



# Intelligence and Security Committee

## Annual Report 2001–2002

Chairman:  
The Rt. Hon. Ann Taylor, MP

Intelligence Services Act 1994  
Chapter 13

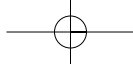


Intelligence and Security  
Committee  
Annual Report 2001–2002

Chairman:  
The Rt. Hon. Ann Taylor, MP

Intelligence Services Act 1994  
Chapter 13

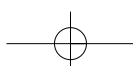
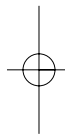
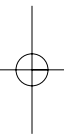
Presented to Parliament by the Prime Minister  
by Command of Her Majesty  
JUNE 2002



**©Crown Copyright 2002**

The text in this document (excluding the Royal Arms and departmental logos) may be reproduced free of charge in any format or medium providing that it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Any enquiries relating to the copyright in this document should be addressed to The Licensing Division, HMSO, St Clements House, 2-16 Colegate, Norwich, NR3 1BQ.  
Fax: 01603 723000 or e-mail: [copyright@hmso.gov.uk](mailto:copyright@hmso.gov.uk)



*From the Chairman: The Rt. Hon. Ann Taylor, MP*

**INTELLIGENCE AND SECURITY  
COMMITTEE**

70 Whitehall  
London SW1A 2AS

8 May 2002

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

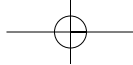
*Dear Tony,*

I enclose the Annual Report of the Intelligence and Security Committee for 2001–2002. Since you appointed us in August, the Committee has been grateful for the time and access that we were given by the Agencies, especially as they were under the intense pressure resulting from the terrorist attacks on the USA. These attacks dominated a significant part of the Committee's time and may continue to do so. However, we were able to consider other matters, such as serious organised crime.

We look forward to discussing this Report with you.

*Yours sincerely,  
Ann Taylor*

**ANN TAYLOR**



## INTELLIGENCE AND SECURITY COMMITTEE

The Rt. Hon. Ann Taylor, MP (Chairman)

The Rt. Hon. Lord Archer of Sandwell, QC

The Rt. Hon. James Arbuthnot, MP

The Rt. Hon. Kevin Barron, MP

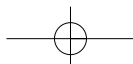
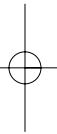
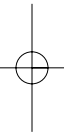
The Rt. Hon. Alan Beith, MP

The Rt. Hon. Alan Howarth, CBE, MP

Mr Michael Mates, MP

The Rt. Hon. Joyce Quin, MP

The Rt. Hon. Gavin Strang, MP

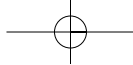


# INTELLIGENCE AND SECURITY COMMITTEE

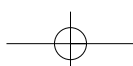
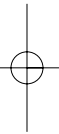
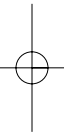
## Annual Report 2001–2002

### Contents

<b>Glossary</b>	–	<b>page 3</b>
<b>Introduction</b>	–	<b>page 5</b>
<b>Work Programme</b>	–	<b>pages 5–6</b>
<b>The National Intelligence Machinery</b>	–	<b>pages 6–11</b>
The Joint Intelligence Committee	–	pages 7–9
Security Service	–	pages 9–10
SIS	–	page 10
GCHQ	–	page 10
Agency Customers	–	page 11
Information Technology	–	page 11
<b>Administration</b>	–	<b>pages 11–13</b>
IPT and Commissioners	–	pages 11–12
Staffing, Recruitment and Retention	–	pages 12–13
<b>Expenditure</b>	–	<b>pages 13–16</b>
Additional Funds	–	pages 14–15
GCHQ and the New Accommodation Project	–	pages 15–16
<b>Policy</b>	–	<b>pages 16–18</b>
<b>Afghanistan and the Attacks on 11 September</b>	–	<b>pages 19–26</b>
Afghanistan	–	pages 19–21
Agencies' Resources	–	page 21
The Attacks	–	pages 21–22
Agencies' Immediate Responses to the Attacks	–	page 23
Agencies' Longer-term Responses and Plans	–	pages 23–26
<b>Serious Organised Crime</b>	–	<b>pages 26–28</b>

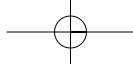


<b>Secure Communications</b>	<b>– pages 28–29</b>
<b>Committee Matters</b>	<b>– pages 29–31</b>
The Investigator	– page 29
<i>A. Agencies' Scientific and Technical             Research and Development Work</i>	– pages 29–30
<i>B. Discharge of Inspectors-General Roles             in the UK Intelligence System</i>	– page 30
Tasking the Investigator	– pages 30–31
<b>Conclusions and Recommendations</b>	<b>– pages 32–35</b>
<b>Future Programme of Work</b>	<b>– page 36</b>
<b>Appendix 1 – Witnesses</b>	<b>– pages 37–38</b>
<b>Appendix 2 – Data Protection Act 1998     Reasons Document</b>	<b>– pages 39–44</b>
<b>Appendix 3 – Inspectors-General Functions     in the UK Intelligence System</b>	<b>– pages 45–52</b>

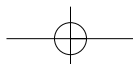
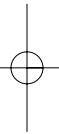
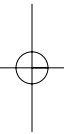


## GLOSSARY

ATCSA	Anti-Terrorism Crime and Security Act 2001
CDI	Chief of Defence Intelligence
CIDA	Concerted Inter-Agency Drug Action
CNI	Critical National Infrastructure
CSI	Ministerial Committee on the Intelligence Services
DCDI	Deputy Chief of Defence Intelligence
DIS	Defence Intelligence Staff
DPA	Data Protection Act 1998
DTI	Department of Trade and Industry
EKP	Economic Key Points
FBI	US Federal Bureau of Investigation
FCO	Foreign and Commonwealth Office
FDA	First Division Association
GCHQ	Government Communications Headquarters
GIAM	Government Internal Audit Manual
IA	Internal Audit
IT	Information Technology
JARIC	Joint Air Reconnaissance Intelligence Centre
JIC	Joint Intelligence Committee
JIO	Joint Intelligence Organisation
MoD	Ministry of Defence
NAO	National Audit Office
NAP	GCHQ's New Accommodation Programme
NCIS	National Criminal Intelligence Service
NCS	National Crime Squad
OCSG	Organised Crime Strategy Group



PSIS	Permanent Secretaries' Committee on the Intelligence Services
RAF	Royal Air Force
RIPA	Regulation of Investigatory Powers Act 2000
SCG	Strategic Customer Group
SIA	Single Intelligence Account
SIS	Secret Intelligence Service
SSA	SIS Staff Association
UBL	Usama bin Laden



## Introduction

1. This Annual Report covers the Intelligence and Security Committee's seventh year and is the first produced by the Committee appointed by the Prime Minister in August 2001. This Committee has four members who sat on the Committee in the previous Parliament and five new members, including the Chairman, the Rt. Hon. Ann Taylor, MP.
2. The 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: the Security Service, the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ). Committee members are notified under the Official Secrets Act 1989 and the Committee operates within the "ring of secrecy". It reports directly to the Prime Minister and through him to Parliament by the publication of this Annual Report. The Committee is supported by a secretariat based in the Cabinet Office.

## Work Programme

3. The work of the Committee has been dominated, inevitably, by the events surrounding the terrible terrorist attacks of 11 September 2001. However, the Committee was also anxious to follow a wider programme of activity because of the importance of the Agencies in other areas. In this work we were guided by the comments made in the previous Committee's Interim Report 2000–2001<sup>1</sup>. The Committee's work programme was as follows:
  - a. To familiarise the new Committee members with the National Intelligence Machinery and the work of the Agencies.
  - b. To assess the implications of the 11 September terrorist attacks for the UK intelligence and security Agencies.
  - c. To continue the statutory work of providing effective oversight of the Agencies' expenditure, administration and policy. In this regard we met the Commissioners and took evidence from the Agencies, members of the Joint Intelligence Committee (JIC) and the Defence Intelligence Staff (DIS); and we tasked the Investigator to carry out five investigations. In particular we took evidence on the Agencies' support for the fight against Serious Organised Crime.
  - d. To develop the Committee's work programme for the future.

---

1. Cm 5126.

4. For this Annual Report the Committee took evidence from 37 witnesses. A full list is at Appendix 1 and includes:

- The Foreign, Home and Defence Secretaries, the Attorney General and Chief Secretary to the Treasury;
- The Heads of the Security Service, SIS, GCHQ, the Chief of Defence Intelligence (CDI) and the JIC Chairman;
- Officers from the three Agencies and officials from the Cabinet Office, the Foreign and Commonwealth Office, the Ministry of Defence, the Home Office, the National Audit Office and Law Enforcement Organisations.

5. In addition to these formal evidence sessions, the Committee undertook visits to the three Agencies, the Joint Intelligence Organisation (JIO), the DIS, and the National Criminal Intelligence Service (NCIS), for informal briefing sessions. The Committee also visited RAF Menwith Hill and met UK and US staff working at this important joint intelligence support facility.

6. A small group of members made a short visit to Washington DC in November 2001 to meet Congressional colleagues and US Intelligence Agencies. The Committee visited France in January 2002 and we have hosted delegations from Australia, Germany, USA and Japan. Additionally, the Committee is hosting the International Intelligence Review Agencies Conference in May 2002, at which Inspectors-General, Parliamentary and other Oversight Committees will discuss oversight issues.

**7. The Committee has been impressed by the Agencies' work during the period covered by this Report. The Committee found it useful to meet some of the Agencies' staff who had been involved in the follow-up work to the 11 September attacks, as well as other areas, and the Committee saw the dedication with which they go about their work. While this Report will highlight the areas about which the Committee has concerns, as that is the purpose of oversight, it must not overshadow the tremendous efforts made by the Agencies' staff, sometimes at great personal risk, to gain valuable secret intelligence for the UK. This intelligence safeguards national security, economic wellbeing and it helps prevent and detect serious organised crime. It significantly reduces the threat to the UK and its citizens.**

## **The National Intelligence Machinery**

8. The National Intelligence Machinery is defined as the three intelligence and security Agencies (SIS, Security Service and GCHQ), the Defence Intelligence Staff (DIS) and the Joint Intelligence Committee (JIC) based in the Cabinet Office. The JIC is supported by the Joint Intelligence Organisation (JIO) which consists of the Assessments Staff, the Intelligence Co-ordinator's group and a Secretariat. The three Agencies are funded by the

Single Intelligence Account (SIA), while the DIS and JIO are funded by the MoD and Cabinet Office respectively.

9. As part of the familiarisation process the Committee took evidence on the JIC and the role of the Intelligence Co-ordinator. The Intelligence Co-ordinator's role is to draft the UK's Requirements and Priorities for Secret Intelligence for the JIC, amend them as necessary during the year and support the Cabinet Secretary in the allocation of funding from the SIA to the three Agencies. The JIC has two functions: it produces assessments using secret intelligence and open source material for Ministers and officials and it establishes the UK's Requirements and Priorities for Secret Intelligence. The procedure is that the UK's Requirements and Priorities are then endorsed by the Permanent Secretaries' Committee on the Intelligence Services (PSIS)<sup>2</sup> and by the Ministerial Committee on the Intelligence Services (CSI)<sup>3</sup>.

10. The Committee notes that CSI has still not formally met to endorse the UK's Requirements and Priorities for Secret Intelligence or the SIA, despite the strong recommendation of the previous Committee that it meet at least annually to so do. We questioned a number of CSI members on whether or not they believed that CSI should meet. They believed that it was a matter for CSI Chairman – the Prime Minister. However, they did not express any reasons why CSI should not meet. We believe that CSI would provide Ministers with the forum to discuss intelligence-related matters, such as requirements, priorities and funding. The Secretaries of State believe that while they do have to rely heavily on the judgement of those involved in the UK's Requirements and Priorities process, they do discuss priorities and the allocation of effort with the Agencies' heads.

