whose function is to field approaches from journalists and discuss with them stories which they intend to publish.

15.49 ASIO’s new media strategy has been well received by media organisations. According to Mr Harvey, the Nine Network has built a relationship of respect with the ASIO media officer, because information from the officer has been shown to be accurate. Mr Grant also welcomed the appointment of an ASIO media officer, and commented favourably on the Director-General’s appearance at the National Press Club. Mr Waterford had found the ASIO media officer particularly useful for checking factual material.

15.50 The ASIO media strategy appears to have broken down some of the aura of mystery which had made ASIO an attractive media target. Mr Harvey considered that there were fewer media stories about ASIO because the media could no longer ‘willy nilly publish material’ without the opportunity of checking it with ASIO. According to Mr Grant, the new approach had helped ‘demystify’ ASIO and reduce the number of stories which ‘take the mickey out of ASIO’, so that it had become ‘less of a bête noire in the public mind’.

---

478 Exhibit 34.1, Attachment A.
479 Exhibit 34.1, p.8. The Director-General appeared at the National Press Club in 1992.
480 T*678*. Mr Harvey is the Director of News, Canberra Bureau, Nine Network.
481 T*750-1*. Mr Grant is Bureau Chief, Channel Seven.
482 T*884*. Mr Waterford is Deputy Editor, the Canberra Times.
483 T*669*.
484 T*750-1*. 
UK Secret Intelligence Service

15.51 The public avowal of the existence of the Secret Intelligence Service (SIS) in 1992 was part of the British government’s efforts to be, in Prime Minister Major’s words, ‘as open as possible about security and intelligence matters without prejudicing national security, the effectiveness of the intelligence and security services or the safety of their staff’. In 1993 the government published booklets on the internal Security Service and on the Central Intelligence Machinery. The latter describes the mechanisms for tasking and co-ordination of the various intelligence agencies, and summarises the functions of the different organisations. The main function of SIS is described as being:

the production of secret intelligence in support of Her Majesty’s Government’s security, defence, foreign and economic policies ... through a variety of sources, human and technical, and by liaison with a wide range of foreign intelligence and security services. Specific operations are subject to longstanding procedures for official and Ministerial clearance.

15.52 In 1994 Parliament passed the Intelligence Services Act to provide a statutory basis for SIS. One of the provisions of the Act was the establishment of an Intelligence and Security Committee, made up of nine members of both Houses of Parliament. The Committee is to ‘examine the expenditure, administration and policy’ of the intelligence agencies, and to produce an annual report which the Prime Minister will table in Parliament. The legislation was described by the Government as a further step in implementing a policy of greater openness in security and intelligence matters, wherever possible.

US Central Intelligence Agency

15.53 In recent years, the CIA has made moves to greater openness in its dealings with the media, in response to a political climate which demands more information and comment from intelligence agencies. The CIA maintains a Public Affairs Staff to produce public information and to deal with inquiries from the media. The Director of Public Affairs told the Commission that each year his staff receives around 2000 calls from the media and produces about 350 background briefings on issues related to the Agency itself and on developments in international affairs. The CIA has also produced a number of booklets providing information on both the US intelligence community as a whole and on the CIA itself. One of these publications, entitled A Consumer’s Guide to

---

485 Exhibit 5.7.1.1, p.3.
486 Ibid, p.20.
487 Exhibit 5.5.1, s.10.
Intelligence, describes the entire intelligence process as one of the functions of government, setting out the respective roles and functions of the various collection and assessment agencies such as the National Intelligence Council, Federal Bureau of Investigation, Defense Intelligence Agency and National Security Agency.

15.54 The CIA’s publications state clearly that the Agency collects secret intelligence. The Consumer’s Guide describes the CIA Directorate of Operations as having ‘primary responsibility for the clandestine collection of foreign intelligence’. Another publication says that the Directorate of Operations:

is a secret service with its own specialized way of recruiting, training, and maintaining networks of human agents – some might call them spies – to collect information about events and issues that threaten or might be potentially harmful to our country.

The CIA does not, however, provide any specific information about operations. The CIA maintains a policy of not commenting on allegations about the Agency, but in some cases, involving more outlandish claims, provides more information to journalists on a ‘background’ or off-the-record basis.

