Intelligence and Security Committee

Annual Report 2009–2010

Chairman:
The Rt. Hon. Dr Kim Howells, MP

Intelligence and Security Committee

Annual Report 2009–2010

Chairman:

The Rt. Hon. Dr Kim Howells, MP

Intelligence Services Act 1994
Chapter 13

Presented to Parliament by the Prime Minister
by Command of Her Majesty
March 2010

Cm 7844

£14.35

ISBN: 9780101784429

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2354911 03/10

Printed on paper containing 75% recycled fibre content minimum.

From: The Chairman, The Rt. Hon. Dr Kim Howells, MP

INTELLIGENCE AND SECURITY COMMITTEE

35 Great Smith Street, London SW1P 3BQ

ISC 2009/10/078 05 March 2010

Rt. Hon. Gordon Brown, MP
Prime Minister
10 Downing Street
London
SW1A 2AA

Dear Prime Minister

I enclose the Intelligence and Security Committee's Annual Report for 2009–2010. This covers our work between August 2009 and March 2010.

The Committee has met on a total of 29 occasions during this time, taking oral and written evidence on the administration, policy and expenditure of the three intelligence and security Agencies.

In addition, I enclose our Review of the Government's draft 'Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees'.

I am grateful that you have agreed to publish both Reports before the House of Commons debate on our work on 18 March.

Yours

Kim

KIM HOWELLS

THE INTELLIGENCE AND SECURITY COMMITTEE

The Rt. Hon. Dr Kim Howells, MP (Chairman)

The Rt. Hon. Michael Ancram QC, MP

The Rt. Hon. Sir Menzies Campbell CBE QC, MP

Mr Ben Chapman, MP

The Rt. Hon. Lord Foulkes of Cumnock

The Rt. Hon. George Howarth, MP

The Rt. Hon. Michael Mates, MP

Mr Richard Ottaway, MP

Ms Dari Taylor, MP

The Intelligence and Security Committee (ISC) is an independent Committee, established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the three UK intelligence Agencies: the Security Service, the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ).

The Committee also examines the work of the Joint Intelligence Committee (JIC), the Assessments Staff and the Intelligence and Security Secretariat in the Cabinet Office, and the Defence Intelligence Staff (DIS) in the Ministry of Defence.

The Prime Minister appoints the ISC Members after considering nominations from Parliament and consulting with the leaders of the two main opposition parties. The Committee reports directly to the Prime Minister and through him to Parliament, by the publication of the Committee's reports. Sometimes we are asked to look into a matter, but most of the time we set our own agenda. We determine how and when we conduct and conclude our programme of work – this gives the Committee the freedom to pursue every avenue of inquiry to its satisfaction. Often this means that the Committee's inquiries are very detailed or wide-ranging.

The Committee has an independent Secretariat currently hosted by the Cabinet Office. The Committee also has a panel of three investigators: a General Investigator to undertake specific investigations covering the administration and policy of the Agencies; a Financial Investigator covering expenditure issues; and a Legal Advisor to provide the Committee with independent legal advice.

The Members of the Committee are notified under the Official Secrets Act 1989 and are given access to highly classified material in carrying out their duties. The Committee holds evidence sessions with Government ministers and senior officials (for example, the head of the Security Service). It also considers written evidence from the intelligence and security Agencies and relevant Government departments. This evidence may be drawn from operational records, source reporting, and other sensitive intelligence (including original records when relevant), or it may be memoranda specifically written.

The Prime Minister publishes the Committee's reports: the public versions have sensitive material that would damage national security blanked out ("redacted"). This is indicated by *** in the text. The Committee agrees what material will be blanked out with the Government, and to date no material has been excluded without our consent.

CONTENTS

INTRODUCTION

1. This Report details the work of the Intelligence and Security Committee ('the Committee') for the period from August 2009 to March 2010. The Committee has held 19 formal sessions and 10 other meetings during this period.[1]

2. During the reporting period the Committee has focused on three key areas:

- Examining and taking evidence on the policy, administration and expenditure of the three intelligence and security Agencies. We report on these matters here. (Due to the time spent on other work and a shorter Parliamentary session we have not this year examined all of the work of the broader UK intelligence machinery.)
- On 18 March 2009 the Prime Minister asked the Committee to review the guidance for the UK intelligence and security Agencies and armed forces on detainees. The Consolidated Guidance was received by the Committee on 18 November 2009. We took evidence from the Heads of SIS and the Security Service, the Foreign Secretary, the Home Secretary, the Secretary of State for Defence and the Attorney General and their officials. The outcome of our inquiry is contained in a separate report.
- Work to revisit those principles, policies and procedures which govern the work, status, remit and responsibility of the Committee and under which the Committee has and continues to operate, including identifying changes essential to safeguard the independence of the Committee.

3. In addition to its formal evidence sessions, the Committee visited all three intelligence and security Agencies and was represented at the International Intelligence Review Agency Conference in Australia in March 2010. As part of the Committee's programme of discussions with our overseas counterparts, we held bilateral discussions with parliamentarians and officials from Australia, Germany, Jordan and the US.