11. It should be noted that meetings of a similar composition to CSI took place after the 11 September terrorist attacks, which demonstrates the importance of ensuring Ministers are correctly briefed on and agree intelligence-related matters. The value of these meetings is significant as it allows informed decisions to be made jointly. **This Committee recommends that CSI meets at least annually. We suggest that these meetings review the UK's Requirements and Priorities for Secret Intelligence, agree the Agencies' budgets and receive briefings on current threats from the Agencies.**

### ***The Joint Intelligence Committee***

12. The JIC consists of the three Agency Heads, CDI and his deputy DCDI, and senior officials from the FCO, MoD, Treasury, DTI, Cabinet Office and Home Office, in addition to the JIC Chairman. Representatives from other government departments,

---

2. *PSIS is chaired by the Cabinet Secretary.*

3. *CSI is chaired by the Prime Minister and its membership is the Deputy Prime Minister, the Chancellor of the Exchequer and the Foreign, Home and Defence Secretaries.*

including the Northern Ireland Office, HM Customs and Excise, NCIS and National Crime Squad, attend meetings as necessary.

13. The Committee welcomes the appointment of Mr John Scarlett to the joint position of Intelligence Co-ordinator and JIC Chairman, as the previous Committee<sup>4</sup> suggested that future holders of this position be filled from within the intelligence community.

14. The Committee was informed that the process for developing, and the format of, the UK's Requirements and Priorities for Secret Intelligence had been improved. The new process is intended to improve the ability to make qualitative judgements about the value of intelligence when marked against the desired policy outcome and to assist in defining gaps in coverage<sup>5</sup>. The restructured paper is in the form of an introduction with a number of annexes detailing requirements and priorities under regional and functional headings. The UK's Requirements and Priorities are used to task the SIS and GCHQ. They are also reflected in the Security Service Plans and Priorities paper. The Defence Intelligence Staff, which is tasked separately by the MoD, feeds its requirements into the UK's Requirements and Priorities process and it is also guided by the outcome.

15. The JIC has revised the previous system of priorities and now the priorities reflect the directness, the immediacy and the scale of the risk or benefit to UK interests. However, it should be remembered that "the devotion of resources to the acquisition of intelligence from secret sources can be justified only in cases where such intelligence can be expected significantly to add value to policy objectives"<sup>6</sup>. First Order priorities, obviously the most important, cover \*\*\*

\*\*\*

\*\*\*

\*\*\*

\*\*\*.

16. Second Order priorities cover \*\*\*

\*\*\*

\*\*\*

\*\*\*. This priority is divided into two categories: starred \*\*\*

\*\*\*

and unstarred \*\*\*

\*\*\*. The lowest priority, Third Order, is also split into two categories: starred \*\*\*

\*\*\*

\*\*\*.

---

4. Cm 4897.

5. Evidence from Cabinet Office, 9 November 2001.

6. Evidence from Cabinet Office, 9 November 2001.

17. In the next three sections, the Agencies' allocations of resources to areas of work are given. The Committee recognises that while these percentages do not tell the full story of the analysis effort allocated to each area, they represent the percentage of the Agency's total resources allocated to that area. In the Security Service, the deployment \*\*\*  
\*\*\* will cause the percentage of resources allocated to that area to increase disproportionately. In GCHQ, given the relative costs of generic technical capability and manpower, changes in allocation of the former have a large impact on these figures, whereas changes in the allocation of manpower have minimal effect. However, the Committee believes that the resource allocation does help to highlight where resource changes have occurred.

### *Security Service*

18. The tasking of the Security Service reflects its functions under the Security Service Acts 1989 and 1996 and the UK's Requirements and Priorities for Secret Intelligence. Overall and for the longer-term tasking, the Security Service's annual Plans and Priorities paper is put to the JIC and consolidated with papers from SIS and GCHQ for Ministerial consideration and approval<sup>7</sup>.

19. In the period 2001–2002 the Service devoted 33% of its effort to Irish Counter Terrorism, a result of which was the successful conviction of three Real IRA terrorists for attempting to buy arms and explosives overseas. Work on International Counter Terrorism accounted for 23%<sup>8</sup> of the Service's effort while Counter Espionage accounted for 16%. During the year, \*\*\* Rafael Bravo \*\*\* arrested under the Official Secrets Acts. Bravo, a security guard at a BAe Systems site, was convicted and jailed earlier this year. It remains the case in the post-cold war era that individuals will sell secret information for financial gain and that this threat to UK national security needs to be constantly guarded against.

20. 11% of the Service's effort was directed at providing Protective Security advice. The Service works with the Civil Contingencies Secretariat, the Home Office and other departments to reduce the vulnerability of \*\*\*

\*\*\* the Critical National Infrastructure (CNI)<sup>9</sup>. \*\*\*

\*\*\*

\*\*\*. The Service has arrangements to ensure that those in Government, industry and among the public who have assets to protect have access to expert advice and training on physical protective security measures. There is a framework of standards and access to specialist help as well as standardised, public information on counter terrorism contingency planning and business contingency plans produced by the Home Office. The

---

7. *Evidence from Home Office, 21 February 2002.*

8. *Evidence from the Security Service, 26 March 2002.*

9. *Evidence from the Security Service, 12 April 2002.*

Service is playing a leading role in identifying new areas for counter terrorism advice, given the recognition of attacks, possibly suicide attacks, aimed at causing mass casualties.

21. Additionally the Security Service manages a Research and Development programme to develop counter terrorism protection technologies for the future. Research is undertaken to \*\*\*

\*\*\*

\*\*\*. For example, analysis of \*\*\*

\*\*\* and the Service has worked to develop \*\*\*

\*\*\*. The Service has also advised \*\*\*

\*\*\*.

### **SIS**

22. For 2001–2002 the SIS allocated \*\*\* of its effort to Counter Terrorism, \*\*\* to Serious Crime and \*\*\* to counter the Proliferation of Weapons of Mass Destruction. The allocation to geographical areas was \*\*\* for the Middle East/North Africa, \*\*\* for Asia, \*\*\* for the Former Soviet Union and \*\*\* for the Balkans.

23. These allocations were revised after the 11 September terrorist attacks, with Counter Terrorism almost doubling to \*\*\* of the effort and minor reductions being made to other areas<sup>10</sup>.

### **GCHQ**

24. The Committee was told that at the beginning of 2001–2002, GCHQ devoted \*\*\* of its resources to Russia, \*\*\* to the Balkans, \*\*\* to the Middle East, North Africa and the Indian Sub-continent, while \*\*\* covered the Rest of the World<sup>11</sup>. In the subject areas, \*\*\* of the resources were allocated to Counter Terrorism, \*\*\* to weapons systems, \*\*\* to Counter-Proliferation and \*\*\* to Serious Crime.

25. By the end of March 2002, these resource allocations had been amended with Counter Terrorism increased by \*\*\* the Rest of the World reduced by \*\*\* and the Balkans falling by \*\*\* Collection on Serious Crime rose by \*\*\* with Weapons systems and Counter-Proliferation each rising \*\*\* respectively.

10. Evidence from SIS, 4 April 2002.

11. Evidence from GCHQ, 19 April 2002.

## *Agency Customers*

26. The Committee took evidence from the Foreign, Home and Defence Secretaries, the Chief of Defence Intelligence and the MoD Policy Director in their capacities as the Agencies' customers. The last two are also JIC members. The Ministers stated that they were content with the Agencies' reporting and timeliness. They told us that due to the terrorist attacks of 11 September, greater emphasis is being attached to intelligence and intelligence-related matters by Ministers than previously had been the case.

27. The Intelligence Co-ordinator produces an annual review of the Agencies' performance, which outlines success in the given reporting period and identifies gaps against the UK's Requirements and Priorities for Secret Intelligence. This review is normally sent to members of CSI and the JIC. This is the only formal assessment of the Agencies' performance, although the Committee was told that the Agencies' performance was also discussed during bilateral meetings with their customers. The Investigator, in his report on *Inspectors-General Functions*, drew the Committee's attention to the fact that the JIC, assessments and the UK's Requirements and Priorities processes had never been audited (see paragraph 93b and Appendix 3).

## *Information Technology*

28. In previous reports<sup>12,13</sup> the Committee commented on the need for IT expertise in the JIO to manage the programme, known as SCOPE, which will give the intelligence community more effective and accountable access to intelligence. SCOPE will develop new possibilities for joint working, using a secure and resilient network working at the highest levels of classification. The Committee noted that a Programme Director has been appointed and that work on this important undertaking is beginning to take shape around a draft programme definition. **The Committee is aware that the SCOPE programme has yet to reconcile different requirements from different participants. We recommend both that the key requirements are finalised and that the funding is agreed as soon as possible. We will continue to monitor the situation.**

## **Administration**

### *IPT and Commissioners*

29. The Committee is grateful to the Interception Commissioner, the Rt. Hon. Sir Swinton Thomas, and the Intelligence Services Commissioner, the Rt. Hon. Lord Justice Simon Brown, for meeting them. These Commissioners, who report to the Prime

---

12. Cm 4897.

13. Cm 5126.

Minister on the lawfulness of warrants, detail errors and mistakes relating to warrants. The Committee has previously requested sight of the confidential annexes to their reports, redacted as necessary to protect operational details, in order to satisfy itself that the Agencies are not making errors which would raise questions about the effectiveness of the Agencies. **The Committee believes that there is still a need to see the confidential annexes to the Commissioners' reports, redacted as necessary, in order to fulfil its statutory requirement to oversee the Agencies' administration processes.**

30. **The Committee notes that the Commissioners now have sufficient Secretariat support for their work. However, we are concerned that, when the provisions covering communications data in the Regulation of Investigatory Powers Act 2000 (RIPA) are brought into force, the Interception of Communications Commissioner may well be overwhelmed by authorisations which he is required to examine as part of his statutory remit. The Committee recommends that additional staff are put in place within the Secretariat before the provisions are enacted to avoid repeating the unacceptable delays that occurred in 2000 with the Investigatory Powers Tribunal and its predecessors.**

31. The Committee was disappointed that The Rt. Hon. Lord Justice Mummery, President of the Investigatory Powers Tribunal, declined the Committee's invitation to discuss his role. The Committee understands his anxieties, which concern his judicial role and the need to maintain a separation between the judiciary and the legislature, but felt that there were matters that could have usefully been discussed.

### ***Staffing, Recruitment and Retention***

32. There have been a number of significant developments within the Agencies on staff matters. One such development is that from March 2002 the SIS's Service Staff Association (SSA) has concluded an affiliation agreement with the First Division Association (FDA)<sup>14</sup>. The purpose in establishing the link to the FDA is to give the SIS staff, who is precluded from trade union membership, an assurance that staff relations are conducted in accordance with best practice within the Public Service. In effect the affiliation will provide the SSA and its members with an additional layer of expertise. **The Committee welcomes this move by the SIS.** The Committee has also been informed that the SIS intends to revise the terms and conditions of employment for all of its staff in the next year. We will monitor these developments and report in due course.

33. We were advised by the Agencies that the events of 11 September had had a positive effect on public perceptions of the importance of their work and that this could help them achieve their challenging recruitment and retention plans. The Security Service informed

---

<sup>14</sup>. Evidence from SIS, 21 March 2002.

the Committee that its future plans for growth were dependent on recruiting some 140 non-graduates. The Director General<sup>15</sup> said that its plans were ambitious but he believed that the Service was taking action, such as the use of recruitment agencies and \*\*\* \*\* The SIS stated that it was encouraged by the number of recruits it was attracting and that it was investigating ways to improve the retention of serving members of the Intelligence Branch. There are roughly \*\*\* SIS staff overseas at any one time on permanent posting, with a lot more on temporary missions. An increasing number of these permanent postings were becoming more uncongenial from a family point of view. The SIS is therefore looking at new ways to support postings, such as locating an officer's family in neighbouring countries where regular visits are possible<sup>16</sup>.