A new approach for ASIS

15.55 While greater publicity can impose its own pressures on an intelligence agency, there is no indication that this has impeded the operational effectiveness of ASIO or the overseas agencies. Comparisons apart, it is, we think, clear that ASIS can no longer afford to maintain a wholly passive stance in public and media relations. While the spate of disclosures may properly be regarded as exceptional, and reflective of particular grievances rather than an endemic problem, it nevertheless demonstrates, as the Minister and the Director-General have acknowledged, a clear need to rethink ASIS’s approach to the media and to public communications in general. Not only is this necessary in the interests of ASIS, but there is a wider public interest in ensuring that information which is published about ASIS is as accurate as possible.

15.56 Both the Minister and the Director-General argued that any new approach to media relations must continue to be governed by ‘a high degree of

488 Exhibit 5.7.3.4, p.7.
489 Exhibit 5.7.3.3, [p.9].
490 Exhibit 39.1, paragraph 60; Exhibit 14.3.
This, it was said, was dictated by the operational requirements of the Service. In our view, it is essential to distinguish between the attitude which the Service adopts towards the media, on the one hand, and the nature of the information which ASIS provides to the media, on the other. We see no reason why an active approach to the media cannot be combined with circumspection where necessary in the provision of information. Of course, such an approach in practice is much more complicated. The old approach has the attraction of great simplicity, in that no decisions have to be made about what can and cannot be said, since nothing at all is said. But the Service has now recognised that there are, for good reason, limits to secrecy. We are not suggesting that the Service should seek publicity, but rather that it should engage with the media and adopt a positive approach to the management of its public profile.

15.57 The challenge is to achieve a fundamental improvement in public awareness of ASIS. There is a good deal which can be stated publicly about ASIS without disclosing information which would prejudice operations or put individuals at risk. We see advantage, and no disadvantage, in public statements being made about:

(a) ASIS's functions – what it does and does not do;
(b) the public and governmental purposes which it serves;
(c) how it is controlled and to whom it is accountable;
(d) why the nature of the work requires a high degree of secrecy; and
(e) the similarities (as well as the differences) between ASIS's management and staffing arrangements and those of other government departments.

Information about the ASIS budget is already published in a one-line appropriation. Some elaboration of that, together with broad staffing information, should be considered.

15.58 The introduction and enactment of legislation for ASIS would itself enhance public knowledge in all these respects. As our draft bill indicates, the legislation should clearly define what ASIS can and cannot do, and the purposes for which it acts. It should define the key control and accountability relationships between ASIS, the Minister and the Parliament. The second

---

491 Ibid.
reading speech could be used as an opportunity to explain the importance of ASIS to Australia’s interests. We have referred elsewhere to the examples used in the British Parliament, drawn from actual operations, to demonstrate how SIS serves the national interest in the fields of counter-terrorism, counter-proliferation and the detection of drug trafficking. A number of these matters can be dealt with more systematically, more permanently and more accessibly in the form of a public booklet, which we consider below.

15.59 We see the Director-General’s role as being of particular significance. If there is to be a new approach, it will be for the Director-General to define it – in conjunction with the Minister – and to educate the staff of the Service about it. Its implementation will impose its own additional responsibilities on the Director-General. He will need to provide leadership in the development of relationships at a high level between the Service and media organisations. Such relationships would largely be conducted at an informal level but could occasionally be formal. Most media witnesses endorsed the concept of an occasional briefing of editors by the Director-General, dealing with general issues about what ASIS does and seeking to define the boundaries of what is and is not publishable, and why.

15.60 The Director-General’s role should be supported and complemented by an ASIS media liaison officer. In addition to being responsible for coordinating the Service’s public information and media relations activities, this officer would be a point of contact for journalists and editors seeking to verify information about ASIS, including allegations against the Service, received from other sources. The officer could give advice about the possible national security and intelligence implications of a proposed story, including possible threats to ASIS operations and the safety of ASIS officers and their sources. In addition the officer could be a source of general background information about ASIS.