[1] *This is a shorter time frame than usual because of the impending General Election.*

THE COMMITTEE'S INDEPENDENCE

Background

4. It is a fundamental principle of our democracy that the Government and its agencies are held to account. The requirement to explain and justify actions encourages better thought out policy, better control of expenditure and adherence to accepted principles and practices. The oversight of intelligence and security Agencies is no different, and if anything is even more essential given that most of their work is kept secret from the general public.

5. In 1994, the Intelligence Services Act established a committee of parliamentarians to provide oversight of the administration, policy and expenditure of the three UK intelligence and security Agencies, a Commissioner to review the lawfulness of their actions and a Tribunal to investigate complaints.

6. The Committee is confident in its ability to hold the Agencies, and other bodies with an intelligence role, to account and to do so independently of Government. Nevertheless, over the last six months, questions have been raised about the independence of the Committee.

7. This has led us to revisit those principles, policies and procedures which govern the work, status, remit and responsibility of the Committee and under which the Committee has and continues to operate. According to the legislation which established the Committee, it can set its own procedures. These have, naturally, evolved over the last 16 years through written agreements and verbal assurances. It has become very clear to us, however, that corporate knowledge of these procedures within Government has been lost over time and there was now very little awareness of our procedures, some of which date back to when the Committee was first established. This has led in some cases to misunderstandings as to the statutory independence of the Committee and its work and the nature of the relationship between the Committee and the Prime Minister. It was therefore clear that our procedures needed to be set out formally, for the avoidance of doubt, and to ensure that the Committee has clarity in its future dealings with Government, and vice versa.[2]

Our proposals for the future

8. In drawing up the principles, policies and procedures it became clear to us that certain administrative arrangements (now 16 years old) were no longer appropriate and required not only updating but also changing if there was to be confidence in the independence of the Committee. These are:

i. the Committee must move to another 'host' department, that does not have such a substantive role with regard to the intelligence and security Agencies; and

ii. the Committee's budget must be similarly separated and instead linked to the Single Intelligence Account (SIA).

[2] *The Committee's principles and policies are included at Annex A.*

Host department

9. Although the Committee is a separate legal entity, it has been hosted by the Cabinet Office since it was set up in 1994. This was a matter of administrative convenience, since the Cabinet Office was a central department used to handling highly classified material and had suitably vetted staff.

10. However, the role of the Cabinet Office in terms of intelligence has grown substantially over the past 16 years, and the Committee's remit has similarly evolved to include the central intelligence machinery in the Cabinet Office. The relationship is, therefore, now very different. We now find ourselves sitting in a department that has a significant role in the UK intelligence community[3] which we oversee. That, obviously, is not appropriate. As a matter of principle, no matter what the circumstances, it clearly is not right to be hosted by an organisation that you have some role in overseeing and there is a danger that boundaries might not be respected.

11. The Committee has therefore recommended to the Prime Minister and Cabinet Secretary that it should be moved to another Government department: one without such a central role in security and intelligence matters. We believe this would serve to demonstrate that there is no link between the Committee and those it oversees, and would also, in our opinion, provide a much-needed separation.

Budget

12. As with its staff, accommodation and other resources, the Committee's budget is decided and allocated by the Cabinet Office. There is clearly a potential conflict of interest in requiring the Committee to go 'cap in hand' to those it oversees in order to get the resources it needs to oversee them.

13. In order to safeguard our budget, we have further recommended to the Prime Minister and Cabinet Secretary that it should be separated from the Cabinet Office, and instead linked as a set percentage of the SIA (although outwith the SIA itself). This would ensure that the Committee's activity and capabilities would grow or shrink in accordance with those it oversees (with a minimum threshold to ensure that fixed costs are covered), thus ensuring that the oversight function is proportionate to the work it oversees.

A. It is, in our view, absolutely fundamental that if the Committee is to maintain independence from Government we cannot continue to sit within, and depend upon, a Government department that now has such a central role regarding the intelligence and security Agencies, which we oversee.

B. The same argument applies to the Committee's budget, which should be set as a proportion of the intelligence and security Agencies' budgets, and should not be determined by an organisation which we oversee.

---

[3] *The intelligence functions of the Cabinet Office include: the Prime Minister's Security Adviser, the Intelligence, Security and Resilience Group (this also includes responsibility for the SIA), the Joint Intelligence Committee, the Assessments Staff, the Professional Head of Intelligence Analysis, and the National Security Secretariat.*

THE AGENCIES

The threat

14. On 20 July 2009, the Joint Terrorism Analysis Centre (JTAC) assessed that the threat to the UK from international terrorism should be reduced from 'Severe' to 'Substantial' – meaning that the threat of a terrorist attack remained a strong possibility, and may have occurred without warning.[4] On 22 January 2010, JTAC raised the threat level back up to 'Severe' – meaning that a terrorist attack is considered to be highly likely. The sources and the types of threats remain unchanged since we reported in our 2008–2009 Annual Report.[5]

The Single Intelligence Account

15. We reported in detail on the Single Intelligence Account (SIA) settlement for the current CSR period in our 2007–2008 Annual Report.[6] The combined budget for the three intelligence and security Agencies under the SIA for 2008/09 was £2,033m (an increase of 15% on the previous year).

