Intelligence and Security Committee

Annual Report 1997-98

Chairman:
The Rt Hon Tom King CH MP

Intelligence Services Act 1994
Chapter 13

Presented to Parliament by the Prime Minister
by Command of Her Majesty
OCTOBER 1998

Cm 4073

£8.65

From the Chairman: the Rt. Hon. Tom King, C.H., M.P.

INTELLIGENCE AND SECURITY COMMITTEE

70 Whitehall
London SW1A 3AS

31 July 1998

ISC 670

The Rt. Hon. Tony Blair, M.P.
Prime Minister
10 Downing Street
London SW1A 2AA

Dear Prime Minister,

I enclose the third Annual Report of the Intelligence and Security Committee on the discharge of our functions under the Intelligence Services Act 1994. Subject to any consultation with the Committee as provided for in section 10(7) of the Act, we hope that it will be possible for you to lay our Report before each House of Parliament at an early date.

Yours sincerely,

TOM KING

INTELLIGENCE AND SECURITY COMMITTEE

The Rt. Hon. Tom King, CH, MP (Chairman)

The Rt. Hon. Lord Archer of Sandwell, QC	Ms Yvette Cooper, MP
Mr Kevin Barron, MP	Mr Barry Jones, MP
The Rt. Hon. Alan Beith, MP	Mr Michael Mates, MP
Mr Dale Campbell-Savours, MP	Mr Allan Rogers, MP

For more than 40 years, the United Kingdom and its NATO allies endured the threatening environment of the Cold War. The genuine menace of an aggressive world power, seeking to subvert and dominate Europe and the wider world, gave abundant justification for substantial defence, intelligence and security structures. In this climate, the case for foreign intelligence and internal security was generally accepted.

It has been said that the public view of intelligence owes more to fiction than to fact. In the UK, with the popularity of Fleming and Le Carré, there has been no shortage of fiction, but there has been a steady supply of facts as well, with a sequence of notorious defections and spy scandals. These raised many suspicions that all was far from well in our intelligence and security services. At the same time, they served to reinforce in the public mind that the country was under threat, and that we needed those same services to protect us.

This recognition of the need for intelligence and security was not, however, accompanied by any great understanding or knowledge of what the Agencies actually did. By their nature, they have not been exposed to detailed public examination, or close scrutiny by the media. Indeed, until only recently the very existence of the Secret Intelligence Service (SIS) and the Security Service was not admitted, with the costs of providing their new headquarters concealed in the Foreign Office and Ministry of Defence budgets. After nearly 90 years in operation, it is only in the last four that the Government has admitted to the existence of SIS, and Parliament has given SIS and Government Communications Headquarters (GCHQ) a statutory legal basis within the Intelligence Services Act 1994.

The public declaration of the existence of the Agencies brought with it the issue of democratic accountability for their activities. In the same Intelligence Services Act that formally established SIS, this Committee was created to oversee SIS, the Security Service and GCHQ. It is a Committee of Parliamentarians, but not of Parliament, appointed by the Prime Minister, reporting to him, and through him to Parliament, and operating within the 'ring of secrecy'.

This new oversight committee came into being at a significant time. With the ending of the Cold War and the disappearance of the threat that had been seen as the main justification of the Agencies' existence, many more questions have rightly been asked

about them: do we still need them? Do we still need so much of them? Could they be reduced or amalgamated? Can you still justify their methods of operation in a world now free of Cold War threats?

The work of the Agencies was necessarily dominated by the need to counter the Soviet threat. When that reduced so dramatically, there was a common assumption that the need for intelligence and security would likewise shrink. That has not happened, and most recently the Government's Review has proposed little change for the future years in the overall scale of resources for the Agencies. Their critics will say that the Agencies have simply invented new threats to justify their existence. Is this true, or is it not truer to say that the world remains, in a host of different and much less predictable ways, a dangerous place? Was not the Cold War, in its awful way, a form of rigid security system that has now collapsed, and have not new developments and technology and 'globalisation' produced their own dangers?

The dust had barely settled from the sudden fall of the Berlin Wall, and the collapse of the Soviet Union and the Warsaw Pact, before Iraq's invasion of Kuwait and the collapse of Yugoslavia created new situations of profound concern for us, and new challenges for intelligence. The Government's Strategic Defence Review lays greater emphasis on expeditionary forces and speed of dispatch. Moving British forces on humanitarian or peace-keeping missions into dangerous and untested territory requires the best possible intelligence on the local situation, and a close watch on what may be rapid and threatening changes in very volatile circumstances. Britain's involvement in such activities has also resulted in new terrorist threats to British interests.

In recent years there has been a growth in serious organised crime, funded significantly by the world-wide trade in drugs. The collapse of the Soviet Union and the removal of barriers to travel from those countries let loose dangerous new criminal groups, often including ex-members of the KGB and other intelligence and security services. They have a substantial involvement in drugs and money laundering and, increasingly, in the traffic in illegal immigrants which is now a major concern in all European countries.

The risk of the proliferation of weapons of mass destruction, nuclear, chemical or biological, had long been recognised as a serious threat. In the post-Cold War environment, that risk has sharply increased, and countering it is now one of the biggest single tasks of SIS.

In recent years, terrorist attacks of all kinds world-wide have averaged almost 60 a month. In the UK, we have all too long an experience of terrorism. Elsewhere, there is increasing concern over Islamic terrorist threats. Whilst we may not have been so affected ourselves by these groups, some of them have used Britain as their base to raise funds and equipment and recruit new members. We have been significantly helped by many other countries in countering Irish terrorism, and we have a clear duty to help them in return.

The alarm over the Millennium Bug has vividly demonstrated how dependent our whole society now is on computer systems. Their security is vital to our lives, and a proper awareness of the opportunities and risks of 'information warfare' is essential. Some recent reports of individual hackers intruding into major defence installations may seem harmless incidents. Pursued on a systematic basis, and with hostile intent, they could have devastating impact.

These are illustrations of new challenges that our intelligence and security services now face. So far from being invented to justify the Agencies' continued existence, they are real enough, and the country rightly expects to be protected against them. Moreover, intelligence and security capabilities cannot be turned on and off like a tap. To meet their responsibilities, they must be maintained, and funded in a sustainable way.

However, the Agencies face these tasks in a new environment of greater openness and accountability. They also face them with new technologies available to bring new capacities for the collection of information in many forms, which may pose new challenges to ensuring that the privacy of law-abiding individuals is respected.

Overall, it is vital that public confidence is maintained in the Agencies. At times of grave national threat, their value is readily accepted. At other times, in the face of a bungled operation or security lapse, public confidence can be very fragile. That is the inevitable consequence of operating within the 'ring of secrecy', which prevents a more balanced public view of their activities and their value. The public must therefore be confident that there is adequate independent scrutiny and democratic accountability on their behalf, by people within that 'ring of secrecy'.

That is the task of this Committee.

INTELLIGENCE AND SECURITY COMMITTEE

Annual Report 1997-98

Contents

Glossary

BfV	Bundesamt fur Verfassungsschutz (German internal security service)
BND	Bundesnachrichtendienst (German foreign intelligence service)
C&AG	Comptroller and Auditor-General
CDI	Chief of Defence Intelligence
CESG	Communications Electronics Security Group, GCHQ
CESIS	Italian intelligence co-ordination body
CIA	Central Intelligence Agency (US)
CSE	Communications Security Establishment (Canadian GCHQ equivalent)
CSI	Ministerial Committee on the Intelligence Services
CSIS	Canadian Security Intelligence Service (Canadian internal security service)
DCI	Director of Central Intelligence (US)
DGSE	Direction Generale de la Securite Exterieure (French foreign intelligence service)
DIS	Defence Intelligence Staff, MOD
DRM	Direction du Renseignement Militaire (French DIS equivalent)
DST	Direction de la Surveillance du Territoire (French internal security service)
FBI	Federal Bureau of Investigation (US)
FISA	Foreign Intelligence Surveillance Act (US)
GAE	General Administrative Expenditure
GAO	General Accounting Office (US)
GCHQ	Government Communications Headquarters
IG	Inspector-General of intelligence and security services (US, Canada, Australia etc)
INR	Bureau of Intelligence and Research, State Department (US)
IOB	Intelligence Oversight Board (US)
IOCA	Interception of Communications Act 1985

ISA	Intelligence Services Act 1994
IT	Information Technology
JIC	Joint Intelligence Committee
MOD	Ministry of Defence
MRP	Security Service Manual of Recording Policy
NAO	National Audit Office
NATO	North Atlantic Treaty Organisation
NCIS	National Criminal Intelligence Service
NSA	National Security Agency (US GCHQ equivalent)
OCE	Other Current Expenditure
PES	Public Expenditure Survey
PFI	Private Finance Initiative
PFIAB	President's Foreign Intelligence Advisory Board (US)
PSIS	Permanent Secretaries' Committee on the Intelligence Services
RG	Renseignements Generaux (French internal police/security service)
SGDN	Secretariat General de la Defense Nationale (French co-ordinating body on national defence and security matters)
SIRC	Security Intelligence Review Committee (Canadian oversight body)
SIS	Secret Intelligence Service
SISDE	Italian internal security service
SISMI	Italian military intelligence service
SIV	Single Intelligence Vote
SIVR	Single Intelligence Vote Review
SO(SSPP)	Sub-committee of the Official Committee on Security, on Security Service Priorities and Performance
VX	SIS, Vauxhall Cross

Introduction

1. The Intelligence and Security Committee is established under the Intelligence Services Act 1994 to examine the expenditure, administration and policy of the United Kingdom's three Intelligence and Security Agencies: SIS, GCHQ and the Security Service. Committee members are notified under the Official Secrets Act 1989 and operate within the 'ring of secrecy'. We report directly to you on our work, and through you to Parliament.

2. Since our appointment at the end of July last year, we have met formally on 30 occasions – once a week while Parliament is sitting, and more frequently on occasion – and taken evidence from 26 separate witnesses. A full list of those who have given evidence is at Appendix 1 to this Report; these included:

- the Foreign and Home Secretaries;
- the Heads of SIS, GCHQ and the Security Service, and a number of their staff;
- officials from the Foreign and Commonwealth Office, the Home Office and the National Audit Office.

3. In addition to formal evidence-taking sessions, we had two briefings from the Chief of Defence Intelligence (CDI) and officers of the Defence Intelligence Staff (DIS). Since this Committee started work four years ago, we have made it our practice to be briefed on the activities of the DIS, which is a key element in the UK intelligence community and has an extremely close relationship with the Agencies, particularly as the principal customer of GCHQ.

4. We have again conducted a series of visits by 'sub-groups' of the main Committee to the three Agencies and their out-stations. This year, the sub-groups have concentrated on issues being pursued in formal Committee inquiries, including those of personnel management and personal files, meeting a broad of range of staff involved at all levels.

5. Part of our work also includes reviewing co-operation with this country's allies in the intelligence and security field. The Committee therefore conducted three working trips overseas – to the United States and Canada in March; Germany in May, and France and Italy in June/July – to discuss intelligence links and security co-operation with the United Kingdom, and comparative oversight arrangements. A full list of those we met is at Appendix 2 to this Report.

6. During the course of the year, we were again pleased to receive officials and Parliamentarians interested in the field of oversight from a number of other countries, including Australia, Belgium, Canada, Germany, Hungary, Italy, Latvia, Norway, Romania, Sweden and the United States.