## Expenditure

34. The Committee took evidence from the Chief Secretary to the Treasury on the internal Treasury processes for allocating funding to the Agencies. The Agencies are funded by the Single Intelligence Account (SIA). The Principal Accounting Officer for the SIA is Sir Richard Wilson, the Cabinet Secretary. He submits the SIA as part of the Comprehensive Spending Review to the Chief Secretary for approval. The Chief Secretary is the only Minister in the formal approval system for the Agencies. The Foreign and Home Secretaries do see the bids from their respective Agencies but do not apply directly to the Treasury for the funding. The Committee welcomes the Chief Secretary's appearance to give evidence this year, particularly as he authorised the claims the Agencies made on the Reserve following the 11 September terrorist attacks. **The Committee welcomes the speed with which the Treasury was able to find additional funding for the Agencies on this occasion.**

35. The Committee notes that the Treasury is a full member of the JIC and that the Chancellor of the Exchequer is a member of CSI, which means that he agrees the UK's National Requirements and Priorities for Secret Intelligence. **The Committee believes that, as the Treasury is fully involved in the setting of the requirements and priorities for the Agencies, it should ensure that the Agencies are funded to be able to meet in full the demands placed on them.**

36. The Chief Secretary concurred with the Committee that the UK/US collaboration is highly valuable and remarked that it "is obviously a very important factor in relation to our thinking"<sup>17</sup>. He also agreed that the provision of imagery by JARIC is very important. **However, the Committee was concerned to hear that the Treasury believed that it was for the MoD alone to judge the priority of imagery rather than an inter-**

---

15. Evidence from DG Security Service, 17 April 2002.

16. Evidence from C, 10 April 2002.

17. Chief Secretary to the Treasury.

**departmental approach.** This means that imagery competed against forms of fighting equipment and other forms of investment. **The Committee<sup>18, 19</sup> believes that imagery meets a national requirement and as such Government must consider it as a whole, perhaps through CSI.** The Committee does not want to see UK developments in imagery and its related technologies limited by financial pressures in the MoD. **We believe that the Government needs to ensure that this vital capability is not only maintained but also enhanced.**

### *Additional Funds*

37. **The Committee continues to work closely with the NAO and we are particularly grateful for the support provided by the NAO during our examination of the Agencies' expenditure.** We were briefed by the Agencies on their baseline budgets, which had been agreed as part of the Comprehensive Spending Review 2000, and the extra funding they had been given in 2001/2002 to conduct additional work. The Committee noted that while the Agencies had put forward strong cases for increased funding, particularly in areas such as \*\*\*\*\*, the Treasury had not agreed to meet the Agencies' bids in full. Consequently, the Agencies had to reduce elements of their existing programme in order to fund important new work.

38. The Agencies received additional, but ring-fenced, funding as a result of the Home Office led bid to undertake work against drugs and illegal immigration. More detail on the operations is given in paragraph 84. We believe it is important as it is to encourage joint working, which we believe has much improved, but we would not wish to see ring-fencing creating undue administrative complexities and constraints.

39. The annual Net Resource Requirements for the Agencies and the SIA can be seen in the table below. To avoid confusion we have only included the years for which resource accounting was in place.

---

18. Cm 4897.

19. Cm 5126.

All figures in £ millions

	Security Service	SIS	GCHQ	SIA Total
1999/2000	***	***	***	869.3
2000/2001	***	***	***	862.6
2001/2002	***	***	***	1015.1
2002/2003	***	***	***	990.8
2003/2004	***	***	***	1099.2

Notes:

1. These figures include the costs of the SIS and Security Service pension schemes.
2. The figures up to 2000/2001 are final outturns, the figures for 2001/2002 are provisional outturns.
3. The figures include the £54 million claims from the reserves for both 2001/2002 and 2002/2003.
4. The figures include the additional funding resulting from the Home Office bid to fight serious organised crime from 2001/2002 to 2003/2004.
5. The figures for 2003/2004 are due to be revised as part of SR2002.

40. As a result of the Agencies' claims on the reserve they were allocated an additional £54 million for 2001/2002 and £54 million for 2002/2003. The additional funds in 2001/2002 were predominately used to conduct operations, although the Agencies began to invest in IT systems and recruiting/re-employing additional staff. All the Agencies are now embarking on major IT projects which will need careful management to ensure that defined requirements are established and that the systems meet the Agencies' requirements and are to budget and time. The Agencies are also employing significant numbers of consultants to assist with these projects. In the past the Committee<sup>20</sup>, through the Investigator, examined the Agencies' record on IT systems. **We will monitor these major IT projects and report in due course.**

### ***GCHQ and the New Accommodation Project***

41. **The Comptroller and Auditor General wrote, in the audit of the 2000/2001 Accounts<sup>21</sup>, "I have not obtained all the necessary information and explanations that I considered necessary for the purposes of my audit; and I was unable to determine whether proper accounting records had been maintained". This resulted in the GCHQ Accounts being qualified.** The NAO told us that the qualification resulted from the inability of GCHQ to correlate the physical assets, involving approximately half of them, with the supporting accounting records as Resource Accounting requires. The introduction of resource accounting both highlighted the poor asset tracking system in GCHQ and forced a culture change<sup>22</sup>. GCHQ has taken steps to address these important

20. Cm 4897.

21. Certificate of the Comptroller and Auditor General to the Chairman of the Committee of Public Accounts, 26 February 2002.

22. Director GCHQ, 1 May 2002.

issues and the 2001/2002 accounts will indicate the degree of progress. **The Committee recommends that the Director GCHQ, the Cabinet Secretary and the Foreign Secretary seek to assure themselves that appropriate management processes, controls and qualified staff have now been put in place.**

42. The Committee recognises that the NAP presents the management of GCHQ with a tremendous challenge. We visited the construction site in September 2001 and have received regular updates from GCHQ, which indicate that the PFI element of the programme is ahead of schedule. The Committee has also monitored changes to the projected cost of relocating to the new building. We have been told that, due to the planned increase in GCHQ staff numbers following the 11 September attacks, additional work-spaces will need to be included in the new building and an additional \*\*\* staff will remain on the Oakley site. This may result in a rise in the costs associated with relocation. We are therefore concerned that the agreed budget for the transition costs may be too low. GCHQ has yet to finish a full register of assets and consequently it is unable to quantify the cost of relocating and installing all necessary equipment to the new building.

43. **The Committee is concerned that, in order to keep within the agreed relocation budget, GCHQ may be forced to reduce its operational effectiveness and agreed service to its customers. We would not wish to see this happening, especially after the 11 September attacks.**

## Policy

44. The Committee has noted that a significant amount of legislation, which has an impact on the intelligence and security Agencies, has come into force in the last two years: the Terrorism Act 2000, the Regulation of Investigatory Powers Act (RIPA) 2000, the Anti-Terrorism Crime and Security Act (ATCSA) 2001 and the Data Protection Act (DPA) 1998. These Acts have increased the demands on the Agencies and the Committee was informed that their legal departments have increased significantly.

45. The Terrorism Act and the ATCSA now allow intercepted material to be used as evidence in the Proscribed Organisations Appeal Commission and the Special Immigration Appeals Commission. In November 2001 the Committee wrote to the Prime Minister and the Foreign and Home Secretaries about the Anti-Terrorism Crime and Security Bill. We informed them that while the Committee had decided not to add to the debate on the detail of the legislation, the Committee would offer its views in the light of the experiences of the Agencies in working under the new statute. The Committee did note that measures giving officials access to ferry manifest data, which Members of the Committee had called for during the debate on the Intelligence Services in 2001<sup>23</sup>, had been included in the legislation.

---

23. *Hansard, 29 March 2001: Column 1159.*

46. Law enforcement organisations and the Agencies stressed the usefulness of communications data in uncovering terrorist and criminal networks. We have noted that the Government is preparing a Code of Practice under the ATCSA to enable the retention of communications data for long enough to be of utility to the intelligence and security Agencies. **The Committee will examine the use of intercepted material and communications data, together with the scope of legislation, in the next year and report further.**

47. On the subject of interception, the Committee noted that, in response to a written question from Mr Norman Baker MP, in December 2001, the Prime Minister confirmed that there had been no change to the Government policy on the tapping of the telephones of Members of either House of Parliament. The full text of the answer was<sup>24</sup>:

As I informed the House on 30 October 1997, *Official Report*, column 861, Government policy remains as stated in 1966 by the then Prime Minister, the Lord Wilson of Rievaulx. In answer to questions on 17 November 1966, Lord Wilson said that he had given instructions that there was to be no tapping of the telephones of Members of the House of Commons and that if there were a development which required a change of policy, he would at such moment as seemed compatible with the security of the country, on his own initiative, make a statement in the House about it. The then Parliamentary Under-Secretary of State for the Home Department, Lord Bassam, confirmed on 27 September 2000 that this policy extended to Members of the House of Lords.

With this long-standing exception in relation to Members of Parliament, it remains the normal policy of the Government neither to confirm nor deny allegations in respect of interception matters.

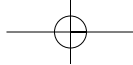
48. **The Committee supports this policy and believes that it is important that it is not eroded in any way. The Committee believes that if the policy is ever changed or altered then Parliament would need to be informed as soon as it was compatible with the security of the country to do so.** Since its establishment in 1994, the Committee has not been informed of any change or alteration to the stated policy.

49. The Data Protection Act (DPA) 1998 was discussed by the Committee in the 1999–2000 Annual Report<sup>25</sup> and since then the Act has been used by individuals in attempts to see what, if any, personal information the intelligence and security Agencies have stored on them. The Agencies operate the “neither confirm nor deny” policy, the underlying purpose of which is, as its name implies, to ensure that the Agencies do not have to indicate whether they hold material on a particular data subject where national

---

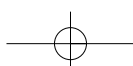
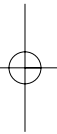
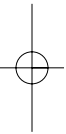
24. *Hansard*, 19 December 2001: Column 367W.

25. *Cm* 5126.



security would be compromised. The DPA allows a Cabinet Minister to certify that exception from certain provisions of the law, including access to specified personal data, is required for the purpose of safeguarding national security.

50. The Home Office has published a reasons document, which is available in the Libraries of both Houses, outlining why a section 28 certificate is necessary to safeguard national security. The Committee, which does not investigate individuals, has also prepared a reasons document, which can be found at Appendix 2, outlining why it needs a section 28 certificate to cover personal information it may have been given whilst conducting its statutory duties, and thus to safeguard national security. The Foreign and Home Secretaries have jointly signed this certificate to protect the Committee's data.



## Afghanistan and the Attacks on 11 September

51. This section focuses on the UK intelligence and security Agencies and their role with reference to the terrorist attacks on the US. Our US Congressional colleagues are making a number of studies into 11 September related matters, and it is for them to comment on issues relating to US Agencies or organisations. We understand that they will be reporting in due course.

### *Afghanistan*

52. **Terrorism** has always been a JIC First Order of Priority<sup>26</sup>. **It is well known that there continues to be a threat to the UK from Northern Ireland related terrorist groups.** As part of the work against international terrorism, the Agencies have been interested in Usama bin Laden (UBL) and related terrorist organisations \*\*\*. These organisations, under UBL's leadership, had bombed the two US Embassies in Africa in 1998 and were regarded as a threat to UK interests abroad. By 2000 GCHQ was describing UBL as "a major preoccupation"<sup>27</sup>.

53. In February 2001 George Tenet, the Director of Central Intelligence in the USA, said, as part of his statement on "Worldwide Threat 2001: National Security in a Changing World", that:

"Usama bin Ladin and his global network of lieutenants and associates remain the most immediate and serious threat [to the USA]. Since 1998, Bin Ladin has declared all US citizens legitimate targets of attack ... he is capable of planning multiple attacks with little or no warning"<sup>28</sup>.

54. However, although terrorism was First Order requirement, as was the combating of illegal drugs, Afghanistan itself was not. \*\*\*

\*\*\*, Afghanistan was a \*\*\* \*\*\*.

The Foreign Secretary told the Committee that, in his view, "the West [had] essentially walked away from Afghanistan, we are trying to get it back"<sup>29</sup>.

55. We were told on both sides of the Atlantic that, in efforts to combat terrorism in the UK, Agencies work very closely with their US counterparts. Intelligence and assessments are exchanged on a regular basis: the level of concern in June 2001 was such that discussions about UBL and his organisation occupied a considerable time during a joint summit \*\*\*

\*\*\*.