16. Looking forward, the SIA for 2009/10 is £2,203m (an increase of 8%), and the 2010/11 settlement is £2,354m (a further increase of 7%). Funding for the period from 2011/12 onwards will be allocated in the next Spending Review (or equivalent process).

17. The Cabinet Office has informed the Committee[7] that it has, in conjunction with the three intelligence and security Agencies, taken a number of steps to begin preparing for the next spending round. These measures include the formation of a cross-Agency working group to facilitate engagement with the Treasury and a cross-Agency Spending Review working group to produce a co-ordinated single bid for the next spending round.

18. We questioned each of the Agencies in detail on their planning for the next spending round. Each of the Agency Heads recognised the challenging financial climate ahead:

i. The Director of GCHQ told us that:

There are obviously some tough financial targets ahead for all departments… My aim is that we should respond actively to funding pressures by reshaping the business in a more streamlined way.[8]

ii. The Director General of the Security Service told us that in order to prepare for "*a more austere financial climate*"[9] the Service had introduced a 'Living Within our Means' programme which aimed to minimise real-term expenditure.

---

4 *www.mi5.gov.uk*

5 *Cm 7807.*

6 *Cm 7542.*

7 *Letter from the Cabinet Office, 28 January 2010.*

8 *Oral Evidence – GCHQ, 9 February 2010.*

9 *Oral Evidence – Security Service, 26 January 2010.*

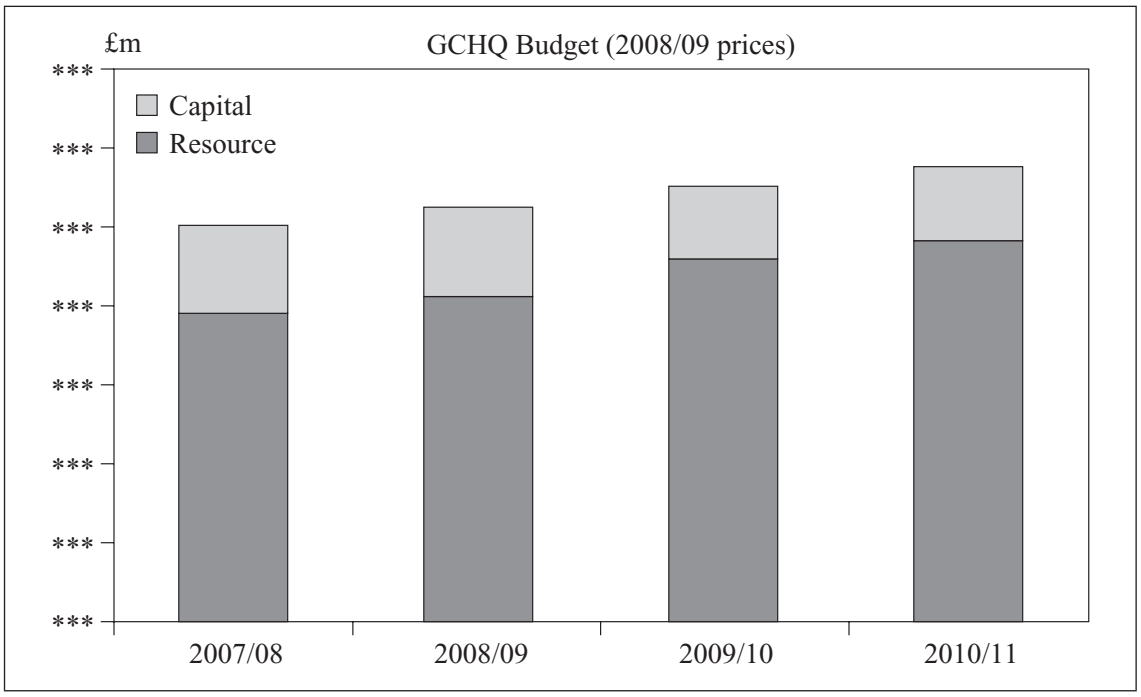
iii. The Chief of SIS, while recognising that the financial climate would be very challenging, also highlighted that in a climate where defence and security budgets are under pressure, intelligence – particularly upstream activity – can effectively act as a 'force multiplier' which:

saves a great deal of investment and resource here in Britain at the downstream end investigating terrorist plots and strengthening our border security. So there are areas where intelligence can compensate for loss of harder edged capability.[10]

Government Communications Headquarters

Expenditure

19. The following chart demonstrates the growth in GCHQ's spending.[11]



GCHQ spent £***m in 2008/09 (against a combined budget of £***m) which was an increase of 5% on the previous year.