Programme of Work

7. On our appointment, we made clear our intention to pursue a number of existing inquiries, including into:

- the Agencies' internal security policies and procedures, their policies and practices on personal records, recruitment and personnel management. These were areas where the Committee had previously had concerns. Particularly in respect of internal security, we wondered whether arrangements were as good as they should be;
- the continuing risks from Irish terrorism; and
- the arrangements for co-ordination between the Security Service and the law enforcement organisations in respect of serious organised crime.

8. We have also considered a number of other intelligence and security matters which are relevant to our remit. In particular, we have been taking a close interest in GCHQ's new accommodation project under the Private Finance Initiative, where a decision on the preferred bidder and the new arrangements is to be made in October. **These decisions on accommodation and location are the most fundamental that GCHQ has faced since its original move from Bletchley Park. In this connection, the rapid series of changes of Director has not been helpful. The new Director is the fourth within two years, and finds himself faced with immediate decisions on these critical issues. The challenge of ensuring no interruption to operating capabilities during this reorganisation is a daunting one, which will demand the highest levels of management skill.**

9. We have also taken some evidence on questions of intelligence policy arising from recent events in Sierra Leone[1]. **We agreed to suspend further inquiries pending publication of the Legg Report. This has now been received, and we shall be considering these matters further.**

The Agencies' Priorities, Plans and Finances

10. The annual presentations to the Committee by each of the Agency Heads on performance, current priorities, future plans and finances took place in the early Spring of this year[2]. To ensure that we are kept fully informed on the full range of the Agencies' activities, we have since agreed on an additional programme of more frequent briefings for the Committee on the Agencies' priorities, successes and problems.

---

1. *Evidence from the Chief of SIS, May 1998. Evidence from the Director of GCHQ, June 1998.*
2. *Evidence from the Chief of SIS, February 1998. Evidence from the Director of GCHQ, February and March 1998. Evidence from the Director-General of the Security Service, February and March 1998.*

11. The Committee's last two Annual Reports[3] described the shifts in the Agencies' effort that followed the ending of the Cold War, reflecting new intelligence requirements on a wide range of threats to, and opportunities for, British interests. This year, the annual presentations took place against a backdrop of the review of the Single Intelligence Vote (SIVR), as part of the Government's Comprehensive Spending Review. That Review examined current levels of expenditure devoted to the Agencies, and addressed a number of other questions including whether the work of the Agencies was focused on the right priorities in the national interest, or whether there should be any change in focus. The intelligence requirements process, therefore, was effectively frozen whilst the review was carried out, as – in many areas – were the Agencies' own allocations of operational resources, for planning purposes at least. We identified, however, a number of significant changes in the allocation of operational resources since the last Report by the Committee was submitted in December 1996[4].

SIS and GCHQ

12. ***
***
*** [5, 6, 7]

13. **Another important change over the past year has been the raising of the priority of work against drugs trafficking to the First Order of Importance, and the effect this has had on the Agencies' work in this area.** SIS devotes *** of operational effort to this task, a figure, on the face of it, unchanged over the past few years. The Chief of SIS told us, however, that what had changed was that the Agency was now concentrating its efforts as far as possible on "going up the supply chain", and has sought and got other departmental sponsorship and funding for "major projects, strategically done, against suppliers"[8]. Director GCHQ also told us of a recent growth in this area of work, reflected in a significant rise in the number of requests by the law enforcement agencies to take action on sigint reports on these subjects[9]. **The drug threat is a major menace to this country. We strongly support the increased priority being given to this work by our intelligence services, and we shall continue to take a close interest in this area.**

---

3. *Cm 3198, March 1996. Cm 3574, February 1997.*
4. *Cm 3574, February 1997.*
5. *Evidence from SIS, February 1998.*
6. *Evidence from the Chief of SIS, February 1998.*
7. *Evidence from the Foreign Secretary, February 1998.*
8. *Evidence from the Chief of SIS, February 1998.*
9. *Evidence from the Director of GCHQ, February 1998.*

14. **We also questioned the Agencies closely on *** work on Iraq, and the extent of intelligence sharing with *** principal allies on this issue[10]. *** We accept these assurances, and the evidence we were given *****

15. The percentages of GCHQ sigint resources for the priorities above are:

***

***[11]

The Security Service

16. **For the Security Service, the renewed ceasefires in Northern Ireland led directly to a drop of over 5% in the Service allocation of resources to Irish and domestic counter-terrorism work, from 24.8% to an anticipated 19.5% during the course of the year**[12]. We took detailed evidence from the Director-General of the Service specifically on work in this area, including the Service's key role in operations AIRLINES and TINNITUS which resulted in the convictions of some of the most important terrorists in the Provisional IRA. In the first case, 40 Security Service staff gave witness statements, in the second, around 200 – though, in the event, none were called to give evidence[13]. This is a graphic illustration of the scale of the resources involved in combating the terrorist threat. **Despite the cease fire and the Good Friday agreement, there are clearly still elements in Northern Ireland who are intent on using terrorism to further their political aims. We strongly support the vital work done by the security forces in countering this threat, and accept that considerable resources will continue to need to be devoted to this work.**

17. **There were also some increases in resources devoted to work against the other threats from international terrorism, at 16.4% and proliferation, espionage and serious organised crime, which together comprise 19.1%**[14]. In the latter respect, we have not had an opportunity during the year to take a detailed look into the arrangements for the operational co-ordination of the Security Service and the law enforcement agencies in this area. The Director-General did, however, tell us that the Service had taken on 24 taskings – from NCIS, the Regional Crime Squads, the Metropolitan Police, provincial forces and HM Customs and Excise – since October 1996, when the new arrangements came into effect. Six of these taskings had been successfully completed, and the Service had issued around 1,000 reports in respect of the investigations in which it was involved[15].

---

10. Evidence from the Chief of SIS, February 1998.

11. Evidence from GCHQ, February 1998.

12. Evidence from the Security Service, January 1998.

13. Evidence from the Director-General of the Security Service, February 1998.

14. Evidence from the Security Service, January 1998.

15. Evidence from the Director-General of the Security Service, February 1998.

We intend to return to this subject in the autumn, to take further evidence in particular on what value is added by the Service's involvement in this new area.

Expenditure

18. As part of the annual presentations, we continued the Committee's previous practice of examining in detail the Agencies' individual budgets and expenditure. In this, we were again aided by valuable advice from senior staff from the National Audit Office. This year we sought more information from the Agencies, and also sought to improve the form in which it was presented. **The new forms, attached at Appendix 3 to this Report, have greatly helped the Committee in its understanding of the Agencies' finances. We were told that they have also been of value to the NAO[16]. Ministers may also wish to have financial information presented in this way, in their own considerations of the Agencies' budgets.**

19. The Single Intelligence Vote (SIV) outturn totals for 1994/95-1996/97, the expected outturn for 1997/98, and the budgets for 1998/99-2001/2002, are shown in the table below[17]. Figures for the individual Agency budgets are not at present published. The Committee believes that the fullest information should be published wherever possible, and will be discussing further whether there could be greater openness in this area.

All figures £m (Cash)

	SIS	GCHQ	Security Service	SIV TOTAL
1994/95	***	***	***	855.1
1995/96	***	***	***	780.8
1996/97	***	***	***	740.7
1997/98	***	***	***	707.8
1998/99	***	***	***	693.7
1999/2000	***	***	***	743.2
2000/2001	***	***	***	745.0
2001/2002	***	***	***	746.9

Notes:

1. *These figures exclude the costs of the SIS and Security Service pension schemes.*
2. *'Exceptional' costs associated with the moves of SIS and the Security Service into Vauxhall Cross and Thames House respectively are included in the earlier years.*
3. *Figures for 1998/99 onwards show a net reduction of around £15m, reflecting accounting adjustments with the introduction of capital charging for property.*

20. We were fully briefed on the Agencies' future plans in the course of the annual presentations. However, since then there has been the Review of the SIV, the outcome of

16. *Evidence from the National Audit Office, April 1998.*
17. *Evidence from the Cabinet Office, July 1998.*

which is shown above in the figures for the years 1999/2000-2001/2002, which were provided to us just prior to submission of this Report. **On our return in the autumn, we shall be examining the detail of the settlement and the full range of issues covered in the Review, taking evidence from the Agency Heads and others who were directly involved in the process.** At the start of this year, early in the review process, we sought a meeting with those responsible for the Review to discuss its remit, and to highlight certain areas that we believed merited particular consideration, including: structural questions on the organisation of the UK intelligence community, and the importance of giving wider consideration to the work of the Defence Intelligence Staff (DIS) in the MOD. **In this latter regard, we shall also be concerned to examine any changes proposed in the funding and structure of the DIS as a result of the Government's Strategic Defence Review, and the implications that these may also have for work of the Agencies.**

The work of the National Audit Office

21. In our work on the Agencies' budgets, we are concerned to ensure that each has access to adequate resources for the tasks they are asked to undertake, and that those resources are being used in a cost-effective way. The external auditing function, however, falls to the NAO which, because of the particular sensitivities in this area, reports directly to the Chairman of the Public Accounts Committee in the House of Commons. This is an important arm of the intelligence oversight structure outside the executive, and we have given some consideration to the practical nature of that department's role in this respect, and the extent of its access to the Agencies' information. We were told, for example, that **no value for money project work in respect of the Agencies had been carried out over the past few years[18]; our own view is that it would be desirable where practicable to carry out further studies into all aspects of the Agencies' activities, and we will be pursuing this issue with the auditors.**

22. We have examined in some detail the Ministerially-approved arrangements for the disclosure of information by each of the Agencies to the Comptroller and Auditor-General (C&AG)[19]. These include certain restrictions to protect the identities of agents and the details of particularly sensitive operations, where the withholding of information would in each case require the approval of the relevant Secretary of State. We were told, however, that the NAO could foresee no requirement for access to information on individual agent identities, and that it had never been refused access to any other sensitive operational information on request. We questioned the NAO in particular on the implications of the recent fraud case in the Metropolitan Police, when the single person responsible for the secret funds for paying agents had fraudulently appropriated very substantial sums of money. **They had identified the**

18. *Evidence from the National Audit Office, April 1998.*

19. *Evidence from the Foreign and Commonwealth Office, February 1998. Evidence from the Home Office, March 1998.*

problem, and believed that adequate checks could be operated to prevent such fraud without direct approaches to individual agents[20].

23. **On the evidence we have taken, it is clear that the auditors believe that they have access to all the necessary information they require from each of the Agencies to enable them to carry out their functions effectively. We nevertheless believe that the procedures for the disclosure of information should be further strengthened in the following respects:**

- there should be a specific obligation on the Agencies to inform the NAO of material items of expenditure;
- the arrangements for the disclosure of information by SIS, approved by the Foreign and Commonwealth Secretary, should be brought as far as possible into line with those for the Security Service, specifically in providing for the C&AG to be given the reasons for any refusal to provide him with information;
- in view of our own statutory responsibility to examine the Agencies' expenditure, formal provision should also be made for the disclosure of information and reports by the C&AG to this Committee, in consultation with the Chairman of the House of Commons Public Accounts Committee.

The Agencies' Internal Security Policies and Procedures

24. In the last Parliament, the Committee stressed that continuing importance needed to be attached to the operation of a range of effective security procedures within the Agencies[21]. At that time, it focused in particular on aspects of personnel security and the vetting processes, and highlighted a number of areas where they believed there was room for significant improvement in the Agencies' application of those procedures. These areas included financial investigations as part of the vetting process; the frequency and nature of vetting reviews; and physical searches of Agency staff entering and leaving their offices. On our appointment, we sought early information from each of the Agencies on internal security measures they may already have taken, or planned to take, in the light both of this Committee's earlier concerns and the more recent experiences in both this country and the United States.