---

26. Evidence from Cabinet Office, 26 October 2001.

27. Evidence from Director GCHQ, 21 March 2001.

28. Statement to the Senate Select Committee on Intelligence, 7 February 2001.

29. Evidence from Foreign Secretary, 28 November 2001.

56. The UK and US Agencies achieved some notable successes against UBL related terrorists in the three years prior to the 11 September attacks<sup>30</sup>. For obvious reasons many of these successes cannot be publicised. Intelligence had been produced linking UBL with the attack on the USS Cole in Yemen and the US Embassies in Africa – the latter being used in the prosecution of the attackers in the USA<sup>31</sup>. Plots to carry out attacks in the US, Europe and the Middle East around the turn of the Millennium were thwarted, as have been more recent attacks.

57. However, despite these successes, UBL remained a hard target for the Agencies. The Intelligence Co-ordinator, in his Review of Agencies' Performance against JIC Requirements in both the periods 1999–2000<sup>32</sup> and 2000–2001<sup>33</sup>, reported that there was a specific lack of intelligence on the thinking of UBL \*\*\* The 2000–2001 Review assured Ministers that the Agencies “have action in hand” to \*\*\*

\*\*\* and the Committee was told that GCHQ were making some headway in \*\*\*

\*\*\*<sup>34</sup>. The Intelligence Co-ordinator, in evidence to the Committee, stated that “in the area of UBL for example, under terrorism, the Agencies have \*\*\*

\*\*\*”<sup>35</sup>.

58. **Drugs** was another First Order of Priority requirement. As 90% of the heroin reaching the UK originates in Afghanistan, the Agencies, in co-operation with UK Law Enforcement Organisations and supportive Governments, \*\*\*

\*\*\*. The Taliban moratorium on planting opium poppies last year limited production but, as large amounts of drugs were and still are stored in Afghanistan, \*\*\*

\*\*\*. However, \*\*\* the now publicly known links, particularly in funding, between UBL and the Taliban. The Taliban taxed the flow of drugs from Afghanistan and this, together with direct funding from UBL as payment for allowing him to operate on their territory, represented the majority of their income.

59. In June 2001 the JIC agreed, as part of its annual review of the UK's Requirements and Priorities and as one of a number of changes, to raise the Order of Priority for Afghanistan \*\*\*. This meant that the Agencies were expected to \*\*\* which would give the UK a better understanding of \*\*\*

\*\*\*. This change would have taken effect \*\*\* when Ministers were due to be invited to endorse the UK's Requirements and Priorities. We believe that this increase would have supported the work that the FCO was undertaking, within the UN context, to examine

---

30. Evidence from Cabinet Office, 26 October 2001.

31. Evidence from Cabinet Office, 17 January 2001.

32. Evidence from Cabinet Office, 17 January 2001.

33. Evidence from Cabinet Office, 18 July 2001.

34. Evidence from Director GCHQ, 21 March 2001.

35. Evidence from JIC Chairman, 24 January 2001.

possible ways forward for Afghanistan, “given the very severe constraints”<sup>36</sup> on what could be done. An example of this work was hosting a UN conference on the future of Afghanistan at Weston Park in July 2001. In anticipation of this increase, the Agencies started to examine \*\*\*

\*\*\*

\*\*\*

\*\*\*.

### *Agencies’ Resources*

60. During evidence on the Agencies’ resources and finance, the Intelligence Co-ordinator in early 2001 stated that “they [the Agencies] have to work with the resources that are available to them, and my judgement is that they can meet their \*\*\*”<sup>37</sup>. GCHQ had already acknowledged a need to acquire extra linguists and analysts to carry out the processing and reporting \*\*\*<sup>38</sup>. However, its Director said that he had been constrained by the Treasury requirement to divert resources into the New Accommodation Programme relocation work<sup>39</sup>. The impression the Agencies gave the Committee is that they were content with the level of resources available, based on the threat assessment, although they all admitted that additional funding would have been welcome and could have been used to good advantage<sup>40</sup>.

61. All three Agencies told the Committee that they were between 2% to 3% below their agreed staffing levels before 11 September and that they were already taking steps to address these shortfalls. **The Committee believes that reductions in the Agencies’ funding during the 1990s, together with staff shortages that were being addressed after the SR2000 settlement, meant that the Agencies were resource limited and operating under financial pressures prior to the 11 September attacks.**

### *The Attacks*

62. The Agencies have told us that they had no intelligence forewarning them specifically about the 11 September attacks on the USA. A subsequent re-examination of material across the intelligence community did not find any that, with the wisdom of hindsight, could have given warning of the attacks<sup>41</sup>. There was “an acute awareness in the period before 11 September that UBL and his associates represented a very serious

---

36. Evidence from Foreign Secretary, 28 November 2001.

37. Evidence from JIC Chairman, 24 January 2001.

38. Evidence from Director GCHQ, 21 March 2001.

39. Evidence from Director GCHQ, 30 October 2001.

40. Evidence from SIS, Security Service and GCHQ, 15 and 19 March 2002.

41. Evidence from the DG Security Service, 30 October 2001.

threat” and that there was planning activity<sup>42</sup>. Experience had demonstrated that UBL could master-mind co-ordinated attacks on US targets resulting in thousands of casualties. At the June 2001 joint meeting with the \*\*\* considerable anxieties were expressed at the lack of specific intelligence. Attacks, probably against US interests, were imminent but their nature and target were unknown.

63. A JIC assessment in July 2001 suggested that UBL organised attacks were in their final stages of preparation. While US or Israeli interests were the most likely targets, UK interests were at risk, including from collateral damage in attacks on US targets<sup>43</sup>. This lack of intelligence access to a notably hard target meant that the UK and the US did not know who was going to carry out attacks, how the attacks were going to be mounted or where the attacks were going to take place. Up to that point the West had not foreseen suicide attacks taking place on the USA mainland and certainly not that the attacks would result in some 3,000 deaths, including the single greatest loss of UK citizens’ lives to terrorist attack.

64. The questions are whether the threat posed by UBL was understood and whether it was effectively brought to Ministers’ attention. The Home Secretary told the House of Commons after the attacks that “...the nature and the level of the threat is different from what was previously envisaged”<sup>44</sup>. In evidence to the Committee, the Home Secretary stated that “the international assessment of the threat, not just in the UK, post the bombing of the US Embassies in East Africa in ’98, underestimated what potentially might happen and the level of threat, particularly to the US .... There is nothing as visionary as hindsight and I don’t pretend for a minute that I would have been able to foresee what was going to happen, so while I think that they [the Agencies] were ‘on the ball’ in terms of recognising that there was a network, that it was operating effectively, that it did take years to put a plan into operation, I don’t think that had been translated in quite the way we can now see”<sup>45</sup>. **The Committee agrees.**

65. The Agencies had identified the pressing need to gather intelligence about UBL \*\*\* – a notably hard target – and informed Ministers that action was in hand. The July 2001 JIC paper concluded that plans for attacks were in their final stages but that the timings, targets and methods of attack were not known. This assessment was not a stark warning of immediate danger to the UK. The shortage of specific intelligence and UBL’s record could have warned all concerned that more urgent action was needed to counter this threat. Whether this could have forestalled any of UBL’s actions can only be a matter for conjecture. **The Committee concludes, with hindsight, that the scale of the threat and the vulnerability of Western states to terrorists with this degree of sophistication and a total disregard for their own lives was not understood.**

---

42. *Evidence from JIC Chairman, 30 October 2001.*

43. *JIC Assessment, 16 July 2001.*

44. *Hansard, 15 October 2001: Column 923.*

45. *Home Secretary, 13 March 2002.*

### *Agencies' Immediate Responses to the Attacks*

66. At the national level the Agencies' Heads played a full role. They were brought into the centre of the UK decision-making process immediately, not only as members of the War Cabinet but as members of smaller decision-making groups<sup>46</sup>. We were told that the day after the attacks the Director GCHQ, Chief of the SIS and the Deputy Director General of the Security Service were in the USA, to co-ordinate the intelligence picture with their US counterparts. For the Agencies themselves the main change after the 11 September attacks was that the volume of reporting increased and the threshold of intelligence that was circulated decreased both internationally and within the UK.

67. The Security Service continued to acquire intelligence from UK and overseas agencies about threats to UK interests, analysing the reports and transferring them into threat assessments. The Service thus re-examined the threat and stepped up its investigative and intelligence collection effort against the Islamic extremists in the UK. It provided relevant protective security advice and took part in the Government's response in consequence management.

68. The SIS re-deployed some \*\*\* staff to the London-based counter-terrorism team and the focus of many stations and teams was redirected. The contacts that had been developed through the Agencies' counter-drugs and international terrorism work were now directed exclusively at al-Qaida and the Taliban.

69. GCHQ doubled the size of its counter-terrorism team to \*\*\* and established a team to \*\*\*. It set up a new team to develop \*\*\*

\*\*\*

\*\*\*.

This was managed by a crisis leadership and management team \*\*\*

\*\*\* and meant that initially GCHQ was devoting 30–40% of its total effort to the crisis.

**70. The Agencies responded very rapidly to the terrorist attacks, appropriately devoting both additional staff and other resources to securing the UK and identifying terrorist networks. The Committee met staff involved and their determination and professionalism impressed us highly.**

### *Agencies' Longer-term Responses and Plans*

71. As has been noted, after the 11 September attacks, the Treasury approved £54 million for use by the Agencies in the financial year 2001–2002 and a further £54 million has been allocated for the year 2002–2003. These amounts were judged necessary to avoid reducing work against other high-priority targets to unacceptably low levels. The

---

46. *Foreign Secretary, 28 November 2001.*

Agencies' plans with this additional funding are given in the section below. None of these amounts has been included in the baselines being considered for the Comprehensive Spending Review 2003–06. The Agencies have been invited to submit bids as part of the normal process.

72. In the Security Service, the increase in capability arising from the extra funding will involve the recruitment of some 130 extra staff by March 2003. They will be directed towards more collection (including surveillance, interception and agent-running), investigation and dissemination of intelligence. As a customer for intelligence, the Service will also benefit from enhanced co-operation with law enforcement agencies and greater exchange of intelligence with security organisations world-wide and from the increased collection effort of SIS and GCHQ. Because intelligence coverage of priority targets can never be total, the defence of this country against terrorist attack must also depend on protective security. The Service plans to expand its protective security work in response to the changed threat, which now includes suicide attacks in the UK, and an increased demand from both old and new customers for advice. Modernisation and integration through information technology of the Security Service's core business processes should enable more efficient use of staff engaged in investigation and analysis.

73. The SIS told the Committee<sup>47</sup> that in order to offset the transfer of resources into counter-terrorism, to develop new capabilities and to maintain global reach, it will need some \*\*\* additional staff over the next 18 months. There will be a particular need for operational officers with the skills and experience to undertake unconventional deployments. In addition to more conventional overseas deployments, the SIS are using its extra resources to extend the focus of its counter-terrorism work in a range of ways, including:

- focusing on \*\*\*  
\*\*\*  
\*\*\*  
\*\*\* the threat;
- identifying emerging threats by closer liaison within Government and with allies;
- working with the Security Service to improve co-ordination with Western European services and promoting joint or burden-sharing operations;
- engaging with a wider range of non-European services;
- developing its infrastructure to accommodate these new deployments; and
- expanding its IT and other technological capabilities.

---

47. Evidence from Cabinet Office, 26 October 2001.

74. GCHQ is significantly improving its capability in the following areas:

- increased access to \*\*\*  
\*\*\*;
- acceleration of its existing programme for \*\*\*  
\*\*\*;
- improved capability to \*\*\*  
\*\*\*;
- improved access to \*\*\*  
\*\*\*;
- an additional \*\*\* to deliver improved capabilities, and \*\*\* to take full advantage of new facilities.

75. The Chancellor of the Exchequer announced<sup>48</sup> in October 2001 that a multi-agency terrorist finance unit within the National Criminal Intelligence Service (NCIS) would be established and funded to build on the successful work that had previously been co-ordinated by NCIS and supported by the Agencies and law enforcement organisations. This unit would be supported by a new taskforce that would bring to the anti-terrorism effort the best of academic, financial and commercial expertise. The work would involve examining different banking systems and bureaux de change, and will be supported by the Agencies.