15.61 Media representatives generally accepted that the government, and ASIS in particular, was best placed to make judgements about risk to national security. Mr Kelly agreed that an ASIS media officer could assist his organisation to make better informed decisions about publication. Mr Grant said that he would also like to be given ‘off-the-record’ background information, regretting that such information was not supplied by ASIO. According to Mr
Kohler, advice from ASIS on the risk to its operations from publication of certain information would be very useful. More information from official sources, including 'off-the-record' comment, would improve the veracity of reporting on ASIS.496

15.62 The success of an ASIS media liaison officer would hinge upon the officer's credibility with journalists and editors. This would in turn depend on what functions the officer was able to perform and how the position was used by the Service. The media would need to be confident that advice given by the liaison officer was reliable and objective. Initially at least, there would naturally be some scepticism:

The problem for the media in such a process is that ASIS would have a number of reasons for discouraging the media from publishing, such reasons not necessarily relating just to the identity of ASIS operatives or national security. So, how confident could the media be in the advice being given from ASIS? One would be inclined to think that this would be fairly self-interested advice.497

15.63 It would be necessary for the officer to demonstrate that ASIS was not interested in secrecy for its own sake or in order to conceal suspect activity. The relationship could be very quickly jeopardised if ASIS were seen to be using the officer in a manipulative or entirely 'self-interested' way. As Mr Harvey said, 'the system would fall down ... if we were ever misled intentionally'.498 Provided that credibility was established, it seems likely that there would be acceptance of a 'no comment' response where this was necessary:

If the journalist, media organisation, feels that that person is scrupulously honest, that he or she will never mislead, although on certain occasions they might say, 'Well, I can't tell you anything', but that they will not deliberately mislead, well they carry much more weight than if they are just seen as stonewallers or people who, in a tight corner, would tell you a lie.499

15.64 The other source of natural media reluctance to make use of an ASIS media liaison officer would be a concern that approaching the officer about a story on ASIS might prompt the Service to take out an injunction to prevent publication. Mr Kohler told the Commission that if ASIS were to use its media officer in this way the system would never work again.500 Clearly, there is a difficulty here. An approach to the media officer would signal an intention to

496 T*829*, *836*, *854*.
497 T*736*.
498 T*670*.
499 T*884*.
500 T*829*
publish, subject to any advice received. The officer might advise that the subject matter referred to by the journalist was sensitive and ought not to be published. If the journalist gave any indication that the advice was not likely to be followed, the media officer would have no alternative but to advise the Government which, in turn, would be bound to consider its legal options. If an injunction application were then made, the process could easily be characterised as a deceitful stratagem on the Government’s part to solicit, under the guise of an advisory service, advance notice of sensitive publications. While this difficulty should not be underestimated, we do not see it as removing the need for a source of advice within ASIS for media who are concerned to honour their commitment to the D Notice system. We have recommended in Chapter 11 that a revised D Notice should provide much fuller advice and explanation about the potential sensitivities of certain categories of information. It should be couched in such a way as to encourage editors to recognise that advice will, from time to time, be necessary.

**The policy of ‘neither confirm nor deny’**

15.65 NCND allows any claim about ASIS to go unchallenged, even where it is entirely fanciful or seriously damaging to ASIS or to Australia’s foreign relations. The Minister has faced the dilemma of determining whether to break the NCND principle and make a public denial of ‘bizarre allegations’ which have been made against the Service.\(^{501}\) We have referred to ASIS’s frustration at its inability to rebut claims made against the Service.\(^{502}\) Silence in the face of repeated assertions about ASIS can be taken by a foreign government or a sceptical public as confirmation.

15.66 There will often be circumstances, concerning operationally sensitive information or allegations, where the appropriate response from any Government will be NCND. But if this media policy is applied in a blanket fashion, it is severely limiting for the reasons we have mentioned earlier.

15.67 ASIO has adopted the practice of issuing selective denials in instances when the allegations are inflammatory and likely to cause conflict in the wider Australian community. The Director-General of Security cited the Organisation’s denial of allegations about purported ASIO operations within the Macedonian and Aboriginal communities.\(^{503}\)

\(^{501}\) T2465.
\(^{502}\) T49.
\(^{503}\) T2604-7.
The disadvantage of selective denials, as advanced to us, is that they tend to undermine NCND in the long term. Senator Evans was opposed to issuing individual denials under ‘the pressure of the moment’, because it weakens the principle as a whole. If one allegation is denied and another is not, a close observer could infer that the unrebuted allegation is true. In the case of the wilder accusations about ASIO which occur in the midst of passing domestic political controversy, this is probably not a concern. Denials by the Australian Government about foreign intelligence could, however, provide information to a watchful overseas intelligence agency. It is even possible that claims could be made in the media in the hope of obtaining a denial and thus allowing information about ASIS operations to be gleaned by a process of elimination.