25. The Security Service, which has a lead advisory role to Government on protective security measures, gave us evidence that they had established a Penetration Risk Assessment Group to "give fresh impetus" to countering the continuing risks of penetration by foreign intelligence services, and also the risks associated with staff exposure to corruption and intimidation by criminals in the course of the Service's new work against serious organised crime. We were told that the group was focusing, in

20. *Evidence from the National Audit Office. April 1998.*

21. *Cm 3574, February 1997, paragraphs 12-16.*

consultation with the other two Agencies, on a range of vetting and personnel security measures; on controls on the handling of and access to – sensitive information, and on increased and more effective security training and security awareness among staff[22].

26. In addition, each of the Agencies told us of a series of security measures they had recently taken, or had under active consideration[23]. These included:

- the collection of more detailed financial information as part of the vetting process (and the less detailed annual security appraisals completed by all staff and their line managers), to provide more detail in particular on the sources of income of staff, and the balance between income and expenditure;
- retaining five-year cycles or less for vetting reviews, even though the 1993 Review of Protective Security recommended that the normal review period could now be seven years;
- increasing the number of such reviews carried out at random intervals, and broadening the range of character referees interviewed as part of the process;
- increases in the number of random searches of staff entering and leaving Agency buildings: the Security Service, for example, has increased such searches by 25-30% on the 1996 figures;
- more stringent security checks on those leaving employment, particularly those resigning or taking early retirement, and exploring better ways of keeping in touch with staff who may be of security concern once they have left; and
- improved mechanisms to control access to IT systems holding sensitive data, and more effective auditing tools to ensure the strict application of the 'need-to-know' principle.

27. Other measures also under consideration included the involvement of clinical psychologists in the vetting process, to help identify actual or potential personality disorders, and more stringent controls on appointments to particularly sensitive posts.

28. **We have not yet had a chance to take detailed evidence on the measures outlined above, which look to be valuable enhancements to the current range of our security defences and seem to go some way towards addressing the concerns of the Committee**. In light of highly publicised instances of the difficulties the Agencies have encountered over the handling of disaffected staff, we have, however, inquired into the procedures and the problems encountered in this respect. We comment on this elsewhere in this Report[24].

22. *Evidence from the Security Service, October 1997.*

23. *Evidence from SIS, October 1997. Evidence from GCHQ, October 1997. Evidence from the Security Service, October 1997.*

24. *See paragraphs 33-38, and Appendix 4.*

29. **We will continue to give high priority to investigating and challenging the Agencies on their security procedures, and to questioning others in Government with responsibilities in this area**. In our inquiries, we shall be concerned to see whether, in the measures they have adopted, the Agencies have struck an appropriate balance between the need to protect their information and operations, and the individual's right to reasonable personal privacy. **We will report further to you in due course**.

Personnel Management Issues

30. **Good personnel policies and practice are important in any organisation. In the intelligence and security Agencies, where the cost of failure may be very great, they are vital. Recent experiences on both sides of the Atlantic underline the importance of having a range of effective measures for dealing with staff problems as they arise, and of making every effort to address and resolve potential disaffection at an early stage**. We therefore decided to continue the Committee's work in the last Parliament by taking a detailed look at the various procedures available to Agency staff with grievances or personal problems, and at some of the measures that might be taken in dealing with threats by disaffected staff to reveal sensitive national security information. We also inquired into a range of related personnel management issues, in particular the selection of new entrants to the services, and career management during the first few years in intelligence work and in the longer term. In so doing, we took evidence from the Heads of the Agencies, and from the Staff Counsellor to the Agencies, Sir Christopher France; we also conducted a series of 'sub-group' visits to each of the Agencies to discuss these issues in more depth with personnel staff involved at all levels.

Recruitment and probation

31. We began by examining the various methods of recruitment into the Agencies, both of mainstream intelligence officers and of the various specialist and administrative support staff. We questioned the Agency Heads on the relative merits, and use, of old methods of recruitment – for example, personal recommendation and the use of 'talent-spotters' – and new, including open recruitment campaigns and the use of recruitment consultants[25]. All three of the Agencies told us that they had adopted, as far as practicable, the Civil Service Code of Practice on recruitment, to help ensure that the procedures used are as open and fair as possible. We discussed, with those staff in the Agencies directly involved in the recruitment processes, the particular qualities and motivations of candidates for employment, and some of the ways in which these are tested during the recruitment process. These issues have a direct bearing on the management of the various occupational groups in the Agencies, most notably in areas of particular recruitment or retention difficulty. **One such area for all three Agencies is that of IT specialists: in earlier reports, this Committee drew attention to critical shortages at GCHQ as high quality**

25. *Evidence from SIS, October 1997. Evidence from GCHQ, October 1997. Evidence from the Security Service, October 1997.*

people were attracted away to industry by very substantial salary increases[26]. To some extent, particularly at GCHQ, the highly specialist and 'cutting edge' nature of the work helps to retain high skills, but this needs to be reinforced by greater pay flexibility for particular groups, and this is being introduced.

32. A particular challenge is faced during the probationary period of an individual's first years in the service. The Agencies cannot afford to carry passengers, and new staff are often used, and tested, in operational postings[27]. This may expose them to challenging and possibly highly sensitive intelligence work at an early stage in their careers, thus placing a high premium on effective and supportive 'mentoring' and guidance, with regular assessments and feedback on performance. **This is clearly not an ideal arrangement, but we accept that the Agencies may on occasion be forced to use relatively new staff in this way. We recommend that wherever possible early postings to the most sensitive areas of work should be avoided until there is clear evidence of an individual's qualities and commitment.**

Dealing with problem cases

33. **Changes in the Agencies' personnel management policies and practices over the last few years have been broadly in line with changes throughout the public sector and with evolving best practice outside.** The Agencies are, for example, developing measures to increase personal responsibility for career development, including: placing a clear emphasis on the development of personal skills or competences to equip an individual for a wide range of jobs; continuous personal development, and the widespread use of open job advertising inside and, whenever possible, outside the department. Career progression is increasingly replacing promotional 'jumps' to more senior grades; and management is able to plan and effect staff deployments with a much clearer idea of individual aspirations, strengths and weaknesses[28].

34. Despite these advances, however, and the development of more rigorous recruitment and enhanced vetting procedures, problem cases still occur. These appear to be relatively few in number but are often complicated in nature involving, for example, misconduct, medical issues, grievances over career progression and, on occasion, ethical concerns about some particular areas of intelligence activity. We have therefore been concerned to see whether those involved in handling such cases are adequately equipped to do so and, in particular, to take effective action whenever possible to resolve those problems that have potential to develop into security concerns.

---

26. *Cm 3574, February 1997, paragraph 23.*

27. *Evidence from the Chief of SIS, November 1997. Evidence from the Director-General of the Security Service, November 1997.*

28. *Evidence from SIS, October 1997. Evidence from GCHQ, October 1997. Evidence from the Security Service, October 1997.*

35. There is a range of individuals or bodies, both inside and outside the Agencies, who may become involved in handling such problems (see table at Appendix 4), including: the individual's line manager, the grade manager in the Personnel Branch, training or security staff, occupational psychologists, or personal and financial counsellors. In addition to this range of management, we have also met the welfare staff now employed by each of the Agencies. **We were impressed by the experience and commitment of this professionally trained group, whose role is to provide confidential support, advice and counselling on any problem, which in many cases will be a personal one.**

36. In addition, since 1987 there has been an external Staff Counsellor, available to be consulted by any member of staff of the Agencies with anxieties relating to the work of his or her service. The Staff Counsellor was originally envisaged as handling 'ethical' problems, but his role has since been widened by mutual agreement with the Agency Heads to include the full range of management issues. On occasion, he is also called upon to help resolve problems arising from grievances held by former staff of the Agencies. Since the creation of the post in 1987, Sir Christopher France and his predecessors have handled some 149 cases: 102 from staff at GCHQ, 34 from SIS and 13 from the Security Service[29]. (We were told that these figures are partly a function of the relative size of the Agencies, but also of issues such as recent outsourcing at GCHQ, which generated a great deal of staff concern.) **On the evidence we have taken, we are convinced of the continuing need for the Staff Counsellor, and of his important role in helping to resolve staff problems once internal procedures have been fully exhausted. The Agencies' management should make particular efforts to publicise his role and work, especially to staff with grievances or concerns which they do not feel have been adequately addressed internally and who may be thinking of leaving, or already have left, employment for this reason.**

37. **On our initial examination of this critical area, we conclude that responses to staff problems of whatever nature should be as early as practicable, and supportive. Ultimately, there are limits to what can be achieved if an individual nursing a grievance refuses to make use of any of the channels described above, or to accept the advice or assistance offered. In such cases, it may be necessary to look to ease the individual out of the service as early as practicable, offering assistance with resettlement – for example, in finding new employment – and making a particular effort, where there are security concerns, to keep in contact following departure.**

38. **The Committee also believes that everything possible should be done to ensure that employees of the Agencies have the same rights as employees elsewhere. One of these is access to industrial tribunals.** Under current procedures, industrial tribunals may hear cases involving national security, in camera and possibly with the Tribunal President sitting alone. However, if this is deemed not to be sufficient protection where

29. *Evidence from the Staff Counsellor, January 1998.*

vital national security matters may be involved, the Secretary of State can issue a certificate preventing an individual from having access to a tribunal. The Tribunals established under the Security Service Act 1989 and the Intelligence Services Act 1994 were not set up to handle complaints involving staff of the Agencies, and have made clear their view that they are not adequately equipped to do so. **We believe that it ought to be possible to constitute a tribunal of members and staff qualified to serve a normal industrial tribunal, but of the necessary integrity and security clearance to handle such potentially sensitive material, and we so recommend.**

Personal Records/Files

39. Soon after our appointment, the Committee's continuing interest in the Agencies' security policies and procedures led us to begin a detailed examination of the Agencies' policies on the creation and use of personal files, in particular those involving British citizens. Security Service files, in particular, are at the heart of much of the Service's work. They are also the subject of a significant proportion of the complaints to the Security Service Tribunal; of continuing debate in Parliament and, last year, of allegations in the national press by an ex-member of the Service. During the year, we took oral evidence from all three Agencies[30] and also, on two occasions, from the Home Secretary[31]; we also received a body of written evidence, and members of the Committee visited the Security Service to be briefed on the records management systems in use there, and to meet some of the staff directly involved in the handling and safe-keeping of files.

40. In our inquiries, we have been concerned in particular to see:

- whether the Agencies have efficient access to the information they require to fulfil their statutory functions;
- whether such personal and often highly sensitive information is afforded a sufficient degree of protection;
- what protection there is for individuals against having information inappropriately or inaccurately gathered, stored and used against their interests;
- that the Agencies are properly accountable for the decisions they make in respect of individual cases; and
- that there are safeguards against any possibility that the Security Service could use its control of the retention or destruction of files to rewrite the historical record.