20. GCHQ's total planned resource budget for 2009/10 is £***m which, added to a capital budget of £***m, gives them a total budget of £***m (an increase of 5% on 2008/09).

[10] *Oral Evidence – SIS, 19 January 2010.*

[11] *Actual spending for 2007/08 to 2008/09, and planned budgets for 2009/10 and 2010/11.*

21. The focus of GCHQ investment in 2010/11 will be:

- sustaining 2009/10 levels of investment;
- realising the staff growth funded through CSR07 to sustain the existing levels of effort across the full range of intelligence outputs; and
- continuing strategic investment in Afghanistan.

22. Last year we reported on GCHQ's SIGINT Modernisation Programme (SIGMOD).[12] SIGMOD comprises four major projects: 'Support to Military Operations'; 'Mastering the Internet'; 'Better Analysis'; and 'IT Services'.

23. This is a very substantial programme with a total budget of £***m over the CSR period – representing a significant proportion of the entire SIA budget. GCHQ has provided the Committee with a brief summary of the programme. However, given the size of SIGMOD, the Committee has asked for further information including a more detailed breakdown of the milestones and progress of each of the individual projects. The Director told the Committee that he will:

> *provide that further detail around spend, around the type of benefit derived, around perhaps some of the key milestones that we are seeking to hit… I will provide what reassurance I can in that I believe it is a well governed, rigorous programme.*[13]

C. It is essential that this Committee, which has a statutory duty to oversee expenditure by GCHQ, is given a fuller explanation of the SIGMOD programme which accounts for a very significant proportion of GCHQ's entire budget.

Policy

International Counter-Terrorism

24. GCHQ's work on counter-terrorism remained steady in 2008/09 at around a third of overall effort. GCHQ is continuing to focus on the PURSUE strand of CONTEST (the UK Counter-Terrorism Strategy), with support for Security Service priority investigations remaining the core task. While the greatest focus of this work remains on *** and ***, this year has also seen significant work on *** and the ***. On PREVENT the focus has been on countering terrorists' use of the internet.[14] GCHQ's work against extremists on the internet includes ***. Despite the challenges of countering the threat from extremist use of the internet, the Director of GCHQ told us that this also ***:

> ***
> ***
> ***.[15]

---

[12] *Cm 7807.*

[13] *Oral evidence – GCHQ, 9 February 2010.*

[14] *Electronic attack and cyber security is covered in paragraphs 48 to 51.*

[15] *Oral Evidence – GCHQ, 9 February 2010.*

Non-ICT work

25. GCHQ continues to provide support to military forces overseas. There has been a reduction of effort in Iraq following the draw down of military operations, although in 2008/09 this still accounted for ***% of overall effort.[16] There has been a continuing demand for GCHQ support in Afghanistan with a growing number of civilian and military GCHQ staff in theatre.

26. GCHQ's allocation of effort on both 'Weapons and Proliferation' and the Middle East and North Africa remained steady, despite extra resources being dedicated to *** and the ***. GCHQ allocated ***% of effort to 'Serious Crime', 'Counter Espionage' and 'Electronic Attack'.

Information Assurance and Communications-Electronics Security Group (CESG)

27. CESG is the national technical authority for Information Assurance (IA) services.[17] Last year we reported that GCHQ, via CESG, was providing IA services to a growing customer base, and that this would require greater resources.[18] This year GCHQ told us that the increasing demand for CESG's services meant that the current repayment model was not viable and there was a shortfall in funded work of several million pounds. The Director said:

> *I want to move from a model where repayment from other Government departments is the norm to one where more work, especially that needed to keep us ahead of technology, is funded centrally… I believe there is a strong argument that as Government becomes more and more dependent on IT… we need to consider what proportion of Government IT spend should be going towards making the systems secure and resilient. I have been recommending to the Cabinet Secretary that we should stop charging Government departments for CESG services with effect from April this year [2010], if not from April this year, April next year [2011].*[19]

D. The Committee considers that the Information Assurance work carried out by the Communications-Electronics Security Group is important for Government as a whole and that – whatever the suggested funding arrangements might be – they are resolved as a matter of priority.

Administration

28. During 2008/09, 600 new staff joined GCHQ resulting in a small net increase in staff numbers of 3% (from 5,051 to 5,296 staff[20]). Its new recruitment target for 2008/09 was its largest to date (at over 700): GCHQ told the Committee that "*recruitment of the much sought after Internet Analysts, those with rare language skills and Information Assurance specialists continue to be our main challenge*".[21]

---

[16] *After the withdrawal of UK forces it was reduced further to about ***%.*

[17] *'Information Assurance' relates to the integrity, confidentiality and reliability of Government ICT systems and data.*