A carefully chosen forms of words and presentation can convey the message that the allegation is too outrageous to be taken seriously. Such an approach may enable the NCND principle to be maintained while allowing the more incredible accusations to be dismissed. The possibility of such an approach was acknowledged by the Minister.

A modified approach to NCND should be possible if, as we recommend, the amount of information on the public record about ASIS and its activities is increased. The legislation we propose will be the key point of reference. Its enactment should enable the Minister, for example, to dismiss out of hand allegations of outrageous behaviour by ASIS such as those made by Ms Holland. The Minister would be able to point to the sections of the Act defining and limiting the functions of ASIS and to the arrangements for oversight, in declaring that ASIS is not authorised to behave in such a fashion and could not possibly do so without detection. This points to the need for a coherent public information strategy, to which we now turn.

A public information strategy

The Service recognises that one of the key factors allowing uninformed speculation about ASIS activities to go unchecked is the absence of any information on the public record about the control and accountability structure. Early in the Inquiry, the Director-General identified this as a problem to be remedied and proposed the development of a public booklet explaining what ASIS does and describing the arrangements for control and accountability. A

504 T2466.
505 Ibid.
506 T46; T524.
draft public booklet was subsequently prepared and submitted in conjunction with ASIS’s proposal for legislation.\textsuperscript{507}

15.72 ASIS believes that a booklet of this kind will help to ‘reassure the public that ASIS is an adequately controlled and accountable organisation’ and enable it counter allegations against it.\textsuperscript{508} As well as describing the elements of the control and accountability framework, it is envisaged that such a booklet would describe the origins and development of ASIS, its role and function in government, what it does and does not do and the kinds of people who work for ASIS.

15.73 Such a booklet would, we believe, make an important contribution towards filling the information gap. The booklet should lay particular emphasis on the value of ASIS’s work to Australia. There are, quite properly, concerns in the community about the role of intelligence and security agencies in the post-Cold War environment. ASIS can point to the strong endorsements of its ongoing role by the Richardson and Hollway reviews, and the continuous assessment of the value of its product by the assessment agencies, ONA and DIO. The booklet could give examples of ASIS operations, suitably sanitised, to illustrate the benefit of ASIS’s work to Australia’s national security and economy, and its contribution to the international effort in support of peace-keeping and against threats such as weapons proliferation, terrorism, illegal drugs traffic and organised crime. All of this can, we think, be achieved without disclosing any operational information.

15.74 The revised draft booklet submitted by ASIS with its final submission is a good starting-point.\textsuperscript{509} It will need refinement, in particular in the light of the decisions which the Government makes on our recommendations for legislation, parliamentary oversight, the role of IGIS and other related areas.

15.75 Consideration should also be given to the issuing of a publication on the intelligence community as a whole. It should describe the functions of the various agencies and the arrangements by which they are controlled. It would provide the opportunity, for example, to emphasise the often misunderstood distinction between the internal role of ASIO and the external role of ASIS. Such a publication, published by ONA or by the Prime Minister’s Department, would reinforce the message that ASIS and the other intelligence agencies are part of the

\textsuperscript{507} Exhibit 6.2.1, Attachment G.
\textsuperscript{508} Exhibit 6.2.1, paragraph 29.
\textsuperscript{509} Exhibit 45.2.12.
ordinary machinery of government and exist within clearly established lines of control and accountability. The recently-published British booklet entitled *The Central Intelligence Machinery* provides a useful reference point.

15.76 A public information program might extend to the publication of an official history of ASIS. A history of the Service was commissioned as part of the work of the first Hope Royal Commission. An edited version was appended to the fifth report of that body but never released publicly. It could be used as the basis for a substantial monograph, supplemented by a study of the period since 1976. The Commission received submissions supporting such a history.\(^{510}\)

**Conclusion**

15.77 The picture of ASIS which is presented to the Australian public should, as nearly as possible, resemble the true position. It seems to us to be self-evident that the persistence of an image of ASIS based on untruths and half-truths is contrary to the public interest. Within the constraints of secrecy which we have discussed in detail elsewhere, the Australian public should know what their foreign intelligence service is and is not doing in their name and on their behalf. We also think it very much in the interests of the Service that this should occur.