30. *Evidence from SIS, October 1997. Evidence from the Chief of SIS, November 1997. Evidence from GCHQ, October 1997. Evidence from the Director of GCHQ, November 1997. Evidence from the Security Service, October 1997 and July 1998. Evidence from the Director-General of the Security Service, November 1997.*

31. *Evidence from the Home Secretary, December 1997 and January 1998.*

Security Service files

41. Security Service policy on the creation, use and retention or destruction of files is set out in a Service Manual of Recording Policy (MRP), whose fundamental purpose is to ensure that the Service complies with its statutory duty to collect and disclose only such information as is necessary for the discharge of its functions under the Security Service Acts 1989 and 1996. Service papers are collected into permanent and temporary files; there are also computerised indices for recording basic details about individuals or organisations which have come to notice in the course of investigations but where there is as yet insufficient information to make a judgement about their significance. Permanent files include personal records, containing security information on individuals, as well as other records covering, for example, organisations of interest, particular subjects of study, major Service projects, and policy and administrative issues. At present, the Service holds around 250,000 hard copy personal records on individuals who may, at some time during the Service's history, have been the subject of inquiry or investigation; a further 40,000 are archived on microfiche[32].

42. The function of opening a file is performed by the Central Registry, acting on a request by a desk officer with management approval where necessary. The Registry, which members of the Committee have visited, is responsible for ensuring that the request complies with Service policy that no file is opened unless the subject falls within a current 'recording category'. We were provided with details of these categories, covering the full range of the Service's current operational work. For the most part, they reflect the nature of the threats which the Service is engaged in countering, and specify types of behaviour which indicate that an individual may pose or contribute to a threat. They are defined by the branches within the Service, in consultation with the Registry and the Service's legal advisers, and are regularly reviewed[33].

43. Once a file is opened it is initially coded green, the first stage in a 'traffic-lighting' process first described in the Security Service Commissioner's 1991 Annual Report[34]:

> **GREEN: 17,500 hard copy files (7% of total)**
>
> Open for inquiries; papers may be added to file. Individual/organisation falls within current recording category, and is or may be subject of current investigation. We were told, however, that at any one time only a very small proportion of GREEN files are the subject of active investigation, and that most such records will never be the subject of intrusive investigation.
>
> Of all GREEN files (permanent and temporary – see below), roughly two-thirds – around 13,000 files – relate to British citizens.

32. *Evidence from the Security Service October 1997. Evidence from the Director-General of the Security Service, November 1997.*

33. *Evidence from the Security Service, October 1997 and July 1998.*

34. *Cm 1946, May 1992.*

File remains GREEN for up to five years, depending on recording category, and is then reviewed for transfer to ...

AMBER: 97,000 hard copy files (39%)

Closed for active inquiries, but may have relevant new papers added.

AMBER period depends on recording category, but in most cases until subject is 75 years old or until five years after investigation ceases, whichever is later.

RED: 135,500 hard copy files (54%)

File closed, and retained for research purposes only, or destroyed.

There are, in addition, some 3,000 temporary (GREEN) files opened to house papers for active investigation pending a decision on whether or not to open a permanent file. These must be converted into a permanent file or destroyed after a maximum of three years, subject to the requirements of the Security Service Tribunal (see below)[35].

44. This amounts to a substantial body of information containing a great deal of sensitive and personal information, and we have questioned the Director-General and others within the Service on the issue of access to files and application of the 'need to know' principle in this area. We were told that some files require and are given special protection because of the particularly sensitive nature of the material they contain, for example, on agents of the Service or on espionage or other especially sensitive investigations. In the majority of cases though, there is potentially much broader access to current files, whether it be by line managers and colleagues working in the same general area or by officers in other branches when, for example, a subject might fall within two separate recording categories[36].

45. Beyond this, whenever an individual comes to the attention of a desk officer, a check must be made with the Service file indices to see whether any record already exists on that individual; the desk officer may need to examine all the files on a resultant list to ascertain whether any of them refer to the particular individual of interest. We were told that this is a process which is repeated "hundreds of times every day across the Service"[37]. **We accept that these are necessary processes to enable the Service to conduct its investigative work in an efficient and effective way, and that all Service staff are security cleared to handle very sensitive material. All reasonable steps should be taken, however, to ensure that access to personal files is restricted to those with a clear need to see them, and that there are detailed audit trails to identify which officers or sections have had access to what information, and the reasons for that access.**

35. *Evidence from the Security Service, October 1997.*

36. *Evidence from the Security Service, October 1997.*

37. *Evidence from the Security Service, October 1997.*

46. On the uses to which such files are put, we have also given some consideration to the system whereby the Service makes available to an incoming Prime Minister, in relation to the formation of a Government, any relevant national security information (concerning, for example, contacts with a foreign intelligence service, or a relationship with a terrorist organisation) held on candidates for election. A similar service has been provided to the Leader of the Opposition, in forming a shadow cabinet, since 1992. The Director-General told us that individuals' files are sifted by the Service's central secretariat, before summaries are prepared for him for a decision on whether to pass on the information to the Prime Minister: the number of records made available in the last two General Elections was in single figures[38]. **There is a heavy responsibility on the Director-General, in putting forward any such file, to ensure that the information on it has been properly checked and relates solely to national security.**

Retention and destruction of files

47. Until 1970, the Security Service weeded and destroyed a proportion of its personal files. When this policy was found to have seriously hampered the investigation of a number of espionage cases, the decision was taken to microfiche closed files, rather than destroy them outright. This remained the position until 1992, when the Service reconsidered its files policy again in the light of the changing nature of the threat with the end of the Cold War and the decline in the threat from subversion i.e. actions intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means. Since that time, the Service has been reviewing and destroying files on a case-by-case basis[39]. We were told by the Director-General that files would normally be reviewed for destruction at the end of their RED period, but that the Service was currently reviewing files systematically by category, and that routine reviewing had been suspended[40]. **110,000 files have been destroyed or "marked for destruction" so far. The vast majority of these relate to subversion, on which the Service is no longer conducting any investigations. We note, however, that reviewing in this respect is currently restricted to files on individuals who are over 55 years old. This means that there may be files on individuals under the age of 55 because they joined an organisation which was categorised as subversive possibly 20 years ago, and that these files may still be used for vetting and other purposes. However, no such files would be opened on somebody who joined the same organisation today. We shall be considering this further.**

48. When reviewing files, a number of considerations are taken into account, including whether the information is of continuing relevance to the Security Service's functions today, and the Service's responsibilities under the Public Records Act 1958. The former

38. *Evidence from the Director-General of the Security Service, November 1997. Evidence from the Security Service, July 1998*

39. *Evidence from the Security Service, October 1997.*

40. *Evidence from the Director-General of the Security Service, November 1997.*

is left entirely to the judgement of the Service alone; the criteria for the retention of files on historical grounds are the subject of discussion with the Public Record Office and a number of historians. The latter were announced by the Home Secretary in the House of Commons on 25 February 1998, and include files relating to: major investigations; important subversive figures, terrorists or spies; individuals involved in historical events; causes celèbres in a security context; major changes in Service's policy, organisation or procedures, and milestones in the Service's history; and cases in which the Service has had a public profile.

49. A further factor is that the Service is required to retain copies of all files where inquiries have been made since 1989 or where vetting disclosures have been made, to meet the requirements of the Security Service Tribunal under the Security Service Act 1989 in relation to the investigation of complaints[41]. There may also be occasions, for example when an investigation of an individual turns out to have been mistaken or where a particular recording category is deleted or assessed in retrospect to have been invalid since its inception, where a file could be destroyed by the Service well prior to its normal review date.

50. **Ultimately, the judgement in respect of the review and destruction of individual files is made solely by the Security Service. We believe, however, that some form of independent check should be built into the process, particularly in respect of files relating to subversion.**

51. As we were finalising our Report, the Home Secretary made an important statement on the Security Service's file holdings, and file destruction programme. At the same time, the Service published a further booklet, which includes information about its files. **We shall be reviewing these issues in the light of this material. We shall be considering, amongst other aspects: whether individuals should have rights in connection with the destruction or otherwise of any file held on them; protections against having inaccurate information gathered, stored and used against individuals' interests; the position under current data protection legislation; and implications of the European Convention on Human Rights.**

Other Agencies' files

52. There are significant differences in the type and use of files in the other two intelligence Agencies. SIS, for example, does not hold files on individuals in the same way as the Security Service. Those that do exist generally relate to staff of the Agency, agents, former agents and others with whom the Service has contact, and may contain information, for example, relating to the subject's potential access to intelligence needed to meet JIC requirements. SIS currently holds 86,000 such records, perhaps half of which relate to UK citizens. Files date back to the earliest days of the Service in 1909; some 75% are closed

41. Evidence from the Security Service, October 1997.

ie. no papers have been placed on the file for three years, and there has been no 'movement' in the file in the preceding 12 months. The vast majority of SIS files are retained both for historical reasons, and also because of the operational value of reference back to files, sometimes after many years[42].

53. Similarly GCHQ does not create or maintain personal records in the same way as the Security Service. Its policy on data classed as personal information ie. records kept for intelligence purposes that contain information about individuals or organisations, falls directly from the Interception of Communications Act 1985 (IOCA) and the Intelligence Services Act 1994[43]. Under the latter Act, where a communication is passing or will pass over a British public telecommunications network, GCHQ require a warrant to carry out interception of that communication. Evidence we took from the Director of GCHQ, however, indicated that there are communications obtained incidentally during the course of an authorised, targeted collection, but relating to an individual who was not the subject of the warrant. We were told that such data which may arise from collection under warrant or otherwise is a necessary and sometimes key analytical tool[44]. **It is particularly important that the use of such material is kept under close review, and that it is destroyed as soon as practicable unless there are clear and continuing operational requirements, which will require its own authority.**

54. We have also received some limited written evidence in respect of policy on the use, retention and destruction of personal files by Special Branches, which acquire intelligence to assist the Security Service in carrying out its statutory duties but also to meet local policing needs[45]. One issue, for example, is the extent to which Special Branches might retain 'subversive files' for their own needs, on individuals whose Security Service file may have been destroyed. **We intend to take further evidence on this subject in the autumn, and to report to you in due course.**

42. *Evidence from SIS, October 1997. Evidence from the Chief of SIS, November 1997.*

43. *Evidence from GCHQ, October 1997. Evidence from the Director of GCHQ, November 1997.*

44. *Evidence from GCHQ, October 1997. Evidence from the Director of GCHQ, November 1997.*

45. *Evidence from the Home Office, January 1998. Evidence from the Security Service, July 1998.*

Other matters

Developing Oversight

55. The new system of intelligence oversight by Parliamentarians has now been in place for almost four years. With the benefit of our own experiences, and our study of oversight policies and practices in a number of other countries, we have been taking stock of this country's oversight structures, and considering the extent to which they are appropriate to the tasks which Parliament originally intended.

Oversight in the UK

56. This Committee is one of several bodies outside government charged with accountability or oversight in relation to intelligence and security issues. The others are:

- the Commissioners and Tribunals established in relation to the interception of communications, the Security Service and the two intelligence services (SIS and GCHQ);
- the National Audit Office – which audits the Agencies' finances but, because of the sensitivity of the subject matter, reports not to the full House of Commons Public Accounts Committee but to the Chairman alone; and
- the Security Commission, which exists to investigate and report on the circumstances in which a breach of security is known or presumed to have occurred in the public service.

57. The Commissioners keep under review the exercise by the relevant Secretaries of State of their warrant and authorisation powers under the appropriate Acts, and provide assistance to the Tribunal. They have the power to call for any papers or information required for the discharge of their functions from any Crown Servant. They may submit ad hoc reports to the Secretary of State, and are required to make annual reports to the Prime Minister, which are laid before Parliament, subject to security excisions. They have no executive powers or public or Parliamentary functions.