[18] *Cm 7807.*

[19] *Oral evidence – GCHQ, 9 February 2010.*

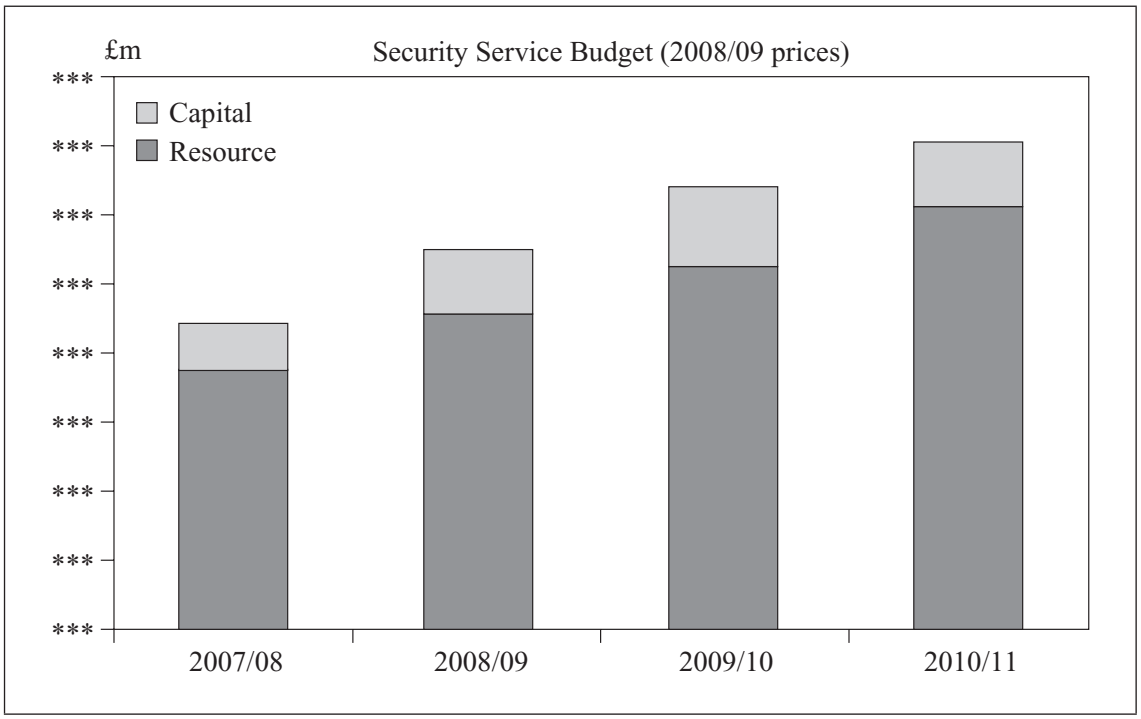
[20] *These figures do not include military personnel and inward secondees.*

[21] *Oral evidence – GCHQ, 9 February 2010.*

The Security Service

Expenditure

29. The following chart demonstrates the growth in the Security Service's spending.[22]



The Security Service spent £***m in 2008/09 (against a combined budget of £***m) which was an increase of 25% on the previous year.

30. The Service's planned resource budget for 2009/10 is £***m which, added to a capital budget of £***m, gives them a total budget of £***m (an increase of 15% on 2008/09).

31. As we mentioned in our last Annual Report,[23] the focus for Security Service investment over the rest of this CSR period is the Intelligence Programme (IQ) and the Service's IT infrastructure. However, an emerging area which will require major investment is digital intelligence (DIGINT). We were told this year that the Service had embarked on scoping work aimed at ensuring that "*in five years' time we are still able to do what we can do today when the use of IT has continued to change as rapidly as it is at the moment*".[24] The cost of the new DIGINT programme was not yet clear, but the Director General estimated that it was likely to be "*tens of millions over the next 12 months*".

---

[22] *Actual spending for 2007/08 to 2008/09, and planned budgets for 2009/10 and 2010/11.*

[23] *Cm 7807.*

[24] *Oral Evidence – Security Service, 26 January 2010.*

Policy

International Counter-Terrorism

32. The Security Service devoted 74% of its effort to international counter-terrorism (ICT) (a 6% increase on the previous year). The Service plans to increase its effort slightly on ICT to 75% during 2009/10. However, it is unlikely that there will be a further increase beyond this level since there is no scope for the Service to cut its non-ICT work further (as has been recognised previously by the Committee).

33. The Director General informed the Committee that at present, with regard to ICT, the Service has "*a couple of hundred cases of one sort or another*".[25] The Service now has an improved and better resourced process to prioritise cases and to ensure that key intelligence from lower priority investigations is not missed: the Director General told us that, as a result of this and the benefits of regionalisation, the Service was "*in a much better position than we were on 7th July [2005 but]… there is still risk in the system because you have to make judgements as to where you put the resources*".