15.78 The essence of the strategy which we recommend is that as much information as possible about ASIS should be on the public record. As we have said, the foundation of this is the legislation we recommend. It will confer legislative authority on the Service and establish a mechanism for parliamentary oversight. The public information booklet should be a simply-expressed document, reinforcing the legislation, which can be used to communicate what ASIS does and why. It should place particular emphasis on the uses to which ASIS product is put, in the service of the national interest.

15.79 ASIS should ensure that public attention is drawn to relevant reports of the proposed parliamentary committee, of the Inspector-General, and of the Auditor-General in the event that full external audit coverage is achieved as we recommend. Such references will no doubt draw attention to positive comment

\(^{510}\) Dr Gregory Pemberton of Macquarie University believed that 'a limited history of ASIS' sponsored by the government would be preferable to the 'more sensationalist and speculative accounts' which emerge in an environment of official secrecy, an argument almost identical to that used by ASIS to support the publication of a booklet. (Exhibit 46.2, p.3). Mr David McKnight of the University of Technology, Sydney, also supported the idea, along with a liberalised archives policy, as an aspect of the accountability of the Service. (Exhibit 46.1, p.2).
about the Service but will also serve to remind the public of the many levels of oversight of ASIS.

15.80 The Director-General and the proposed media liaison officer need to work to build relationships with the media. These relationships will be enhanced by the ability to refer to the legislation and the booklet and the reports of those other agencies. If the blanket of secrecy is lifted in all these different ways, it should become much more possible – and credible – for the Service and the Minister to deny obviously false assertions of the kind we have described in this chapter.
Appendix A

Letters Patent
COMMONWEALTH OF AUSTRALIA

ELIZABETH THE SECOND, by the Grace of God Queen of Australia and Her other Realms and Territories, Head of the Commonwealth:

TO:

THE HONOURABLE GORDON JACOB SAMUELS AC QC

GREETING:

WHEREAS it is desired to have an inquiry into matters relating to the Australian Secret Intelligence Service:

NOW THEREFORE We do by these Our Letters Patent issued in Our name by Our Governor-General of the Commonwealth of Australia on the advice of the Federal Executive Council and in pursuance of the Constitution of the Commonwealth of Australia, the Royal Commissions Act 1902 and other enabling powers, appoint you to be a Commissioner to inquire into:

(a) the effectiveness and suitability of existing arrangements for:
   (i) the control and accountability of the Service;
   (ii) the organisation and management of the Service;
   (iii) the protection of the Service's intelligence sources and methods;
   (iv) the resolution of grievances and complaints relating to the Service; and

(b) whether any changes in existing arrangements are required or are desirable:
AND We direct you to produce with Michael Henry Codd AC a single report of the results of your inquiries and his inquiries under the relevant Commission:

AND We further direct you to consult with Michael Henry Codd with regard to the methods and procedures to be followed in relation to his and your inquiries and concerning the content and preparation of that report:

AND We authorise you in the conduct of your inquiry to have regard to any information, evidence, document or thing communicated or furnished to you by Michael Henry Codd under the relevant Commission:

AND We declare that in these Our Letters Patent, the expression "relevant Commission" means the Commission of inquiry issued this day by Our Governor-General of the Commonwealth of Australia by Letters Patent to Michael Henry Codd:

AND We require you as expeditiously as practicable to make your inquiry and, not later than 31 December 1994, to furnish to Our Governor-General of the Commonwealth of Australia the report of the results of the inquiries and such recommendations as you consider appropriate.

WITNESS the Honourable William George Hayden, Companion of the Order of Australia, Governor-General of the Commonwealth of Australia on 15 March 199

By His Excellency's Command,

Minister for Foreign Affairs
for the Prime Minister
COMMONWEALTH OF AUSTRALIA

ELIZABETH THE SECOND, by the Grace of God Queen of Australia and Her other Realms and Territories, Head of the Commonwealth:

TO:

MICHAEL HENRY CODD AC

GREETING:

WHEREAS it is desired to have an inquiry into matters relating to the Australian Secret Intelligence Service:

NOW THEREFORE We do by these Our Letters Patent issued in Our name by Our Governor-General of the Commonwealth of Australia on the advice of the Federal Executive Council and in pursuance of the Constitution of the Commonwealth of Australia, the Royal Commissions Act 1902 and other enacting powers, appoint you to be a Commissioner to inquire into:

(a) the effectiveness and suitability of existing arrangements for:
   (i) the control and accountability of the Service;
   (ii) the organisation and management of the Service;
   (iii) the protection of the Service's intelligence sources and methods;
   (iv) the resolution of grievances and complaints relating to the Service; and
(b) whether any changes in existing arrangements are required or are desirable:

200
AND We direct you to produce with the Honourable Gordon Jacob Samuels AC QC a single report of the results of your inquiries and his inquiries under the relevant Commission:

AND We further direct you to consult with the Honourable Gordon Jacob Samuels with regard to the methods and procedures to be followed in relation to his and your inquiries and concerning the content and preparation of that report:

AND We further direct you, in conducting your inquiry and preparing the report, to take account of any views of the Honourable Gordon Jacob Samuels concerning how those inquiries are to be conducted and that report prepared:

AND We authorise you in the conduct of your inquiry to have regard to any information, evidence, document or thing communicated or furnished to you by the Honourable Gordon Jacob Samuels under the relevant Commission:

AND We declare that in these Our Letters Patent, the expression "relevant Commission" means the Commission of inquiry issued this day by Our Governor-General of the Commonwealth of Australia by Letters Patent to the Honourable Gordon Jacob Samuels:

AND We require you as expeditiously as practicable to make your inquiry and, not later than 31 December 1994, to furnish to Our Governor-General of the Commonwealth of Australia the report of the results of the inquiries and such recommendations as you consider appropriate.

WITNESS the Honourable William George Hayden, Companion of the Order of Australia, Governor-General of the Commonwealth of Australia on 15-3-91.

[Signature]
Governor-General

By His Excellency's Command,

[Signature]
Minister for Foreign Affairs for the Prime Minister
COMMONWEALTH OF AUSTRALIA

ELIZABETH THE SECOND, by the Grace of God, Queen of Australia and Her other Realms and Territories, Head of the Commonwealth:

TO:

THE HONOURABLE GORDON JACOB SAMUELS AC QC

GREETING:

WHEREAS by Letters Patent issued in Our name by Our Governor-General of the Commonwealth of Australia on 15 March 1994 We appointed you to be a Commissioner to inquire into and report upon the Australian Secret Intelligence Service:

AND WHEREAS it is desirable that those Letters Patent be varied in certain respects:

NOW THEREFORE We do, by these Our Letters Patent issued in Our name by Our Governor-General of the Commonwealth of Australia on the advice of the Federal Executive Council and pursuant to the Constitution of the Commonwealth of Australia, the Royal Commissions Act 1902 and every other enabling power, declare that the Letters Patent issued on 15 March 1994 shall have effect on and from 20 December 1994 as if the words "not later than 3 March 1995" were substituted for the words "not later than 31 December 1994".

WITNESS the Honourable William George Hayden
Companion of the Order of Australia
Governor-General of the Commonwealth of Australia on 20-12-94

Governor-General

By His Excellency's Command,

Minister for Foreign Affairs for the Prime Minister
COMMONWEALTH OF AUSTRALIA

ELIZABETH THE SECOND, by the Grace of God, Queen of Australia and Her other Realms and Territories, Head of the Commonwealth:

TO:

MR MICHAEL HENRY CODD AC

GREETING:

WHEREAS by Letters Patent issued in Our name by Our Governor-General of the Commonwealth of Australia on 15 March 1994 We appointed you to be a Commissioner to inquire into and report upon the Australian Secret Intelligence Service:

AND WHEREAS it is desirable that those Letters Patent be varied in certain respects:

NOW THEREFORE We do, by these Our Letters Patent issued in Our name by Our Governor-General of the Commonwealth of Australia on the advice of the Federal Executive Council and pursuant to the Constitution of the Commonwealth of Australia, the Royal Commissions Act 1902 and every other enabling power, declare that the Letters Patent issued on 15 March 1994 shall have effect on and from 20 December 1994 as if the words "not later than 31 March 1995" were substituted for the words "not later than 31 December 1994".

WITNESS the Honourable William George Hayden, Companion of the Order of Australia, Governor-General of the Commonwealth of Australia on 20-12-94

Governor-General

By His Excellency's Command,

Minister for Foreign Affairs
for the Prime Minister