58. The Tribunals are required to investigate complaints about Agency activities affecting a complainant or his property, or in respect of the interception of communications. Again, Crown Servants are under a duty to give the Tribunals such documents and information as they require. The Tribunals determine whether the Agencies had reasonable grounds for doing what they did, applying the principles of judicial review; they may also refer to the Commissioners complaints concerning property or which may concern authorisations by the Secretary of State. The Tribunals have the power to order redress in the form of terminating inquiries or other activities and ordering the destruction of records, quashing warrants and ordering compensation. Thus far, however, none of the Tribunals has found

in favour of a complainant. **Some see this as evidence that the Tribunal system does not work. We merely state this as a fact since we have not had access to the material to enable any judgement to be made.**

59. Since it was established in 1964, the Security Commission has conducted 14 separate inquiries, involving various security breaches or reviews of security procedures. In particular, two investigations concerned cases of espionage by Agency staff: Geoffrey Prime (GCHQ) in May 1983 and Michael Bettaney (Security Service) in May 1985. All but one of the Commission's investigations – that into the case of Michael John Smith in July 1995 – were conducted prior to the formation of this Committee. **Depending on the type of case, we can certainly envisage this Committee conducting its own inquiry in areas that previously only the Security Commission could have handled. In those circumstances, it would then be sensible to consider whether a duplicate inquiry by the Commission was necessary.**

Oversight in other countries

60. The UK structure of accountability and oversight has evolved over recent years, with either new bodies being created or existing ones having their remits extended. This Committee however, with a remit covering oversight of all three of the Agencies, is still relatively new – certainly, in comparison to many of our counterparts, or nearest equivalents, overseas. In our discussions with these bodies during the course of the year, we have focused in particular on their different methods and powers of oversight, and on a number of related accountability issues, notably:

- legal constraints on intelligence methods and targets;
- executive and judicial checks that intelligence and security services are obeying the law, in particular on acts which would be unlawful but for express authorisation;
- oversight by the legislature of the appropriateness and legality of intelligence and security services' activities; and
- the impact of oversight and accountability on the effectiveness of intelligence and security services.

For illustration, the table at Appendix 5 sets out the various systems in the UK, the United States and Canada. We have considered these, and also those in Europe, Australia and New Zealand.

61. In respect of legislative oversight, it comes in many shapes and sizes. The most substantial and developed is in the United States, with substantial access to all the Agencies and large staffs and resources at the disposal of the Congressional oversight committees. It was in the United States, however, that we also took serious notice of

concerns expressed to us that the oversight system is so extensive and bureaucratic that it hinders the effectiveness of the agencies.

62. Several countries have more extensive forms of 'independent' oversight. One feature that is common to the United States, Canada, Australia and New Zealand is the Inspector-General (IG). IGs' remits vary but, in general, they have considerable powers of access to the operational and other information they may require, similar to those of the Commissioners and Tribunals in this country. In the UK, however, the Commissioner for the Security Service has indicated that it is not his function to review operations[46], and the Tribunals would only do so in response to a direct complaint from a member of the public.

63. Most IGs answer to the executive rather than the legislature. They are full-time appointments, with significant staff support. As a result, those IGs we have met, and their investigative staff, are often able to devote considerably more time and resources to pursuing their various inquiries, and in more depth, than can the serving judges, senior lawyers and, indeed, Parliamentarians appointed to UK 'oversight' positions.

64. **The introduction of an IG system in the UK would require careful analysis of the alternative structures that are used in different countries, and primary legislation. This will inevitably mean that some significant period would elapse before such changes could be introduced. It should also be recognised that there are sharply divergent views in different countries on the value of IGs and to whom they should report.**

65. A feature particular to the UK is the style of our Committee, which is not a Parliamentary Select Committee. **There are arguments for and against such a status, and we have not as yet formed a view on the issue.**

66. **Even if thought desirable, however, such changes would take time to introduce, and could alter significantly the structure of relationships between the Committee and the intelligence community.**

Further evolution of the UK oversight structure

67. **In our review of our arrangements, we recognise that the present system and the manner in which it operates is a serious approach to meeting the needs of oversight**. We have a broad remit, we work within the 'ring of secrecy' and we have a unique right of access under the law to highly sensitive intelligence and security material. The Intelligence Services Act 1994 places a duty on the Heads of the Agencies to disclose information to us on request, subject to arrangements approved by the Secretary of State. The Agency Heads do have specific discretion to withhold information from the

46. *Report of the Commissioner for 1997. Cm 4002, July 1998, paragraph 27.*

Committee where that information may involve, for instance, specific operations or individuals. The Secretary of State, however, can over-ride an Agency Head in this respect, if he considers this desirable in the public interest.

68. This is the legal position, but within it **the level of disclosure of information to the Committee actually depends to a significant extent on the quality of the relationship between the Committee and the Agency Heads and the wider intelligence community. Questions of our access to particular information do arise from time to time, but we have usually been able to reach a satisfactory arrangement. In this connection, it is most important that all in the intelligence community recognise that the greatest possible openness and frankness with the Committee is ultimately in their best interests as well.**

69. **That said, however, we are conscious that, in comparison to other countries, we lack the ability to investigate directly different aspects of the Agencies' activities, some of which have been highlighted in earlier Committee reports. We believe that enhancement of the present arrangements can be achieved without necessarily changing our remit or the law, at this stage, but by extending the Committee's reach with an additional investigative capacity. Such a person would need access to the Agencies' staff and papers, when required to meet the Committee's particular inquiry. We receive much helpful evidence from the Agency Heads and the staffs concerned, but we have not had the capability to conduct independent verification ourselves. Without such a capability, the Committee cannot make authoritative statements on certain issues. It would reinforce the authority of any findings that we make, and be an important element in establishing public confidence in the oversight system. This is important not just for oversight, but for the Agencies themselves and the public view of them. We believe that this is the right approach, and intend to introduce this capability in the coming year.**

Conclusions and recommendations

70. On the basis of the evidence we have taken this year, we conclude that:

The Agencies' Priorities and Plans

A. ***
***
*** (Paragraph 12.)

B. We strongly support the increased priority being given to counter-drugs work by our intelligence services. We shall continue to take a close interest in this area. (Paragraph 13.)

C. We accept the assurances that we were given concerning *** work on Iraq, and the evidence we were given ***
*** (Paragraph 14.)

D. We strongly support the vital work done by the security forces in countering the continuing terrorist threat in Northern Ireland, and accept that considerable resources will continue to need to be devoted to this work. (Paragraph 16.)

Finances

E. The new form in which information was presented to the Committee has greatly helped our understanding of the Agencies' finances. We were told that this has also been of value to the NAO. Ministers may also wish to have financial information presented in this way, in their own considerations of the Agencies' budgets. (Paragraph 18.)

F. On the evidence we have taken, it is clear that the NAO believes that it has access to all the necessary information it requires from each of the Agencies to enable it to carry out its functions effectively. We nevertheless believe that the procedures for the disclosure of information to the C&AG should be further strengthened in a number of areas. In view of our own statutory responsibility to examine the Agencies' expenditure, formal provision should also be made for the disclosure of information and reports by the C&AG to this Committee, in consultation with the Chairman of the Public Accounts Committee. (Paragraphs 22-23.)

G. It would be desirable where practicable for the NAO to carry out further value for money studies into all aspects of the Agencies' activities. (Paragraph 21.)

Personnel Management Issues

H. Good personnel policies and practice in the Agencies, where the cost of failure may be very great, are vital. Recent experiences on both sides of the Atlantic underline the importance of having a range of effective measures for dealing with staff problems as they arise, and of making every effort to address and resolve potential disaffection at an early stage. (Paragraphs 30-38.)

I. We accept that the Agencies may on occasion have to use, and test, relatively new staff in operational postings. We recommend, however, that wherever possible early postings to the most sensitive areas of work should be avoided until there is clear evidence of an individual's qualities and commitment. (Paragraph 32.)

J. On the evidence we have taken, we are convinced of the continuing need for the Staff Counsellor, and of his important role in helping to resolve staff problems. The Agencies' management should continue to make particular efforts to publicise his role and work. (Paragraph 36.)

K. We believe that everything possible should be done to ensure that employees of the Agencies have the same rights as employees elsewhere. One of these is access to industrial tribunals. It ought to be possible to constitute a tribunal of members and staff qualified to serve a normal industrial tribunal, but of the necessary integrity and security clearance to handle such potentially sensitive material, and we so recommend. (Paragraph 38.)

Personal Records/Files

L. 110,000 Security Service files have been destroyed or "marked for destruction" since 1992. The vast majority of these relate to subversion, on which the Service is no longer conducting any investigations. We note, however, that reviewing in this respect is currently restricted to files on individuals who are over 55 years old. This means that there may be files on individuals under the age of 55 because they joined an organisation which was categorised as subversive possibly 20 years ago, and that these files may still be used for vetting and other purposes. However, no such files would be opened on somebody who joined the same organisation today. We shall be considering this further. (Paragraph 47.)

M. The judgement in respect of the review and destruction of Security Service personal files is made solely by the Service. We believe, however, that some form of independent check should be built into the process, particularly in respect of files relating to subversion. (Paragraph 50.)

N. All reasonable steps should be taken by the Agencies to ensure that access to personal files is restricted to those with a clear need to see them, and that there are detailed audit trails to identify which officers or sections have had access to what information, and the reasons for that access. (Paragraph 45.)

O. There is a heavy responsibility on the Director-General of the Security Service, in putting forward to the Prime Minister or Leader of the Opposition files on candidates for election, to ensure that the information on them has been properly checked and relates solely to national security. (Paragraph 46.)

P. On the evidence we took from the Director of GCHQ, there are communications obtained incidentally during the course of an authorised, targeted collection, but relating to an individual who was not the subject of the warrant, which might be said to have been 'incidentally collected'. It is particularly important that the use of such material is kept under close review by GCHQ, and that it is destroyed as soon as practicable unless there are clear and continuing operational requirements, which will require its own authority. (Paragraph 53.)

Oversight Issues

Q. Depending on the type of case, we can envisage this Committee conducting its own inquiry in areas that previously only the Security Commission could have handled. In those circumstances, it will be sensible to consider whether a duplicate inquiry by the Commission was necessary. (Paragraph 59.)

R. Within the current statutory framework, the level of disclosure of information to this Committee depends to a significant extent on the quality of the relationship between the Committee and the Agency Heads and the wider intelligence community. Questions of our access to particular information do arise from time to time, but we have usually been able to reach a satisfactory arrangement. It is most important that all in the intelligence community recognise that the greatest possible openness and frankness with the Committee is ultimately in their best interests as well. (Paragraph 68.)

S. We are, however, conscious that, in comparison to other countries, the Committee lacks the ability to investigate directly different aspects of the Agencies' activities. We believe that enhancement of the present oversight arrangements can be achieved without necessarily changing our remit or the law, at this stage, but by extending the Committee's reach with an additional investigative capacity. Such a person would need access to the Agencies' staff and papers, when required to meet the Committee's particular inquiry. We receive much helpful evidence but do not have the capability to conduct independent verification ourselves. Without such a capability, the Committee cannot make authoritative statements on certain issues. It would reinforce the authority of any findings that we make, and be an important element in establishing public confidence in the oversight system. We believe that this is the right approach, and intend to introduce this capability in the coming year. (Paragraph 69.)

Others

GCHQ PFI Accommodation Project

T. GCHQ faces the most fundamental decisions on its accommodation and location since its original move from Bletchley Park. In this connection, the rapid series of changes of Director has not been helpful. The new Director of GCHQ is the fourth within two years, and finds himself faced with immediate decisions on these critical issues. The challenge of ensuring no interruption to operating capabilities during this reorganisation is a daunting one, which will demand the highest levels of management skill. (Paragraph 8.)