Non-ICT work

34. During 2008/09, the Security Service allocated 13% to Irish-related terrorism. The Director General told us that "*what was not anticipated when we went into this spending period was the way in which the situation in Northern Ireland has degenerated*".[26] In January 2010 the Service had "*considerably more what we would call priority 1, i.e. life-threatening investigations, in Northern Ireland than we do in the rest of Great Britain*". As a result of the increased threat from dissident republican terrorists in Northern Ireland, the Service is planning to increase its effort in this area during 2009/10 to 18%.

35. During 2008/09 the Service allocated 3% of its overall effort to hostile foreign activity in the UK. The main threats continue to be posed by Russia and China, both in the conventional and cyber spheres. The Director General told the Committee that "*there's no doubt that the internet*[27] *is a strong vector of threat as far as espionage is concerned*".[28] For 2009/10, the Service planned to increase its effort in this area to 4%.

Administration

36. During 2008/09, 610 new staff joined the Service. Overall, there has been a 40% increase in Security Service staff between April 2006 and April 2009. However, this expansion is set to slow in pace. The Service aimed to recruit a further 253 staff by April 2010 (an increase of 7%).

---

[25] *Oral Evidence – Security Service, 26 January 2010.*

[26] *Oral Evidence – Security Service, 26 January 2010.*

[27] *Further detail on the threat from electronic attack and cyber security is covered in paragraphs 48 to 51.*

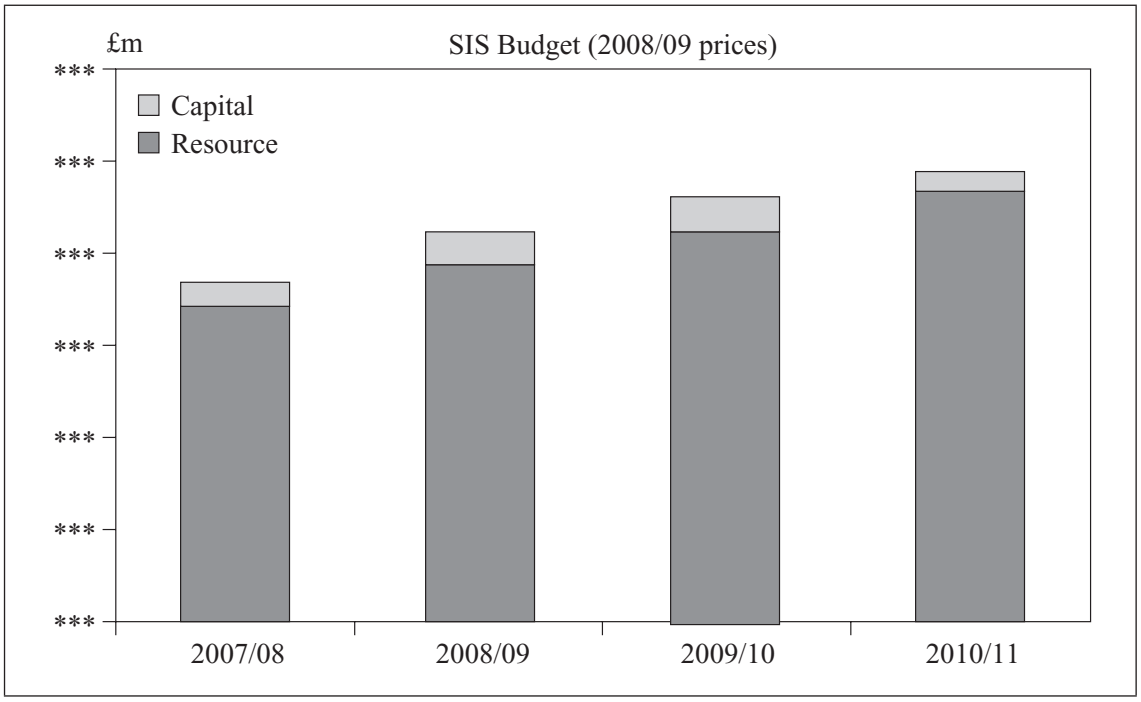
[28] *Oral Evidence – Security Service, 26 January 2010.*

37. The Service has also been reviewing its staff profile. One particular area of concern was the level of IT skills. The Director General told us that "*I think some of the staff perhaps aren't quite the ones that we will want for the future*"[29] and that, as a result, a programme of both voluntary and compulsory redundancies were being introduced.

The Secret Intelligence Service

Expenditure

38. The following chart demonstrates growth in the SIS's spending.[30]



SIS spent £***m in 2008/09 (against a combined budget of £***m) and its capital budget was £***m (an increase of 57% on the previous year).

39. The Service's total planned resource budget for 2009/10 is £***m which, added to a capital budget of £***m, gives them a total budget of £***m (an increase of 8% on 2008/09). SIS's main area of investment is a programme to join up its various IT systems.