76. The 11 September attacks once again demonstrated the international mobility of terrorists – those involved in the attacks had stayed in and passed through a number of countries. Such international mobility is also a striking factor of drugs trafficking and money laundering. For these reasons, co-ordination and co-operation between intelligence agencies is increasingly necessary. The Committee has been briefed on the UK Agencies' various international links and we have highlighted elsewhere in this Report that joint working with the US is particularly effective. However, good links have also been forged with the European intelligence agencies and agencies in other parts of the world where such co-operation is not always easy. Agencies in other countries have different powers, they operate in different legal frameworks and their collection priorities are also different – all a product of their cultures and history. **Such co-operation and co-ordination are vital in today's fight against terrorism and we welcome the progress that has already been made.**

77. The UBL-related terrorists tended to speak Arabic \*\*\*  
\*\*\*. However, there is a recognised shortage of linguists \*\*\*  
\*\*\*.

---

48. *Hansard, 15 October 2001: Column 941.*

The Agencies \*\*\* and there were some problems re-balancing their workload and consequently \*\*\* were temporarily reduced. Whilst linguists in similar languages can be retrained, the process takes time. The Committee has tasked its Investigator to examine elements of the Agencies' language/linguist situation because concerned that the Agencies do not have sufficient flexibility to cover all the languages they need to cover.

78. An additional area of concern is the work that has been reduced by the Agencies. The SIS informed us that they had reduced collection on \*\*\*

\*\*\*. The cut in \*\*\* has been particularly severe, with only \*\*\* of SIS effort now allocated to this task. However, we were told that due to the nature of their collection methods there had not yet been a significant drop in reporting, just that new targets were not being developed. GCHQ reported a \*\*\* reduction in collection on \*\*\*

\*\*\*. The Security Service has reduced on reporting \*\*\* as well as its support \*\*\* and it had reduced work on internal matters.

79. These reductions are causing intelligence gaps to develop, which may mean that over time unacceptable risks will arise in terms of safeguarding national security and in the prevention and detection of serious organised crime. The Agencies must be given sufficient resources to enable them not only to fill the staff vacancies that have been created but also to expand sufficiently to ensure that they can meet the new demands now being placed on them.

## Serious Organised Crime

80. The Committee took evidence from the Home Secretary and the Directors General of the National Crime Squad (NCS) and the National Criminal Intelligence Service (NCIS), together with the Chief Investigations Officer, HM Customs and Excise. We were told that most law enforcement requests for assistance from the intelligence and security Agencies are handled by NCIS, who then pass them on to the relevant Agency. The Committee enquired about the degree of co-operation between them. We were told that the UK community has recognised the importance of joined-up working and that there now exists an Organised Crime Strategy Group (OCSG), which works both structurally and strategically. All interested parties belong to the OCSG, which is chaired by the Home Office and includes the intelligence and security Agencies and law enforcement organisations, together with heads of relevant Government departments. Within the context of Ministerial policy the OCSG sets the overall strategy, based on the NCIS Threat Assessment for Serious Crime, and decides the priorities to be followed.

---

49. Director General NCIS, 6 February 2002.

81. In support of the OCSG, the Strategic Customer Group (SCG) has been formed which agrees how priorities are going to be met. The Committee was given two examples where the SCG had targeted maximum effort on a given criminal activity. First is the Concerted Inter-Agency Drug Action (CIDA) group, led by HM Customs and Excise, now involving the MoD due to its presence in Bosnia, Kosovo and Afghanistan; and second, Operation REFLEX, led by NCS to counter organised immigration crime.

82. Ensuring that intelligence flows are operating effectively is a major challenge and a major opportunity for law enforcement organisations. Reporting coming into NCIS from the Agencies has increased and NCIS knows that the Agencies are committed to enhancing the speed and content of the reporting. As part of this work the JIC has established a team in the Assessments Staff covering serious organised crime. They are represented on the OSCG and SCG, and receive information and papers from the law enforcement organisations. Papers are regularly considered by the JIC on crime and its impact on other activities, whether economic or political. This is a welcome development, not least because it is a very useful mechanism for flagging up changes and trends for Ministers.

83. The law enforcement organisations are consulted on the relevant parts of the UK Requirements and Priorities and they are discussed at the SCG. We were told that their requests have been incorporated. Class A drugs and organised immigration crime issues are First Order of Priority, as are the requirements for serious financial crime and the funding of terrorist activities. The Committee was also briefed on the money laundering conducted through bureaux de change in the UK one case £4.2 billion of drugs-related cash was laundered through a number of bureaux in the North West during a four-month period. The new legislation regulating the bureaux will help to gauge the scale of the problem and gives new opportunities to stop the laundering of cash.

84. The Agencies were allocated £11.45 million in 2002, which has been ring-fenced, as part of the Government's anti-drugs strategy. The money was spent under the guidance of CIDA and linked to specific targets, which are defined before the money is allocated. This has resulted in a number of successful joint HM Customs and Excise and SIS operations in \*\*\*. The Committee was also briefed on the work that the SIS undertook \*\*\*

\*\*\*

\*\*\*

85. Following the terrorist attacks of 11 September, Europol, which concentrates largely on international crime, took on an added mandate for counter-terrorism. The UK supports Europol having a role in intelligence assessment and analysis, and there is a debate about

---

50. Director General NCIS, 6 February 2002.

51. Chief Investigating Officer HM Customs and Excise, 6 February 2002.

the extent to which they might become involved in tactical counter-terrorism operations, which has yet to be resolved.

86. The Europol staff allocated to counter-terrorism has now increased from six to around 50, including \*\*\* one from the Metropolitan Police, and may grow to 70. But the real problem remains the practical one of ensuring that national law enforcement organisations are prepared to share information. That issue remains a problem in some member countries – which diminishes Europol’s effectiveness.

**87. The Agencies, when engaged in fighting serious and organised crime abroad, make a real and valuable impact, as does their support to law enforcement organisations in the UK. However, due to limited resources, their contribution is less than it might be. The Committee has commented on this twice before<sup>52, 53</sup>, making the point that providing extra resources to combat serious crime has been shown to bring a demonstrable return to society. Drug, tobacco and people smuggling could be further combated and curtailed.**

**88. We repeat that assertion: providing the Agencies with additional resources not only recognises the contribution that they can make, but is a sound investment bringing net benefit to the Exchequer and the country.**

## Secure Communications

89. The previous Committee commented in the 2000–2001 Interim Report that the Investigator had reported on *Secure Communications within the FCO* within the intelligence context. As part of our work into 11 September related matters, we questioned the Agencies and Departments to see if the UK had enough secure communications equipment. The Committee was \*\*\*\*\*<sup>54</sup>. Further we were told that \*\*\* which meant that it was \*\*\* and the same was true for \*\*\*\*\*. Whilst an interim solution is being introduced this year, no funding has been identified \*\*\*.

90. The second major \*\*\* were told that, while there have been \*\*\* this was by no means as simple as it sounded and exposed a number of problems.

---

52. Cm 4532.

53. Cm 4897.

54. Evidence from GCHQ, April 2002.

91. **The Committee is concerned that the UK does not have sufficient secure communications equipment \*\*\***

**\*\*\*. We believe that funding must be identified, as a priority, to meet the necessary \*\*\* requirements, including \*\*\*, and to allow timely and secure communications \*\*\***  
**\*\*\*.**

92. The Committee was given a copy of the review undertaken by Sir Edmund Burton on the UK Information Security Capability in November 2001. In this review, Sir Edmund stated that “there is no unified national process for delivering information assurance; no central sponsor figure in authority; and no agreement over *who* needs protecting against *what* and by *whom*”<sup>55</sup>. He recommended that a Central Sponsor, accountable to Government for setting the strategic direction for all stakeholders and for auditing performance, needs to be established, together with suitable oversight arrangements. Sir Edmund believes that a unified technology strategy, together with increased central resources for information assurance, is needed. The Committee has noted that the e-Envoy, Mr Andrew Pinder, has just been appointed as the Central Sponsor. **The Committee is concerned that the provision of an effective Information Security Capability may be hampered by a lack of central strategic direction and funding for a shared capability. We recommend that the matter is addressed as a matter of urgency and we will report on this next year.**

## Committee Matters

### *The Investigator*

93. The Investigator, Mr John Morrison, has continued to be a valuable asset to the Committee. In the Interim Report produced by the previous Committee, it was announced that the Investigator would investigate Scientific and Technical Research and Development supported by the Agencies and how the roles discharged by Inspectors-General in other countries are met in the UK Agencies. The Committee has considered both these reports and has reached the following conclusions:

#### **A. Agencies’ Scientific and Technical Research and Development Work**

**The Committee is satisfied with the structures established between the relevant bodies, including the Agencies and the MoD, to cover the Agencies’ scientific and technical research and development work.**

---

55. *Review of UK National INFOSEC Capability, 30 November 2001.*

However, the Committee believes that there could be value in re-examining closer relationships between \*\*\*

\*\*\*

\*\*\*.

## B. Discharge of Inspectors-General Roles in the UK Intelligence System

The Committee noted that the Investigator did not identify any significant shortcomings in the UK intelligence and security oversight system as a whole when compared to those countries in which Inspectors-General had responsibility for oversight of intelligence and security. A summary of the report can be found at Appendix 3.

One key area is Internal Audit (IA), which in other countries is an important IG function and is separate from Government or Parliamentary audit functions as carried out by the General Accounting Office in the US or the National Audit Office (NAO). In the UK, every department and agency is required to have an internal audit system and the Government Internal Audit Manual (GIAM) includes the audit of inter-departmental systems and agreements, and thus potentially covers the JIC processes. The NAO consider that IA within the Agencies is conducted effectively and errors are identified, and the Investigator found nothing to cast doubt on this judgement. The JIC processes, through which the Agencies are tasked by customers and supply intelligence to them, have not been subject to IA. **The Committee recommends that the JIC processes should be subjected to the disciplines of the Internal Audit process for inter-departmental systems, as prescribed in the Government Internal Audit Manual.**

The Committee noted that neither SIS nor the Security Service had carried out – or intended to carry out – audits of their new headquarters building projects to find out, after a period of several years, whether the assumed benefits of the moves had in fact materialised. Such retrospective audits might, by identifying any systemic errors in the starting assumptions, help future projects. **The Committee recommends that for major programmes, such as GCHQ's New Accommodation Programme, an assessment is made of the long-term financial and other benefits, and of whether these expectations have been fulfilled.**

### *Tasking the Investigator*

94. During the period 2001–2002, this Committee tasked the Investigator to conduct investigations into recruitment, retention and career development in the Agencies and The Joint Working Initiative, which was established to identify possible joint working

arrangements within two or three Agencies and completed its three years in April 2002. These reports have been completed and the Committee is raising the key findings and conclusions with the Agencies.

**95. As part of the Committee's work on security, we tasked the Investigator to review the US report "A Review of FBI Security Programs" conducted by the Commission for Review of FBI Security Programs, chaired by William H. Webster. The Investigator reviewed the report's recommendations in the light of previous Committee Reports and investigations and has briefed the Committee. The Committee will be taking these matters further and we will be reporting in due course.**

## Conclusions and Recommendations

- A. The Committee has been impressed by the Agencies' work during the period covered by this Report. The Committee found it useful to meet some of the Agencies' staff who had been involved in the follow-up work to the 11 September attacks, as well as other areas, and the Committee saw the dedication with which they go about their work. While this Report will highlight the areas about which the Committee has concerns, as that is the purpose of oversight, it must not overshadow the tremendous efforts made by the Agencies' staff, sometimes at great personal risk, to gain valuable secret intelligence for the UK. This intelligence safeguards national security, economic wellbeing and prevents and detects serious organised crime. It significantly reduces the threat to the UK and its citizens.

### National Intelligence Machinery

- B. This Committee recommends that CSI meets at least annually. We suggest that these meetings review the UK's Requirements and Priorities for Secret Intelligence, agree the Agencies' budgets and receive briefings on current threats from the Agencies.
- C. The Committee is aware that the SCOPE programme has yet to reconcile different requirements from different participants. We recommend both that the key requirements are finalised and that the funding is agreed as soon as possible. We will continue to monitor the situation.