Future programme of work

71. Over the course of the next year, we shall pursue a number of issues identified elsewhere in this Report, including:

- the detail of the Single Intelligence Vote settlement and the full range of issues covered in the recent review of the Vote;
- any changes proposed in the funding and structure of the DIS as a result of the Government's Strategic Defence Review, and the implications that these may have for work of the Agencies;
- in respect of personal files:
  i. policies on the use, retention and destruction of personal files by Special Branches, and connections with Security Service files in this respect;
  ii. whether individuals should have rights in connection with the destruction or otherwise of any file held on them;
  iii. protections against having inaccurate information gathered, stored and used against individuals' interests;
  iv. the position under current data protection legislation; and
  v. implications of the European Convention on Human Rights;
- recent measures taken to enhance the Agencies' internal security policies and procedures;
- questions of intelligence policy in relation to recent events in Sierra Leone, in light of the findings of the Legg Report; and
- co-ordination between the Agencies and the law enforcement organisations in fighting serious organised crime, in particular what value is added by the Security Service involvement in this new area.

We shall also be developing the investigative oversight capability referred to elsewhere in this Report.

72. We also propose to conduct inquiries into two areas of particular concern to the Committee: the Agencies' work in respect of the security of Government communications and our defences against what is commonly termed information warfare; and the Agencies' work in countering the proliferation of weapons of mass destruction.

Signed TOM KING
Chairman, on behalf of the
Intelligence and Security Committee
31 July 1998

APPENDIX 1

THOSE WHO HAVE GIVEN ORAL EVIDENCE

MINISTERS

The Rt. Hon. Robin Cook, MP
Secretary of State for Foreign and Commonwealth Affairs

The Rt. Hon. Jack Straw, MP
Secretary of State for the Home Department

OFFICIALS

FOREIGN AND COMMONWEALTH OFFICE
Senior officials

GCHQ
Mr David Omand, Mr Kevin Tebbit, Senior officials

HOME OFFICE
Senior officials

NATIONAL AUDIT OFFICE
Senior officials

SECURITY SERVICE
Mr Stephen Lander, Senior officials

SIS
Sir David Spedding, Senior officials

OTHERS

Sir Christopher France GCB

31 July 1998

APPENDIX 2

THOSE MET DURING THE COMMITTEE'S WORKING TRIP TO THE UNITED STATES AND CANADA

8-13 MARCH 1998

UNITED STATES

INTELLIGENCE AND SECURITY AGENCIES

CIA – General John Gordon (Deputy Director of Central Intelligence) and senior staff

FBI – Mr John Lewis (Assistant Director, National Security Division)

NSA – Lt. Gen. Kenneth Minihan (Director) and senior staff

INR – The Honorable Phyllis Oakley (Assistant Secretary) and senior staff

CONGRESSIONAL OVERSIGHT COMMITTEES

House Permanent Select Committee on Intelligence
Congressman Porter Goss (Chairman), other members and staffers

Senate Select Committee on Intelligence
Senator Kyl, other members and staffers

PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD, AND INTELLIGENCE OVERSIGHT BOARD

Senator Warren Rudman (Chairman, PFIAB), Mr Anthony Harrington (Chairman, IOB), other members and staffers

OTHERS

Ms Barbara Duckworth, Chief of Staff to Director, Defense Intelligence Agency
Ms Mary McCarthy, Acting Senior Director, Intelligence Programmes, National Security Council

CANADA

PRIVY COUNCIL OFFICE

Mr John Tait

SOLICITOR-GENERAL'S OFFICE

The Honourable Andy Scott, Solicitor-General

CANADIAN SECURITY AND INTELLIGENCE SERVICE

Mr Ward Elcock (Director) and senior staff

SECURITY INTELLIGENCE REVIEW COMMITTEE

Madame Paule Gauthier (Chair), other members and staffers

AUDITOR-GENERAL'S OFFICE

Mr Denis Desautels and staff

COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

Honourable Claude Bisson and staff

INSPECTOR-GENERAL OF CSIS

Mr Vic Gooch (Assistant Inspector-General)

THOSE MET DURING THE COMMITTEE'S WORKING TRIP TO GERMANY

4-6 MAY 1998

MINISTERS

Minister of State Bernd Schmidbauer

INTELLIGENCE AND SECURITY AGENCIES

BfV – Herr Klaus-Dieter Fritsche (Vice-President) and senior staff

BND – Dr Hansjörg Geiger (President) and senior staff

PARLIAMENTARY CONTROL COMMISSION

Wolfgang Zeitlmann MdB (Chairman), other members and staff

INTELLIGENCE BUDGETARY SUB-COMMITTEE

Dr. Erich Reidl MdB (Chairman) and other members

THOSE MET DURING THE COMMITTEE'S WORKING TRIP TO FRANCE AND ITALY

29 JUNE – 2 JULY 1998

FRANCE

MINISTERS

Interior Minister Jean-Pierre Chevènement and other senior members of the French intelligence and security community

ITALY

INTELLIGENCE AND SECURITY AGENCIES

SISDE – Signore Mario Fasano (Deputy Director)

SISMI – Admiral Gianfranco Battelli (Director)

PARLIAMENTARY COMMITTEE FOR THE INTELLIGENCE AND SECURITY SERVICES

Onorevole Franco Frattini and other members

CESIS

Prefetto Francesco Berardino (Secretary-General) and senior staff

31 July 1998

APPENDIX 3: SECURITY SERVICE ESTIMATES AND OUTTURN DETAILS (CASH)

	SUMMARY: £K								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 to 98/99 outturn est. outturn baseline
Running Costs	***	***	***	***	***	***	***	***	***
Other Current Expenditure (OCE)	***	***	***	***	***	***	***	***	***
Capital	***	***	***	***	***	***	***	***	
Appropriations-in-Aid (Receipts)	***	***	***	***	***	***	***	***	***
Control Total	***	***	***	***	***	***	***	***	
Net Superannuation	***	***	***	***	***	***	***	***	***
Total	***	***	***	***	***	***	***	***	***

SECURITY SERVICE ESTIMATES AND OUTTURN DETAILS (CASH)

	A1 – RUNNING COSTS: £K								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn est. outturn 98/99 baseline
Staff Numbers	***	***	***	***		***	***	***	***
Staff Salaries			***	***	***	***	***	***	***
Seconded Staff Salaries									***
Casual/local staff			***	***	***	***	***	***	***
Overtime			***	***	***	***	***	***	***
Cost of Living Allowance (COLA), transfer costs, overseas rent and detached duty expenses etc.			***	***	***	***	***	***	***
Redundancy Costs			***	***	***	***	***	***	***
Pensions Contributions			***	***	***	***	***	***	***
TOTAL STAFF			***	***	***	***	***	***	***
Accommodation, maintenance, utilities, rates and rents			***	***	***	***	***	***	***
Other Gov Depts.			***	***	***	***	***	***	
Training, Phones & other supplies			***	***	***	***	***	***	***
VAT Refunds			***	***	***	***	***	***	
TOTAL	***	***	***	***	***	***	***	***	

SECURITY SERVICE ESTIMATES AND OUTTURN DETAILS (CASH)

	A2 – OTHER CURRENT EXPENDITURE: £K								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn est. outturn 98/99 baseline
Costs of running agents			***	***	***	***	***	***	***
***			***	***	***	***	***	***	***
Ops. Transport									
Ops. Stores									
Ops. Research & Development									
Other Operational Expenditure			***	***	***	***	***	***	***
TOTAL OPERATIONAL			***	***	***	***	***	***	***
Supplies & Consumables			***	***	***	***	***	***	***
Other Gov Depts.			***	***	***	***	***	***	
VAT refunds			***	***	***	***	***	***	***
Capital Charging						***	***	***	***
TOTAL	***	***	***	***	***	***	***	***	

SECURITY SERVICE ESTIMATES AND OUTTURN DETAILS (CASH)

	A3 – CAPITAL EXPENDITURE: £K								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 to 98/99 outturn est. outturn baseline
Operational Items			***	***	***	***	***	***	***
IT Equipment			***	***	***	***	***	***	***
Building Projects			***	***	***	***	***	***	***
Furniture									
Property			***	***	***	***	***	***	***
Vehicles			***	***	***	***	***	***	***
VAT refunds			***	***	***	***	***	***	***
TOTAL	***	***	***	***	***	***	***	***	

SECURITY SERVICE ESTIMATES AND OUTTURN DETAILS (CASH)

	AZ – APPROPRIATIONS IN AID: £K (ANTICIPATED RECEIPTS)								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn est. outturn 97/98 to 98/99 baseline AND DETAILS OF INDIVIDUAL RECEIPTS OVER 500k
Seconded Staff	***	***	***	***	***	***	***	***	***
Rents									
Other Non-Capital Receipts									
Capital Receipts	***	***	***	***	***	***	***	***	***
TOTAL	***	***	***	***	***	***	***	***	
	B1 – PENSIONS								
Payment of Pensions & Lump Sums			***	***	***	***	***	***	
Receipts			***	***	***	***	***	***	
TOTAL	***	***	***	***	***	***	***	***	

SIS ESTIMATES AND OUTTURNS DETAILS (CASH)

	SUMMARY: £M								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn est. outturn to 98/99 baseline
A1 Running Costs	***	***	***	***	***	***	***	***	***
A2 Other Current Expenditure (OCE)	***	***	***	***	***	***	***	***	***
A3 Capital Expenditure	***	***	***	***	***	***	***	***	***
AZ Receipts	***	***	***	***	***	***	***	***	***
Control Total	***	***	***	***	***	***	***	***	
B1 Pensions	***	***	***	***	***	***	***	***	***
***	***	***	***	***	***	***	***	***	***
Note 1 The 1997/98 Estimate figures are drawn from the position post-Spring Supplementary.									
Note 2 Figures for 1998/99 – 2000/01 are as currently recorded in HMT PES database.									
Note 3									

SIS ESTIMATES AND OUTTURNS DETAILS (CASH)

	A1 – RUNNING COSTS: £M								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 to 98/99 outturn est. outturn baseline
Staff numbers	***	***	***	***	***	***	***	***	***
Staff salaries	***	***	***	***	***	***	***	***	***
Seconded staff numbers	***	***	***	***	***	***	***	***	***
Seconded staff salaries	***	***	***	***	***	***	***	***	***
Casual/local staff	***	***	***	***	***	***	***	***	***
Overtime	***	***	***	***	***	***	***	***	***
Redundancy Costs	***	***	***	***	***	***	***	***	***
Pensions Contributions	***	***	***	***	***	***	***	***	***
Total Staff	***	***	***	***	***	***	***	***	***
COLA, transfer costs, overseas rent and detached duty expenses etc.	***	***	***	***	***	***	***	***	***
Accommodation, maintenance, utilities, rates and rents	***	***	***	***	***	***	***	***	***
Other Gov Depts.	***	***	***	***	***	***	***	***	***
Training, Phones & other supplies	***	***	***	***	***	***	***	***	
VAT Refunds			***	***	***	***	***	***	
TOTAL	***	***	***	***	***	***	***	***	
Note 1	The 1997/98 Estimate figures are drawn from the position post-Spring Supplementary.								
Note 2	The COLA transfer costs, overseas rent and detached duty expenses category includes expenditure on non-operational travel and security costs.								
Note 3	***								

SIS ESTIMATES AND OUTTURNS DETAILS (CASH)

	A2 – OTHER CURRENT EXPENDITURE: £M								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 to 98/99 outturn est. outturn baseline
Costs of running agents	***	***	***	***	***	***	***	***	***
***	***	***	***	***	***	***	***	***	
Ops. Transport	***	***	***	***	***	***	***	***	***
Ops. R&D	***	***	***	***	***	***	***	***	***
Total operational	***	***	***	***	***	***	***	***	***
Supplies and consumables	***	***	***	***	***	***	***	***	***
Other Government departments	***	***	***	***	***	***	***	***	***
Capital charge	***	***	***	***	***	***	***	***	***
VAT refunds			***	***	***	***	***	***	
TOTAL	***	***	***	***	***	***	***	***	

Note 1	The 1997/98 Estimate figures are drawn from the position post-Spring Supplementary.
Note 2	Ops. R&D includes expenditure on Comms development and IT development.
Note 3	Additional line for capital charging accounting adjusting included to avoid distortion of other figures.