[29] *Oral Evidence – Security Service, 26 January 2010.*

[30] *Actual spending for 2007/08 to 2008/09, and planned budgets for 2009/10 and 2010/11.*

40. The Committee has previously criticised SIS for 'end-of-year surges' in its spending. However, an end-of-year surge was also seen in 2008/09 and we were told that a similar surge is expected towards the end of 2009/10. We have questioned SIS in detail on its financial management. We have been told that since the Treasury removed end-year spending flexibility, departments are now forced to spend their capital budgets within the financial year or risk losing them. Since this risks uncontrolled spending and a 'spend it or lose it' mentality, SIS has put in place rigorous control and prioritisation processes for capital spending. However, these processes inevitably delayed spending, and it was this that was leading to surges in spending at the end of the financial year.

Policy

International Counter-Terrorism

41. During 2008/09, SIS allocated approximately 37% of its effort to international counter-terrorism. The Committee were told that the Service is now better placed than a year ago and that it had increased its 'upstream' effort. However, we were reminded that the operational challenges remain formidable. 'C' told us that the Khost bombing on 30 December 2009 highlighted the fact that "*this is a very difficult area of activity for all intelligence services*".[31] The Christmas Day Detroit bomb plot and the resulting increased focus on al-Qaeda in the Arabian Peninsula highlighted another challenge for the Service – being able to respond quickly and effectively to the evolving international terrorist threat. While SIS's key contribution in the work against international terrorism is the collection of intelligence, 'C' told us that the Service aimed:

> *not just to illuminate what's going on, but to try to prevent the undesirable activity as well… at the end of the day, it's stopping the terrorist from committing the atrocity which is our goal.*[32]

Non-ICT work

42. During 2008/09, SIS allocated approximately ***% between Russia and ***. In relation to the latter, the Chief highlighted the fact that SIS had increased its "*effort by about *** per cent over the last two or three years*".[33] Looking forward, in 2009/10 SIS intended to devote just under ***% of its effort to Russia and ***.

43. SIS devoted ***% of its effort to counter-proliferation and ***% to Iran. Both allocations are set to increase in 2009/10 to ***% on counter-proliferation and ***% on Iran. 'C' explained that the increase in effort with regard to Iran was primarily "*because of the nuclear threat*".[34]

---

[31] *Oral Evidence – SIS, 19 January 2010.*
[32] *Oral Evidence – SIS, 19 January 2010.*
[33] *Oral Evidence – SIS, 19 January 2010.*
[34] *Oral Evidence – SIS, 19 January 2010.*

Administration

44. During 2008/09, SIS grew from 2,084 staff to 2,252 (an increase of 8%). SIS aims to increase further to 2,527 during 2009/10 (an additional 12%). Last year we noted that SIS's plans to increase overseas deployments significantly had been affected by security concerns. This year we were told that challenges remain with regard to the staffing of SIS stations in both *** and *** mainly because of the numbers of staff required and the high turnover, however, SIS has informed us that:

> *all posts in *** and *** are currently filled. We have been able to achieve this because of improvements in our planning and the support that we provide to staff filling these posts.*[35]

[35] *Letter from SIS, 4 February 2010.*

CROSS-CUTTING ISSUES

Business continuity

45. In last year's Annual Report we recommended that "*regularly tested business continuity plans are essential for all organisations*".[36] This year we questioned each Agency on its arrangements:

- GCHQ undertook four business continuity exercises during 2008/09. The Director told the Committee that as a result of these tests "*our crisis management arrangements have further improved*" so much so that "*business continuity feels more like business as usual*".[37]
- The Director General of the Security Service informed us that the situation is "*not as bad as it was, but it's not where we want to be*".[38]
- SIS told the Committee that testing its business continuity arrangements had proved useful since it had highlighted some areas of risk. However, the Service is satisfied that it is "*aware of where we have weaknesses, and we are trying to address them as quickly as we can*".[39]

We have impressed on each of the Agencies that it is vital that they regularly test their business continuity arrangements.

46. Another key aspect of business continuity is that of IT backup. The Security Service and SIS are planning to establish a joint data centre to provide secure storage for both Services' data records outside London. SIS and the Security Service are splitting the cost of the project which is estimated to be approximately £***m over eight years. The data centre is expected to be operational by 2011.

47. GCHQ is not – at least in the short term – taking part in the joint data centre project despite the fact that, as we have previously highlighted, it is vulnerable with so much of its key operational equipment in one area.[40] This is primarily because it does not have the funding at present. We were also told that GCHQ was not planning to participate in the joint data centre currently being developed by the Security Service and SIS because it:

> *doesn't offer sufficient space for our requirements or indeed a resilient solution. It's just effectively another data centre. But there is an option, and we have an option to consider participation with that project at a later phase as and when we may have funding.*[41]

E. With GCHQ's key operational equipment concentrated in the Cheltenham area, it is essential that it establishes a backup site at a different location.