### Administration

- D. The Committee believes that there is still a need to see the confidential annexes to the Commissioners' reports, redacted as necessary, in order to fulfil its statutory requirement to oversee the Agencies' administration processes.
- E. The Committee notes that the Commissioners now have sufficient Secretariat support for their work. However, we are concerned that, when the provisions covering communications data in the Regulation of Investigatory Powers Act 2000 (RIPA) are brought into force, the Interception of Communications Commissioner may well be overwhelmed by authorisations which he is required to examine as part of his statutory remit. The Committee recommends that additional staff are put in place within the Secretariat before the provisions are enacted to avoid repeating the unacceptable delays that occurred in 2000 with the Investigatory Powers Tribunal and its predecessors.
- F. The Committee welcomes the affiliation between the SIS Service Staff Association and the First Division Association.

## Expenditure

- G. The Committee welcomes the speed with which the Treasury was able to find additional funding for the Agencies following the 11 September attacks.
- H. The Committee believes that, as the Treasury is fully involved in the setting of the requirements and priorities for the Agencies, it should ensure that the Agencies are funded to be able to meet in full the demands placed on them.
- I. The Committee was concerned to hear that the Treasury believed that it was for the MoD alone to judge the priority of imagery rather than an inter-departmental approach. The Committee<sup>56, 57</sup> believes that imagery meets a national requirement and as such Government must consider it as a whole, perhaps through CSI. We believe that the Government needs to ensure that this vital capability is not only maintained but also enhanced.
- J. All the Agencies are now embarking on major IT projects which will need careful management to ensure that defined requirements are established and that the systems meet the Agencies requirements and are to cost and time. The Agencies are also employing significant numbers of consultants to assist with these projects. We will monitor these major IT projects and report in due course.
- K. The Comptroller and Auditor General wrote, during the audit of the 2000/01 Accounts, "I have not obtained all the necessary information and explanations that I considered necessary for the purposes of my audit; and I was unable to determine whether proper accounting records had been maintained"<sup>58</sup>. This resulted in the GCHQ Accounts being qualified. The Committee recommends that the Director GCHQ, the Cabinet Secretary and the Foreign Secretary seek to assure themselves that appropriate management processes, controls and qualified staff have now been put in place.
- L. The Committee is concerned that, in order to keep within the agreed relocation budget, GCHQ may be forced to reduce its operational effectiveness and agreed service to its customers. We would not wish to see this happening, especially after the 11 September attacks.

## Policy

- M. The Committee will examine the use of intercepted material and communications data, together with the scope of legislation, in the next year and report further.

---

56. Cm 4897.

57. Cm 5126.

58. *Certificate of the Comptroller and Auditor General to the Chairman of the Committee of Public Accounts, 26 February 2002.*

- N. The Committee supports the policy of not tapping the telephones of Members of both Houses and believes that it is important that it is not eroded in any way. The Committee believes that if the policy is ever changed or altered then Parliament would need to be informed as soon as it was compatible with the security of the country to do so.
- O. The Committee believes that reductions in the Agencies' funding during the 1990s, together with staff shortages that were being addressed after the SR2000 settlement, meant that the Agencies were resource limited and operating under financial pressures prior to the 11 September attacks.
- P. The Committee concludes, with hindsight, that the scale of the threat and the vulnerability of Western states to terrorists with this degree of sophistication and a total disregard for their own lives was not understood.
- Q. The Committee believes that the Agencies responded very rapidly to the terrorist attacks, appropriately devoting both additional staff and resources to securing the UK and tracking down the perpetrators of the attacks. The Committee met the staff involved and their determination and ability impressed us.
- R. The Committee supports and wishes to see the collaborative work undertaken by the Agencies and intelligence agencies abroad being vigorously pursued. Such co-operation and co-ordination is vital in today's fight against terrorism and we welcome the progress that has already been made.
- S. We are concerned that the Agencies do not have sufficient flexibility to cover all the languages they need to cover.
- T. Reductions in coverage are causing intelligence gaps to develop, which may mean that over time unacceptable risks will arise in terms of safeguarding national security and in the prevention and detection of serious organised crime. The Agencies must be given sufficient resources to enable them not only to fill the staff vacancies that have been created but also to expand sufficiently to ensure that they can meet the new demands now being placed on them.

### Serious Organised Crime

- U. The Agencies, when engaged in fighting serious organised crime abroad, make a real and valuable impact, as does their support to law enforcement organisations in the UK. However, due to limited resources, their contribution is less than it might be. The Committee has commented on this twice before<sup>59, 60</sup>, making the point that providing extra resources to combat serious crime had been shown to bring a

---

59. Cm 4532.

60. Cm 4897.

demonstrable return to society. Drug, tobacco and people smuggling could be further combated and curtailed.

- V. We repeat the assertion that providing the Agencies with additional resources not only recognises the contribution that they can make, but is a sound investment bringing net benefit to the Exchequer and the country.

### Secure Communications

- W. The Committee is concerned that the UK does not have sufficient secure communications equipment \*\*\*

\*\*\*. We believe that funding must be identified, as a priority, to meet the necessary \*\*\* requirements, including \*\*\*, and to allow timely and secure communications \*\*\*

\*\*\*.

- X. The Committee is concerned that the provision of an effective Information Security Capability may be hampered by a lack of central strategic direction and funding for a shared capability. We recommend that the matter is addressed as a matter of urgency and we will report on this next year.

### Investigator's Reports

- Y. The Committee is satisfied with the structures established between the relevant bodies, including the Agencies and the MoD, to cover the Agencies' scientific and technical research and development work. However, the Committee believes that there could be value in re-examining closer relationships between \*\*\*

\*\*\*.

- Z. The Committee recommends that the JIC processes should be subjected to the disciplines of the Internal Audit process for inter-departmental systems, as prescribed in the Government Internal Audit Manual.

- AA. The Committee recommends that for major programmes, such as GCHQ's New Accommodation Programme, an assessment is made of the long-term financial and other benefits, and of whether these expectations have been fulfilled.

- BB. As part of the Committee's work on security, we tasked the Investigator to review the US report "A Review of FBI Security Programs" conducted by the Commission for Review of FBI Security Programs, chaired by William H. Webster. The Investigator reviewed the report's recommendations in the light of previous Committee Reports and investigations and has briefed the Committee. The Committee will be taking these matters further and we will be reporting in due course.

## Future Programme of Work

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

- ⌘ the role and function of the National Intelligence Machinery, including IT developments;
- ⌘ recent legislation and its usefulness to the Agencies;
- ⌘ the progress of the GCHQ New Accommodation Programme;
- ⌘ the work of the Agencies to counter the proliferation of Weapons of Mass Destruction; and
- ⌘ the work of the Agencies against serious organised crime.

We also propose to examine the developments in the Agencies' work in Information Warfare and we have now tasked the Investigator to conduct investigations into who collects, analyses and assesses intelligence and into the Agencies' business processes. The Investigator is due to report back to the Committee on these matters in the autumn.

## APPENDIX 1

# THOSE WHO HAVE GIVEN ORAL EVIDENCE

## MINISTERS

Rt. Hon. Jack Straw, MP – Foreign Secretary  
Rt. Hon. David Blunkett, MP – Home Secretary  
Rt. Hon. Geoff Hoon, MP – Defence Secretary  
Rt. Hon. Andrew Smith, MP – Chief Secretary to the Treasury  
Rt. Hon. The Lord Goldsmith, QC – Attorney General

## OFFICIALS

### CABINET OFFICE

Mr John Scarlett, CMG OBE  
Other Officials

### SECRET INTELLIGENCE SERVICE

Sir Richard Dearlove, KCMG OBE  
Other Officials

### GOVERNMENT COMMUNICATIONS HEADQUARTERS

Mr Francis Richards, CMG CVO  
Other Officials

### SECURITY SERVICE

Sir Stephen Lander, KCB  
Other Officials

### FOREIGN AND COMMONWEALTH OFFICE

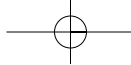
Mr Stephen Wright  
Mr Matthew Kidd

### HOME OFFICE

Mr John Warne  
Other Officials

### MINISTRY OF DEFENCE

Air Marshal Joe French, CBE RAF  
Mr Simon Webb  
Mr David Ferbrache



**HM TREASURY**

Mr William Nye

Mr Jonathan Stephens

**NATIONAL AUDIT OFFICE**

Mr Martin Daynes

Mr Bob Burwood

**LEGAL SECRETARIAT TO THE LAW OFFICERS**

Mr David Brummell

Ms Susan Ross

**HM CUSTOMS AND EXCISE**

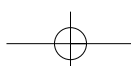
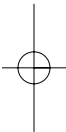
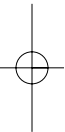
Mr Paul Evans

**NATIONAL CRIMINAL INTELLIGENCE SERVICE**

Mr John Abbott, QPM CBE

**NATIONAL CRIME SQUAD**

Mr William Hughes



## APPENDIX 2

### REASONS FOR THE FOREIGN SECRETARY AND THE HOME SECRETARY SIGNING THE DATA PROTECTION ACT 1998 s28 (NATIONAL SECURITY) EXEMPTION CERTIFICATE COVERING PERSONAL DATA PROCESSED BY THE INTELLIGENCE AND SECURITY COMMITTEE AND ITS SECRETARIAT

#### 1. Introduction

1.1 A section 28 certificate was signed by the Foreign Secretary and the Home Secretary for the Intelligence and Security Committee. This document explains the reasons they did so.

1.2 Before signing the certificate the Ministers considered the following factors:

- the DPA, its national security exemptions and the role of the National Security Panel of the Information Tribunal;
- the functions of the Intelligence and Security Committee in relation to the safeguarding of national security;
- why secrecy is essential in the work of the Intelligence and Security Committee and the damage or potential damage that can be done to national security if compromised;
- the need and the use of the “neither confirm nor deny” policy by the Government;
- the test that should be used to balance the need to safeguard national security and the purposes of the DPA;
- the form and scope of the certificate;
- the checks, procedures and reporting obligations placed on the Intelligence and Security Committee as conditions of their use of the certificate; and
- other points on the Intelligence and Security Committee’s need for use of exemptions under the DPA.

These factors are explained below.

1.3 This document focuses on the use of the national security exemption from the entitlement of an individual, under section 7 of the DPA, to be told by a data controller whether or not that data controller holds personal data on that individual

and, if held, provide information on the data being held. A subject access request will, almost inevitably, be the first step for anyone concerned by the possibility of the Intelligence and Security Committee processing personal data on them. The Intelligence and Security Committee is seen to be a data controller, with the Secretariat under the Clerk of the Committee as the data processor.

## **2. The DPA, its national security exemptions and the role of the National Security Panel of the Information Tribunal (“Tribunal”)**

- 2.1 The DPA came into force on 1 March 2000. The DPA made new provisions for the regulation of the processing of information relating to the individuals, including holding, use or disclosure of such information.
- 2.2 Section 7 of the DPA created a general entitlement for an individual to ask and be told by anyone who decides on the purpose of processing personal data whether personal data on them is being processed, which includes being held, and if it is be told certain information about that data. This entitlement to ask and be told in this way is known as “subject access”. The main rationale for subject access is so an individual can satisfy themselves to what, if any, personal data is being processed about them; that any processing is done for a proper purpose; that the data is accurate; and to whom the data may be disclosed. If dissatisfied with the outcome of their request the individual can then take corrective action.
- 2.3 The DPA recognises that there are certain circumstances when it would be inappropriate to comply with certain of the DPA’s provisions and therefore provides a number of exemptions. One, at section 28 of the DPA, exempts personal data from a number of provisions, including those of subject access, if the exemption is required for the purpose of safeguarding national security.
- 2.4 Section 28 of the DPA also provides that a Minister of the Cabinet or the Attorney General or the Advocate General may sign a certificate as conclusive evidence of the need for the use of the national security exemption. The certificate may identify the personal data to which it applies by means of a general description and may cover personal data processed after the date the certificate came into effect. Such a certificate will channel appeals against the certificate or its coverage to the Tribunal for consideration and determination.
- 2.5 The Tribunal considers appeals against a section 28 certificate by applying the principles used by the court on a judicial review. If the Tribunal determines that the Minister did not have reasonable grounds for issuing the certificate or the actions in issuing the certificate were inappropriate for the purpose the Tribunal may quash the certificate.