SIS ESTIMATES AND OUTTURNS DETAILS (CASH)

	A3 – CAPITAL: £M								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 to 98/99 outturn est. outturn baseline
Operational items	***	***	***	***	***	***	***	***	***
IT equipment	***	***	***	***	***	***	***	***	
Building materials	***	***	***	***	***	***	***	***	***
Furniture	***	***	***	***	***	***	***	***	***
Property	***	***	***	***	***	***	***	***	***
Vehicles	***	***	***	***	***	***	***	***	***
VAT refunds	***	***	***	***	***	***	***	***	***
TOTAL	***	***	***	***	***	***	***	***	
Note 1 ***									
Note 2 The 1997-98 Estimate figures shown are drawn from the position post-Spring Supplementary.									
Note 3 IT equipment includes communication infrastructure expenditure.									
Note 4									

SIS ESTIMATES AND OUTTURNS DETAILS (CASH)

	AZ – APPROPRIATIONS IN AID: £M (ANTICIPATED RECEIPTS)								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 to 98/99 outturn est. outturn baseline
Seconded staff	***	***	***	***	***	***	***	***	***
Rents	***	***	***	***	***	***	***	***	***
Other non-capital receipts	***	***	***	***	***	***	***	***	
Capital receipts	***	***	***	***	***	***	***	***	***
TOTAL	***	***	***	***	***	***	***	***	
B1 – PENSIONS									
Payment pensions and lump sums	***	***	***	***	***	***	***	***	***
Receipts	***	***	***	***	***	***	***	***	***
TOTAL	***	***	***	***	***	***	***	***	
Note 1									
Note 2									
Note 3									
Note 4									

GCHQ ESTIMATES AND OUTTURN

	SUMMARY: £m cash								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 to 98/99 outturn est. outturn baseline
A1 – Running Costs	***	***	***	***	***	***	***	***	***
(Of which CESG)	***	***	***	***	***	***	***	***	***
A2 – Other Current Expenditure (Of which CESG)	***	***	***	***	***	***	***	***	***
	***	***	***	***	***	***	***	***	***
									***
									***
									***
A3 – Capital Expenditure (Of which CESG)	***	***	***	***	***	***	***	***	
	***	***	***	***	***	***	***	***	
AZ – Appropriations in Aid (Receipts) (Of which CESG)	***	***	***	***	***	***	***	***	***
	***	***	***	***	***	***	***	***	***
TOTAL (Of which CESG)	***	***	***	***	***	***	***	***	***
	***	***	***	***	***	***	***	***	***

GCHQ ESTIMATES AND OUTTURN

	A1 – RUNNING COSTS: £m cash								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn / est. outturn to 98/99 baseline
Staff numbers (Of which CESG)	*** ***	*** ***	*** ***	*** ***	*** ***	*** ***	*** ***	*** ***	*** ***
Staff salaries	***	***	***	***	***	***	***	***	***
Seconded staff	***	***	***	***	***	***	***	***	
Casual/local staff	***	***	***	***	***	***	***	***	***
Overtime	***	***	***	***	***	***	***	***	
COLA: transfer costs; overseas rent; detached duty expenses etc	***	***	***	***	***	***	***	***	***
Redundancy costs	***	***	***	***	***	***	***	***	***
Pension contribution	***	***	***	***	***	***	***	***	
Total Staff Costs	***	***	***	***	***	***	***	***	
Accommodation, maintenance, utilities, rates & rent	***	***	***	***	***	***	***	***	***
Other Government departments	***	***	***	***	***	***	***	***	***
Training, phones, and other supplies	***	***	***	***	***	***	***	***	***
VAT refunds	***	***	***	***	***	***	***	***	***
TOTAL	***	***	***	***	***	***	***	***	

GCHQ ESTIMATES AND OUTTURN

	A2 – OTHER CURRENT EXPENDITURE: £m cash								Explanation of Variances of +/-10%	
	a	b	c	d	e	f	g	h		
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn	97/98 to 98/99 est. outturn baseline
Military manpower services	***	***	***	***	***	***	***	***		
Numbers of military manpower	***	***	***	***	***	***	***	***		***
Other services from MoD	***	***	***	***	***	***	***	***		
Services from other government depts	***	***	***	***	***	***	***	***		***
Technical maintenance	***	***	***	***	***	***	***	***		
Communications rental				***	***	***	***	***		***
Technical services				***	***	***	***	***		***
Surveying and other services for accommodation	***	***	***	***	***	***	***	***		***
VAT refunds	***	***	***	***	***	***	***	***		***
TOTAL	***	***	***	***	***	***	***	***		

GCHQ ESTIMATES AND OUTTURN

	A3 – CAPITAL EXPENDITURE: £m cash								Explanation of Variances of +/-10%	
	a	b	c	d	e	f	g	h		
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn est. outturn	97/98 to 98/99 baseline
IT equipment	***	***	***	***	***	***	***	***	***	***
Building projects	***	***	***	***	***	***	***	***	***	
Plant infrastructure	***	***	***	***	***	***	***	***		
Vehicles	***	***	***	***	***	***	***	***		
Furniture	***	***	***	***	***	***	***	***		
VAT refunds	***	***	***	***	***	***	***	***	***	
TOTAL	***	***	***	***	***	***	***	***		

GCHQ ESTIMATES AND OUTTURN

	AZ – APPROPRIATIONS IN AID: £m cash (ANTICIPATED RECEIPTS)								Explanation of Variances of +/-10%
	a	b	c	d	e	f	g	h	
	94-95 Outturn	95-96 Outturn	96-97 Outturn	97-98 Cash Limit	97-98 Est. Outturn	98-99 Base line	99-00 Base line	00-01 Base line	96/97 to 97/98 outturn est. outturn 98/99 baseline AND DETAILS OF INDIVIDUAL RECEIPTS OVER £500K
Seconded staff	***	***	***	***	***	***	***	***	
Rents	***	***	***	***	***	***	***	***	
CESG receipts from industry	***	***	***	***	***	***	***	***	***
Other non-capital receipts	***	***	***	***	***	***	***	***	
Capital receipts	***	***	***	***	***	***	***	***	*** *** ***
TOTAL	***	***	***	***	***	***	***	***	

CESG EXPENDITURE

Although GESG's planned spend no longer appears on the face of the Vote, plans for 1997/98 and 1998/99 are shown below, plus the probable outturn for 1997/98:

	1997/98 (Planned)	£m	1997/98 (Probable Outturn)	£m	1998/99	£m
	Running Costs	***	**Running Costs**	***	**Running Costs**	***
	Other Current Expenditure	***	**Other Current Expenditure**	***	**Other Current Expenditure**	***
	Capital	***	**Capital**	***	**Capital**	***
	GCHQ support to CESG	***	**GCHQ support to CESG**	***	**GCHQ support to CESG**	***
	Net accruals element	***	**Net accruals element**	***	**Net accruals element**	***
	Total	***	**Total**	***	**Total**	***

APPENDIX 4: PERSONNEL MANAGEMENT ISSUES

	Handling Disaffected staff	Handling personal/ personnel problems	Handling complaints by members of staff	Handling complaints by outsiders	Identifying and dealing with potential problems
ISC	Examines policies and practices, not individual cases, makes recommendations as appropriate to PM.	See across.	See across.	Not individual cases (forwarded to appropriate Tribunal). May examine policy issues arising from complaints.	Enquiries into policies and practices, and recommendations as appropriate. Not individual cases. Could become involved if approached by Agency/member of staff.
Security Commission	Recommendations from inquiries into breach of security may be relevant.	See across.	See across.	—	See across.
Tribunals (x3)	See across.	—	Intelligence Services Tribunal considers has jurisdiction to hear complaints, but has called for change in legislation: willing to hear complaints in absence of alternative method of appeal. But can only apply judicial review considerations, and no legal representation. Security Services Tribunal may consider complaints relating to vetting, but only whether reasonable grounds for considering information disclosed to be true.	Investigate complaints by members of public. Any person can complain if aggrieved by anything he believes Agencies have done in relation to him or his property; or in respect of communications. Property complaints referred to Commissioner.	—
Commissioners (x3)	—	—	Complaint by member of staff to Tribunal could be referred for investigation.	Assist Tribunals investigating issues relating to property to determine whether warrants issued properly. Tribunals can refer other matters for determination as to whether agencies have acted unreasonably in relation to complainant or his property.	—

APPENDIX 4: PERSONNEL MANAGEMENT ISSUES

continued

	Handling Disaffected staff	Handling personal/ personnel problems	Handling complaints by members of staff	Handling complaints by outsiders	Identifying and dealing with potential problems
Industrial Tribunal	See across.	—	Can hear sensitive cases involving national security *in camera* or President sitting alone. Where safeguards do not provide sufficient protection, S of S issues certificate barring access.	—	—
Security Vetting Appeals Panel	See across.	—	Not available to Agency staff; envisaged that they should be able to appeal to Security Tribunal on issues relating to vetting.	—	—
Staff Counsellor	See across.	Can be consulted by any member of staff who has anxieties about nature of his work (legal or ethical). Remit interpreted loosely so that can consider grievances/ problems of any kind.	See across.	—	—
Line Management	See across.	Provision of advice and support; may refer individual to welfare staff, Staff Counsellor, etc.	Main channel for resolving grievances. Raise matter with line management, personnel, Principal Establishment Officer, appeal to head of department.	—	See across.
Welfare Staff and Counsellors	See across.	Confidential service to individual members of staff and managers.	—	—	See across.

APPENDIX 4: PERSONNEL MANAGEMENT ISSUES

continued

	Handling Disaffected staff	Handling personal/ personnel problems	Handling complaints by members of staff	Handling complaints by outsiders	Identifying and dealing with potential problems
Staff Fora	See across.	All provide route to management for dealing with a grievance/problem – from individual cases to general issues affecting groups of staff or whole department.	See across.	—	See across.
Vetting Officers	Pre-departure security interviews for staff leaving employment. Offer point of contact on security issues.	—	—	—	Initial vetting and subsequent re-vettings throughout career help pick up potential or developing problems.
Resettlement Officers and Outplacement Consultants	Advice on CVs, jobs market, career prospects, network of contacts.	—	—	—	See across.

APPENDIX 5: OVERSIGHT AND ACCOUNTABILITY ISSUES – COUNTRY COMPARISONS

	UK	US	CANADA
1. Purpose of Intelligence and Security Agencies			
Security Service equivalent	Functions of Security Service set out in Security Service Act 1989 (amended by SSA '96): • protect national security • safeguard economic well-being of UK • support prevention/detection of serious crime	Federal Bureau of Investigation (FBI) – component of Justice Department – dual role in counter-intelligence and law enforcement. National Security Division of FBI responsible for countering espionage and terrorist threats in US and supporting CIA/NSA by collecting foreign intelligence within US. Also has power of arrest.	Canadian Security Intelligence Service (CSIS) governed by Canadian Security Intelligence Service Act 1984: • mandate to gather and advise on threats to national security.
SIS equivalent	Functions of Secret Intelligence Service set out in Intelligence Services Act 1994 (ISA): • obtain/provide information relating to actions/intentions of persons outside UK • perform other tasks relating to actions/intentions of such persons But functions can only be exercised: • in interests of national security • in interests of economic well-being of UK • in support of prevention/detection of serious crime	Central Intelligence Agency (CIA) established by National Security Act 1947: • provide accurate, comprehensive and timely foreign intelligence on national security topics • conduct counter-intelligence activities, special activities and other functions as directed by the President.	No foreign intelligence service. (s16 CSIS Act lays down process for foreign intelligence tasking.)
GCHQ equivalent	Functions of GCHQ set out in ISA '94: • monitor/interfere with signals • provide advice/assistance about languages/cryptography But functions can only be exercised: • in interests of national security • in interests of economic well-being of UK • in support of prevention/detection of serious crime	National Security Agency (NSA) founded in 1952: • intercepts and analyses foreign signals.	Communications Security Establishment (CSE) (agency of Dept. of National Defence) not governed by legislative framework – mandate based on royal prerogative and order-in-council.

APPENDIX 5: OVERSIGHT AND ACCOUNTABILITY ISSUES – COUNTRY COMPARISONS

	UK	US	CANADA
2. Legal constraints on methods and targets			
a) Property warrants	• Governed by SSA '89 (amended by SSA '96) and ISA '94 • Warrants only issued if likely to be of 'substantial value' in carrying out statutory functions (see 1 above). Warrants in support of prevention/detection of serious crime cannot relate to property in UK (unless involves violence, substantial financial gain or conducted by large number of people for common purpose). Secretary of State can authorise acts outside UK if necessary for proper discharge of any of SIS's functions (subject to certain safeguards); person carrying out act not then liable under criminal/civil law of UK. • Warrants signed by Secretary of State (normally Home Secretary for Security Service, Foreign Secretary for SIS), or by senior official (valid for under 72 hours) but only in urgent cases and where expressly authorised by Secretary of State.	• Governed by Foreign Intelligence Surveillance Act (FISA). • Warrants issued only if 'probable cause' that target is foreign power or agent of foreign power and collection is for purpose of obtaining foreign intelligence. • Warrants authorised by special FISA court comprising selected Federal judges. Attorney General can in certain circumstances authorise by Executive Order searches/warrants which would otherwise have required a warrant.	• Governed by CSISA '84. • Warrants issued only if 'reasonable grounds' for believing warrant required to investigate threat to national security. • Warrants approved personally by Solicitor General; then go before Federal Court judge.
b) Interception warrants	• Governed by Interception of Communications Act 1985. • Warrants issued only if necessary in: interests of national security; preventing/detecting serious crime; safeguarding economic well-being. (But warrant for purpose of safeguarding economic well-being only considered necessary (and therefore granted) if information relates to acts/intentions of person outside UK.) • Warrants signed by Secretary of State, or by senior official (valid for under 72 hours) but only in urgent cases and where expressly authorised by SofS.	• See 2a) above. But communications which both originate and terminate outside US not regarded as 'US calls' and may be intercepted without warrant. Would not normally target US citizens (would need warrant to do so).	• See 2a) above. But interception of communications which both originate and terminate outside Canada does not require authorisation. Warrants only issued to CSIS – CSE then act on behalf of CSIS.
c) Establishing/ holding files on individuals	• No statutory restrictions [Proposed that new Freedom of Information Bill will not cover Intelligence Agencies.]	• Can only establish and hold records on individuals relevant to conduct of authorised intelligence activities. • Freedom of Information Act enables individuals to ask to see files. May be given edited version, but Agency can choose neither to confirm nor deny that material has been withheld.	• Agencies subject to privacy and access to information legislation, but individuals have no right of access to files and not told whether or not file exists. Edited version of files may be made available but will be limited to information already in public domain.

APPENDIX 5: OVERSIGHT AND ACCOUNTABILITY ISSUES – COUNTRY COMPARISONS

continued

	UK	US	CANADA
3. Oversight			
a) Judicial checks	• No judicial involvement in granting of warrants. • *Security Service Commissioner* (Lord Justice Stuart-Smith), set up under SSA '89, reviews property warrants issued to Security Service; *Intelligence Services Commissioner* (Lord Justice Stuart-Smith), set up under ISA '94, reviews property warrants issued to SIS and GCHQ; *Interception of Communications Commissioner* (Lord Nolan), set up under IOCA '85, reviews interception warrants. Each Commissioner: – assists relevant Tribunal in investigating complaints – makes annual report to Prime Minister (laid before Parliament) – has statutory right of access to whatever documents/information required to discharge functions (visit Agencies during year to check sample of warrants issued properly). • Agencies can be sued for unlawful actions, although primary method of recourse for individuals is to the Tribunals (see 4 below).	• FISA Court grants warrants. • Agencies can be sued for actions undertaken in course of official duties.	• Federal Court grants warrants. • Human Rights, Privacy and Information Commissioners can investigate activities of Agencies. • CSIS can be sued under Security Offences Act but must show unlawfulness and intention to commit; no prosecutions brought to date.

APPENDIX 5: OVERSIGHT AND ACCOUNTABILITY ISSUES – COUNTRY COMPARISONS

continued

	UK	US	CANADA
b) Executive oversight/accountability	• Director General, Security Service reports to Home Secretary; Chief of SIS and Director, GCHQ report to Foreign Secretary. Home Office and Foreign Office officials can pursue issues with agreement of Head of relevant Agency. • Ministerial Committee on Intelligence Services (CSI) keeps under review policy on security and intelligence services, assisted by Permanent Secretaries' Committee on Intelligence Services (PSIS). • Remit of Joint Intelligence Committee includes 'to provide direction and keep under review organisation and working of intelligence activity to ensure efficiency, economy and prompt adaptation to changing requirements.' Intelligence requirements set by JIC. SIS/GCHQ performance reviewed annually by Intelligence Co-ordinator; Security Service reviewed by SO(SSPP). Reports go to CSI. • Intelligence and Security Committee makes annual report to Prime Minister. Edited version laid before Parliament.	• Agencies report to relevant Secretary. Head of the Intelligence Community reports to the President. • Inspectors General within each Agency report to Agency Directors. IGs' remit varies (some statutory) but primarily focus on compliance with laws/rules; and identifying waste, fraud and abuse. • Inspection Division/Oversight Board within Agencies with remit to review 'questionable' activities. • Intelligence Oversight Board reports to President on activities which may be illegal under US law – receives reports from IGs and Agencies (does not report to Congress). • President's Foreign Intelligence Advisory Board assesses quality, quantity and adequacy of intelligence collection. Provides private advice to President (does not report to Congress).	• Director of CSIS responsible to Solicitor General for control and management of Service; and consults with Deputy Solicitor General on operational policy. Chief of CSE responsible to Minister of National Defence. • Inspector General reviews compliance with law by CSIS (acts as eyes and ears of executive) and carries out annual certification procedure. IG reports through Deputy Solicitor General to Solicitor General. • Commissioner for CSE reports to Minister for National Defence but mandate only relates to ensuring compliance with law. • Co-ordinator plays similar role to Co-ordinator in UK.

APPENDIX 5: OVERSIGHT AND ACCOUNTABILITY ISSUES – COUNTRY COMPARISONS

continued

	UK	US	CANADA
c) Legislative oversight	• Intelligence and Security Committee, set up by ISA '94, composed of 9 members of House of Commons and House of Lords. ISC members appointed by Prime Minister; make annual reports to Prime Minister and can report at other times on any matters relating to discharge of functions. Redacted version of annual reports laid before Parliament by Prime Minister.	• Congressional oversight committees (House and Senate) governed by Intelligence Oversight Act 1980 and Intelligence Authorisation Act 1993. Senate Committee has 19 members; House Committee has 16 members.	• Security Intelligence Review Committee (SIRC), set up under CSIS '84, acts as 'surrogate' of Parliament. Between 3 and 5 Privy Councillors (not members of House of Commons or Senate); appointed by Governor in Council.
	• Remit of ISC is to examine expenditure, administration and policy of Agencies.	• Remit of Committees is to authorise funding for intelligence activities; and conduct investigations, audits and inquiries as may be required.	• Remit of Committee is to review performance of CSIS's duties and functions; investigate complaints from public; and consider reports concerning immigration and citizenship applications. Committee has authority to direct Inspector General to examine specific activities.
	• Access to information set out in ISA '94 – restrictions on access to 'sensitive information' (sources, information about particular operations), but Agency Head and/or Secretary of State can authorise disclosure if 'safe to do so'/'in public interest'. Guidelines on disclosure approved by Ministers in December 1994.	• Access is unrestricted. DCI has statutory duty to keep Committees 'fully and currently informed of all intelligence activities'. But Agencies not expected to reveal details of sources and methods. Committees receive IG reports.	• SIRC has access to all information under CSIS's control (except Cabinet confidences).
	• ISC has 3 full-time staff provided by the Cabinet Office.	• Senate Committee has 35–40 staff; House Committee has 25 staff.	• Staff of around 12.
4. Individual recourse	• Members of public can complain: – to Security Service Tribunal or Intelligence Services Tribunal if aggrieved by anything they believe Agencies have done in relation to them or their property – to Interception of Communications Tribunal if they believe their communications have been intercepted	• Public can raise issues with Oversight Committees, but Committees will not normally choose to become involved in individual cases.	• Public can complain to: – SIRC about any act or thing done by CSIS – CSE Commissioner, but has limited powers to investigate complaints and cannot inform individual of findings.
	• No right of access to files (see 2c) above)	• Individuals may be given access to files (see 2c) above).	• Individuals may be given access to files (see 2c) above).

ISBN 0-10-140732-7

APPENDIX 5: OVERSIGHT AND ACCOUNTABILITY ISSUES – COUNTRY COMPARISONS

continued

	UK	US	CANADA
5. Value for money	• Single Intelligence Vote (SIV): aggregate of Agencies' expenditure. PSIS scrutinises annual expenditure forecasts; submitted to Ministers who agree funding through SIV. • National Audit Office has full access to information subject to restrictions necessary to protect identities of certain sources of information and details of particularly sensitive operations. Reports to Chairman of Public Accounts Committee. NAO completes annual audit of SIV and has power to carry out value-for-money reviews of significant areas of expenditure. • ISC examines expenditure across the board, including resource allocation and reaches value-for-money judgements on specific areas of inquiry.	• Director of Central Intelligence (DCI) supervises budget for community as a whole (National Foreign Intelligence Programme). • GAO has no authority over intelligence budget – IGs responsible for auditing and investigating value-for-money issues. • Congressional oversight committees approve budget for intelligence activities. (Members of Oversight Committees only politicians involved in intelligence budget.)	• Auditor-General responsible for all government auditing, including intelligence community – reports to Public Accounts Committee. Does not carry out intelligence value-for-money studies. • Inspector General (for CSIS) and CSE Commissioner carry out value-for-money studies of operational areas.

Printed in the UK for The Stationery Office Limited on behalf of the Controller of Her Majesty's Stationery Office
Dd 5068393 10/98 76368 Job No. J0063121