### **3. The functions of the Intelligence and Security Committee and in relation to the safeguarding of national security**

- 3.1 The Intelligence and Security Committee is a statutory body of nine parliamentarians established by the Intelligence Services Act 1994. The Committee examines the expenditure, administration and policy of the Security Service, the Secret Intelligence Service and the Government Communications Headquarters (GCHQ). The Committee is required to report at least annually to the Prime Minister, although it can submit reports to him at any time. The Prime Minister is required to lay before each House of Parliament a copy of the annual report. However, after consultation with the Committee, the Prime Minister may exclude any matter in a report that would be prejudicial to the continuing discharge of the functions of the three intelligence and security Agencies. The Committee is supported by a small secretariat, headed by the Clerk to the Committee, in discharging its functions.
- 3.2 In the preparation of its reports to the Prime Minister, and as part of its work under the Intelligence Services Act 1994, the Committee takes evidence and briefings from the three intelligence and security agencies, the Ministry of Defence (the Defence Intelligence Staff in particular), the Joint Intelligence Organisation of the Cabinet Office and a number of Law Enforcement Organisations.
- 3.3 Like the intelligence and security agencies, the Intelligence and Security Committee maintains its own liaison with analogous organisations in Allied countries. Such liaison arrangements follow access to information and analysis on intelligence, security and oversight matters. The Committee regards it as important to be able to have constructive discussions with countries to enable proper and robust systems of legislature based oversight to exist for intelligence and security organisations.
- 3.4 The Committee does not investigate individuals.

### **4. Why secrecy is essential in the Intelligence and Security Committee and the damage or potential damage that can be done to national security when secrecy is compromised**

- 4.1 It is fundamental to the integrity of intelligence and security related material information from whatever source that the information is kept in confidence and not disclosed outside the intelligence and secrecy community. The inappropriate disclosure of such information could cause harm or distress and result in putting the continued supply from one or other of the sources at risk.
- 4.2 Where personal data features as part of the information that is used to reach a decision, whether a collective decision or otherwise, relating to national security it is essential that the decision-making process can take place without the fear of the

information being disclosed in an unauthorised and inappropriate manner. The same applies to such information recorded or stored for whatever other purpose.

- 4.3 Depending on the nature and source of the personal data involved the disclosure of such information could lead to varying degrees of damage, up to and including exceptional damage, to the continuing effectiveness or security of security or intelligence operations. The same could also apply to the operational effectiveness or security of United Kingdom or allied forces.

## **5. The need for and use of the “neither confirm nor deny” policy**

- 5.1 It has been the policy of successive governments neither to confirm nor to deny suggestions put to them on the work of the intelligence and security agencies or such matters in general. The policy, put simply, is a way to preserve secrecy by giving a vague and non-committal answer.

- 5.2 The need for such a policy and Parliament’s acceptance of this is reflected in legislation. Such legislation includes the Official Secrets Acts 1911 to 1989. The 1989 Act makes it unlawful for any member of the Intelligence and Security Committee or of the ISC Secretariat to make any unauthorised disclosure of information held by virtue of their work. It also includes the predecessor of DPA, the Data Protection Act 1984. The Code of Practice on Access to Government Information, Second Edition 1997, gives “information whose disclosure would harm national security” as a category of information that is exempt from the provisions of the Code.

## **6. The test that should be used to balance the need to safeguard national security and the purposes of the DPA**

- 6.1 Section 28 of the DPA states that “Personal data are exempt . . . if the exemption . . . is required for the purposes of safeguarding national security”. The term “national security”, however, is not defined. Both domestic and European courts have accepted that the Government has significant discretion in what constitutes national security. In addition when considering safeguarding national security the courts have accepted (see the House of Lords’ Judgement of 11 October 2001 in the appeal of Shafiq Ur Rehman against deportation) that it is proper to take a precautionary approach. That is it is not necessary only to consider circumstances where actual harm has or will occur to national security, but also to consider preventing harm occurring and avoiding the risk of harm occurring.

6.2 Even so the Foreign Secretary and the Home Secretary have balanced the need to safeguard national security against the purposes and entitlements conferred by the DPA. This was balanced against the following factors:

- the consequences of an individual not knowing whether the Intelligence and Security Committee processes personal data on them provided in the course of the Committee's work;
- if processed, an individual not knowing the purpose why it is processed, whether the data is accurate and to whom the data may be disclosed;
- the consequences of, for practical purposes, denying an individual the opportunity to challenge the purpose for processing, the accuracy of the data and to whom the data may be disclosed;
- the consequences to national security of the individual not correcting inaccurate data on him or her; and
- the consequences of the Information Commissioner or the courts not having a role in examining the use of the national security exemption in regard to the provisions of the DPA.

## **7. The form and scope of the certificate**

7.1 As expressly permitted by the DPA, the certificate identifies personal data by general description and it covers personal data processed after the date that the certificate came into effect. A general description certificate reflects the primary need for secrecy in the Intelligence and Security Committee to protect national security. Without this an individual certificate would be required for every appeal against the Intelligence and Security Committee's use of the national security exemption. In many instances the Intelligence and Security Committee will need to use the exemption to preserve the neither confirm nor deny policy or to limit the extent of disclosure. The administrative burden of individual certificates, and the fact that only members of the Cabinet or the Attorney General or the Advocate General may sign such certificates, were also factors taken into consideration in the form and scope of the certificate.

7.2 The terms of the certificate were drafted to reflect the functions of the Intelligence and Security Committee and the terms of the DPA. A proportionate approach was adopted with careful consideration being given to the range of exemptions required in respect of each of the different categories so that only those that were absolutely necessary would be included.

7.3 To further insure that as much personal data as possible is disclosed the Foreign Secretary and the Home Secretary requires the ISC Secretariat to give due consideration to the:

- age of a document;
- continued validity of any protective marking assigned to the document;
- source of the personal data; and
- context in which the personal data is given.

## **8. The checks, procedures and reporting obligations on the Intelligence and Security Committee as conditions of their use of the certificate**

8.1 The Foreign Secretary and the Home Secretary before signing the certificate considered the Intelligence and Security Committee's handling arrangements for dealing with subject access requests made under the DPA.

8.2 In summary the ISC Secretariat is required to examine each subject access applications and to:

- decide whether the use of the neither confirm nor deny approach is necessary;
- decide, if not, to what extent the national security exemption is necessary.

The Clerk to the Committee is required to report back to the Foreign Secretary and the Home Secretary on the working of these arrangements.

8.3 The neither confirm nor deny approach will only be used where there is a particular and identified need to do so and there are no other alternatives. It is also relevant that there could be occasions when disclosure is required.

## **9. Other points on the Intelligence and Security Committee's need for use of exemptions under the DPA**

9.1 When signing the certificate the Ministers noted that other exceptions under the DPA might well also apply to the personal data covered by the certificate.

9.2 It was further recognised that the signing of the certificate did not exclude the possible necessity of signing other national security certificates relating to personal data processed by the Intelligence and Security Committee.

## **10. Conclusion**

10.1 Having considered the above factors the Foreign Secretary and the Home Secretary decided it was right to sign the certificate on behalf of the Intelligence and Security Committee.

APPENDIX 3

# INSPECTORS-GENERAL FUNCTIONS IN THE UK INTELLIGENCE SYSTEM

## INTRODUCTION

1. In the Committee’s visits to the US and discussions with other oversight bodies it has taken a particular interest in the responsibilities of Inspectors-General (IGs). These form part of the oversight structure in the US, Canada, Australia, New Zealand and South Africa. These IGs’ responsibilities vary widely as shown below:

### Comparison of Inspectors-General and ISC Functions, Freedoms and Powers

Inspectors-General Functions	USA	Canada	Australia	New Zealand	South Africa	ISC Functions
Ensures compliance with current legislation	Exists	Exists	Exists	Exists	Exists	Does not exist
Ensures compliance with standards of propriety	Exists	Exists	Exists	Exists	Exists	Exists
Carries out audits, investigations and inspections	Exists	Exists	Exists	Exists	Exists	Exists
Prevents and detects waste, fraud and abuse	Exists	Does not exist	Does not exist	Does not exist	Inapplicable or unclear whether exists	Does not exist
Promotes economy, effectiveness and efficiency	Exists	Does not exist	Does not exist	Does not exist	Does not exist	Exists
Reviews compliance with executive directives and operational policies	Exists	Exists	Exists	Does not exist	Exists	Does not exist
Ensures compliance with warrant authorisations	Does not exist	Inapplicable or unclear whether exists	Exists	Exists	Does not exist	Does not exist
Reviews operational activities	Exists	Exists	Exists	Exists	Does not exist	Does not exist
Reviews pending legislation and regulation	Exists	Does not exist	Exists	Does not exist	Does not exist	Exists
Reports regularly to the agency head(s)	Exists	Does not exist	Does not exist	Does not exist	Does not exist	Does not exist
Reports regularly to executive, legislature or oversight commission	Exists	Exists	Exists	Exists	Exists	Exists
Reports in response to requests by legislature or oversight commission	Exists	Exists	Exists	Exists	Exists	Exists
Investigates complaints about the agency	Exists	Does not exist	Exists	Exists	Exists	Exists
Ensures proper regard to human rights	Exists	Does not exist	Exists	Does not exist	Inapplicable or unclear whether exists	Exists
Ensures compliance with regulations on release of records & information	Exists	Does not exist	Exists	Does not exist	Inapplicable or unclear whether exists	Does not exist

**Key to Functions, Freedoms and Powers**

Exists  Inapplicable or unclear whether exists  Does not exist 

Inspectors-General Freedoms and Powers (F/P)	USA	Canada	Australia	New Zealand	South Africa	ISC F/P
Is immune from arbitrary sacking	■	■	■	■	■	■
Hires and controls own staff and contract resources	■	■	■	■	■	■
Has ready access to the agency head(s)	■	■	■	■	■	■
Has access to all records and information of the agency	■	■	■	■	■	■
Initiates investigations on own initiative	■	■	■	■	■	■
Issues subpoenas for information/documents outside the agency	■	■	■	■	■	■
Administers oaths for taking testimony	■	■	■	■	■	■

**Key to Functions, Freedoms and Powers**

Exists ■ Inapplicable or unclear whether exists ■ Does not exist ■

2. The Committee wanted to identify who or what organisation carried out each of these “IG functions” for the UK intelligence and security Agencies. The Agencies provided the Committee with memoranda, on the basis of which the Committee selected eight areas for investigation. The Investigator’s findings on each of these are covered in more detail in separate sections of the report and the Committee’s conclusions on each are set out below.

## SECTION 1: ADHERENCE TO LEGISLATION AND PROCEDURES GOVERNING AGENCY ACTIVITIES

3. A key function for any IG overseeing an intelligence agency is to ensure its activities comply with current legislation and meet appropriate standards of propriety. Each of the Agencies in the UK has strong internal control mechanisms to ensure that their activities conform to all relevant legislation. These mechanisms include written instructions, staff training, record keeping and advice from the Legal Advisers’ teams. The current external control mechanism was set up by the Regulation of Investigatory Powers Act 2000 (RIPA 2000), which provided for two Commissioners: the Interception of Communications Commissioner and the Intelligence Services Commissioner, who have unrestricted access to Agency records and staff and report annually to the Prime Minister. Prior to RIPA 2000 the different Commissioners’ powers were established under the Interception of Communications Act 1984, the Security Services Act 1989 and the Intelligence Services Act 1994.

4. Though it is tempting to see the two Commissioners as “British Inspectors-General”, they themselves reject that description as implying a wider range of powers than they in fact possess. The Committee believes that the Commissioners do carry out part of the role assigned to the IG in other countries by reviewing the lawfulness of warranted Agency

activities. It should be noted that several other jurisdictions require judicial approval of interception, and in part the Commissioner's role is regarded as an additional safeguard within a system of executive authorisation. In essence, the laws governing the Agencies' activities permit them to undertake actions under warrant which would be illegal if performed by a member of the public. The Agencies must ensure – and the Commissioners check – that their operations have complied fully with current legislation. The Commissioners then report to the Prime Minister on their findings and their reports are published. Confidential annexes to the reports are not published and this Committee has not been given access to them. The Committee was informed that actions have never been authorised in the face of contrary advice from the Agencies' Legal Advisors. The UK systems relies on a combination of internal and external control systems to carry out the IG function of ensuring that the Agencies adhere to the legislation and procedures governing their activities.

## **SECTION 2: EDUCATION OF STAFF ON THEIR RESPONSIBILITIES AND RIGHTS**

5. This is not strictly an IG function, but the IGs' role requires that the staff of the establishments they cover are fully aware of their legal and ethical responsibilities and their personal rights, including the right to bring any evidence of wrongdoing to the IG's attention. This imposes a requirement upon an Agency to ensure that all staff are appropriately educated through training programmes and other means. In the UK each of the Agencies has a broadly-based induction training package followed by more specialised training, either as part of a staff member's career development or to meet particular job requirements. Increasingly, the Agency intranets are being used as training tools, with staff being encouraged to access and "pull" information rather than waiting for a course to "push" it at them. The Agency staff also have access to the Legal Advisor and to the Staff Counsellor, with whom they can consult on any matters.

6. The Committee concludes that, insofar as an IG has an explicit or implicit responsibility to ensure that staff are aware of their responsibilities and rights, this function is carried out in the UK by a combination of the Agencies' own training programmes and by the unrestricted access which Agency staff have to the Staff Counsellor.

## **SECTION 3: INTERNAL AUDIT**

7. Internal Audit (IA) is an important IG function and is separate from Government or Parliamentary audit functions as carried by the General Accounting Office in the US or the National Audit Office (NAO) here. In the UK, every department and agency is required to have an internal audit system; the Treasury states that "The prime function of internal audit is to provide Accounting Officers with assurance on the internal control system". In recent years the scope of IA in the UK has broadened to cover wider control,

corporate governance and risk management issues, and to provide an impartial internal consultancy service. It should be noted that the Government Internal Audit Manual (GIAM) includes the audit of inter-departmental systems and agreements, and thus potentially covers the JIC process.

8. The Committee noted that neither SIS nor the Security Service had carried out – or intended to carry out – audits of their new headquarters building projects to find out, after a period of several years, whether the assumed benefits of the moves had in fact materialised. It could be argued that after a decade the findings would be of interest only, but such retrospective audits might, by identifying any systemic errors in the starting assumptions, help future projects.

9. The NAO consider that IA within the Agencies is conducted effectively and errors are identified, and the Investigator found nothing to cast doubt on this judgement. But, despite the guidance in the GIAM, inter-departmental systems, and particularly the JIC process through which the Agencies are tasked by customers and supply intelligence to them, have not been subject to IA.

#### **SECTION 4: SECURITY POLICIES AND PROCEDURES**

10. An important task for any IG responsible for an intelligence or security agency is to ensure that it maintains effective security policies and procedures; security audits may be part of an IG's routine work or carried out as a special review. In the UK it is government policy that security is the responsibility of each individual government Department or Agency, whose head is ultimately answerable for the security of the organisation and its activities. The centre provides the Agencies with a general security framework, but does not mandate their detailed security policies and procedures; not does it monitor the effectiveness of their security arrangements in practice. Given the nature of their work, it is not surprising that all three Agencies put the greatest stress on effective security and see it as an integral part of their working culture. Each Agency has a Director of Security whose staffs are responsible for checking the effectiveness of the security regime and recommending improvements; there is no equivalent of an independent IG within the organisation.

11. There are two external bodies who essentially fulfil the IG's security oversight function: the ISC and the Security Commission. The ISC's oversight of the Agencies' policies, administration and finances includes their security policies and procedures, in which the Committee has always taken a keen interest. It has not so far investigated specific breaches of security in detail, but has followed up their implications. The Security Commission has traditionally been charged, by the Prime Minister, with investigating and reporting upon major breaches of security such as espionage cases, although there is no legal requirement for the Commission to report. The Committee

believes that, between them and the Security Commission, most of the security-related oversight functions of an IG are carried out.

## **SECTION 5: INVESTIGATING AND RESPONDING TO STAFF AND PUBLIC COMPLAINTS**

12. Inspectors-General would usually be expected to investigate a complaint from a member of an intelligence agency or the public and decide whether it was justified or not. In principle, once the normal managerial lines of communication had been exhausted, the Staff Counsellor could investigate a complaint for Agency members of staff. However, he sees his prime functions as mediation and reconciliation rather than investigation and adjudication. The specially constituted Employment Tribunal will be able to deal with individual grievance cases from Agency staff in which could otherwise have gone to a normal tribunal, but is limited to the area of employment law, and its procedures can impose security-related limitations on the applicant's access to the evidence against them. To date, the ISC has only investigated a complaint by an Agency employee because the Agency asked it to do so and the Committee agreed it would be appropriate to follow up the wider issues of administration, finance or policy raised by the complaint. The Commissioners' function is to ensure that the activities of the Agencies conform to the relevant Acts and not to pursue individuals' complaints.

13. For every member of the public, the Investigatory Powers Tribunal, established under Regulation of Investigatory Powers Act 2000, provides the UK with a body which in effect exercises an IG's responsibility to investigate an individual's complaints that an Agency's activities had adversely affected them. The threshold for considering a complaint is set very low, with the Committee informed that only in the most extreme cases would the Tribunal reject a complaint on the grounds that it was frivolous or vexatious. It must be stressed, however, that the IPT will only respond to the individual claiming to be directly affected by an Agency's conduct, and it will not look into reports of activities affecting third parties. This means that the allegedly aggrieved party has to make the complaint. In producing its assessment, the IPT will determine the complaint by applying the same principles as would be applied by a court on an application for judicial review, and report as necessary to the complainant whether or not anything unlawful had occurred. In preparing its assessment, the IPT can call on the Commissioners to support its work into allegations of wrong-doing.

## **SECTION 6: RELEASING REQUESTED INFORMATION TO INDIVIDUALS OR THE PUBLIC**

14. In the UK the release of Agency information to individuals or the public is subject to the provisions of the Data Protection Act 1998. One of the reasons that the Agencies can withhold information from disclosure is for the purposes of safeguarding National Security by means of a Certificate signed by a Secretary of State. This Certificate can be

examined by a specially constituted Tribunal, which can overturn the certificate if it believes that the data it covers is not related to National Security or that the Certificate is too general. Contrary to the situation in the US, the intelligence and security Agencies are excluded from the provisions of the UK Freedom of Information Act 2000, so there is no need for the exercise of an IG function in ensuring adherence to this legislation.

## SECTION 7: RECORDS AND ARCHIVES

15. Although this was not always the case, there are now satisfactory procedures for handling the Agencies' records and selecting those for permanent preservation, which will be further improved by the creation of Operational Selection Policies. The IG function, such as it is in this area, is exercised by the Lord Chancellor under the Public Records Act 1958, with practical advice on record management provided by the Public Record Office. The Committee noted that while the Security Service and GCHQ have a policy of releasing selected records to the Public Record Office, SIS have no plans to release any of their post-1909 records. All three Agencies are facing similar issues in moving from paper to electronic records, and while they do speak to each other, the establishment of a wider PRO/Agency Working Group on Electronic Intelligence Records to ensure that each participant learns as much as possible from the others is recommended. Such a body would also benefit from the involvement of other members of the Intelligence Community such as the DIS and JIO. The Investigator noted that all three Agencies help preserve their corporate memories through the production of internal classified histories and ad hoc reports, with GCHQ having the most structured programme.

## SECTION 8: AD HOC REPORTS

16. The Committee believes that, although there are no Inspectors-General in the UK system to produce ad hoc reports on Agency activities, there are several alternative mechanisms. They include:

- a. reports commissioned by an Agency itself as an internal aid to management;
- b. reports by an Agency to Ministers or officials;
- c. reports by external consultants at the direction of Ministers or officials;
- d. reports produced by the NAO either on their own initiative or at the request of the Chairman of the Public Accounts Committee; and,
- e. reports produced by the ISC and its Investigator at the Committee's initiative or in response to a request.

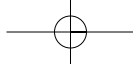
17. The Investigator judges that, of these, the ad hoc reports produced by the NAO and ISC on their own initiative are the most demonstrably independent and impartial. We believe that the addition of an Investigator has allowed us to pursue issues in greater

depth than if we had to rely on our own efforts and resources. While the Investigator does not have an IG's powers, in practice the Agencies have proved most co-operative; the knowledge that they can call for any operationally sensitive material to be removed from an Investigator's report before it goes to the Committee has encouraged them to be frank.

## OVERALL CONCLUSIONS

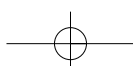
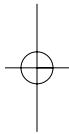
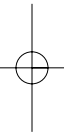
18. In the eight areas covered in this report, the IG functions are variously discharged in the UK intelligence system by the following formally constituted organisations, bodies and individuals, separately or in combination, all of whom operate within the "ring of secrecy":

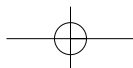
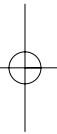
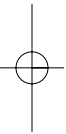
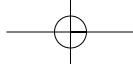
- (a) **The Agencies** themselves, including their internal control mechanisms and staff education programmes, Legal Advisers and Internal Audit teams.
- (b) **Ministers**, who prospectively authorise warrants and provide political approval for sensitive operations and are advised by their Departments.
- (c) **The Commissioners**: the Interception of Communications Commissioner and the Intelligence Services Commissioner, who retrospectively review the legality of Agency operations under the relevant legislation.
- (d) **The National Audit Office**, which is responsible for the financial audit of the individual Agencies' accounts and the consolidated account for the Single Intelligence Vote (SIV) and produces reports on specific Agency projects.
- (e) **The Cabinet Office**, which has responsibility for the SIV, the workings of the JIC system as a whole and provides a security framework for the Agencies.
- (f) **The Staff Counsellor**, who seeks to resolve the problems of individual Agency members of staff through discussion and advice.
- (g) **The Employment Tribunal** which has been specially constituted to hear employment grievances from Agency staff members.
- (h) **The Investigatory Powers Tribunal**, which considers complaints from members of the public under the Regulation of Investigatory Powers Act 2000.
- (i) **The Public Record Office**, which provides advice to the Agencies on the release and safe-keeping of their records.
- (j) **The Security Commission**, which investigates major breaches of security such as espionage cases.
- (k) **The Intelligence and Security Committee**, which reviews the policies, administration and finance of the Agencies and has developed a degree of *de facto* oversight of the UK Intelligence Community as a whole.



19. To these could be added the Attorney-General, who receives bimonthly reports on cases involving Agency staff, allowing the Law Officers to provide appropriate advice to the Agency concerned, and the Information Commissioner.

20. While an Inspector-General system appears far simpler than this lengthy list of diversified responsibilities in the UK, in practice the organisations and bodies involved cover all the IG functions under review. The Investigator did not identify any significant failings of the UK intelligence and security oversight system as a whole when compared to those countries in which Inspectors-General had responsibility for oversight of intelligence and security.







**Published by The Stationery Office Limited**

and available from:

**The Stationery Office**

(Mail, telephone and fax orders only)

PO Box 29, Norwich NR3 1GN

General enquiries 0870 600 5522

Order through the Parliamentary Hotline Lo-call 0845 7 023474

Fax orders 0870 600 5533

Email [book.orders@theso.co.uk](mailto:book.orders@theso.co.uk)

Internet <http://www.ukstate.com>

**The Stationery Office Bookshops**

123 Kingsway, London WC2B 6PQ

020 7242 6393 Fax 020 7242 6394

68-69 Bull Street, Birmingham B4 6AD

0121 236 9696 Fax 0121 236 9699

33 Wine Street, Bristol BS1 2BQ

0117 9264306 Fax 0117 9294515

9-21 Princess Street, Manchester M60 8AS

0161 834 7201 Fax 0161 833 0634

16 Arthur Street, Belfast BT1 4GD

028 9023 8451 Fax 028 9023 5401

The Stationery Office Oriel Bookshop

18-19 High Street, Cardiff CF1 2BZ

029 2039 5548 Fax 029 2038 4347

71 Lothian Road, Edinburgh EH3 9AZ

0870 606 5566 Fax 0870 606 5588

Accredited Agents

(See Yellow Pages)

and through good booksellers

ISBN ●