---

[36] *Cm 7807.*
[37] *Oral Evidence – GCHQ, 9 February 2010.*
[38] *Oral Evidence – Security Service, 26 January 2010.*
[39] *Oral Evidence – SIS, 19 January 2010.*
[40] *Cm 7807.*
[41] *Oral Evidence – GCHQ, 9 February 2010.*

Electronic attack and cyber security

The threat

48. Last year we raised concerns about the potential threat posed to the UK from electronic attack. We recommended that the UK accord the area a similar priority and resources as do the US and Canada.[42] The Chief of SIS told the Committee this year that "*the whole question of cyber security is shooting up everybody's agendas*" and that it is "*a major new challenge to the intelligence community*".[43] The Director General of the Security Service observed that "*I don't think we are where we need to be*" and that "*it's a difficult threat to grasp*".[44]

49. GCHQ informed the Committee that it is not known whether terrorist groups intend, or have the capability, to launch significant attacks over the internet but this, along with extremist use of the internet, remains an area of considerable concern. Nevertheless, we have been told by GCHQ that the greatest threat of electronic attack to the UK comes from State Actors, with Russia and China continuing to pose the greatest threat. The Director General of the Security Service told us that:

> *At the moment my understanding is that there will be considerable impact if a state, be it Russia or China, and probably those are the most likely, decided to do serious damage to us one way or another.*[45]

Machinery

50. The Cyber Security Strategy[46] published in June 2009 established two new organisations, the Office of Cyber Security (OCS) and the Cyber Security Operations Centre (CSOC):

i. The OCS is based in the Cabinet Office. Its role is to provide strategic leadership and coherence on cyber security issues across Government and to "*drive delivery of the strategy through a cross-government programme*".[47] As of 1 November 2009 it had 11 staff, drawn from across a range of departments and agencies with a further seven staff expected to join by March 2010 (full capacity is expected by April 2010).

---

[42] *Cm 7807.*

[43] *Oral Evidence – SIS, 19 January 2010.*

[44] *Oral Evidence – Security Service, 26 January 2010.*

[45] *Oral Evidence – Security Service, 26 January 2010.*

[46] *Cm 7642.*

[47] *Cm 7642.*

ii. The CSOC was established in September 2009 and is hosted by GCHQ. The role of the CSOC is to:

monitor the health of cyber space and co-ordinate incident response, enable better understanding of attacks against UK networks and users, and, provide better advice and information about risk to both business and the public.[48]

As of 1 November 2009, the CSOC had 11 staff, drawn from across a range of departments and agencies, with 19 staff planned by the end of March 2010.

51. In addition to this work being done by the OCS and the CSOC there are a number of other bodies working in this field including: the Network Defence Intelligence and Security Team (NDIST) and the Internet Operations Centre (INOC), which are part of GCHQ, the Centre for the Protection of National Infrastructure (CPNI), and the Technical Counter-Intelligence Team at SIS. The Cyber Strategy states that "*there is no intention to replace or duplicate existing work*".[49] However, with such a number of units operating in this area this must be a concern. We note the comments made by Baroness Eliza Manningham-Buller that:

This area is covered by acronyms; there are lots of different units and organisations. But… the focus should be on what improvements result from these new structures, not the structures and their names themselves.[50]

F. The Committee welcomes the new developments in the field of cyber security which indicate that the threat of electronic attack is now being taken seriously across both Government and the intelligence and security Agencies. However, we are concerned that there is a risk of duplication of effort in this important area.

The exchange of intelligence

52. In our 2007 Report on Rendition[51] we explained the importance of intelligence exchanges with foreign liaison partners, including intelligence relating to detainees. We concluded that:

Our intelligence sharing relationships, particularly with the United States, are critical to providing the breadth and depth of intelligence coverage required to counter the threat to the UK posed by global terrorism. These relationships have saved lives and must continue.

---

[48] *Cm 7642.*

[49] *Cm 7642.*

[50] *Baroness Eliza Manningham-Buller, Hansard, House of Lords, 4 February 2010.*

[51] *Cm 7171.*

53. Since that report was published, the principle of confidentiality of intelligence exchanges has been challenged in the High Court as part of a case relating to Binyam Mohamed.[52] Among the material submitted to the Court we have noted, in particular, three letters from the US authorities asserting that the US/UK intelligence relationship would be damaged if the UK courts were to publish US intelligence material. One of these, sent from the Central Intelligence Agency (CIA) to SIS on 30 April 2009,[53] asserts that:

> *The cooperation and sharing of intelligence between the United Kingdom and the United States, as well as with other foreign governments, exists under strict conditions of secrecy. Public disclosure by the United Kingdom of information garnered from such relationships would suggest that the United Kingdom is unwilling or unable to protect information or assistance provided by its allies. As a consequence, if foreign partners learn that information it has provided is publicly disclosed, these foreign partners could take steps to withhold from the United Kingdom sensitive information that could be important to its safety and security.*

It concludes that:

> *If it is determined that your Service is unable to protect information we provide to you even if that inability is caused by your judicial system, we will necessarily have to review with the greatest care the sensitivity of information we can provide in future.*

54. The High Court ruled in its fifth and sixth judgments that certain intelligence material (or summaries thereof) originating from the US should be placed into the public domain. The Committee supported the Government's decision to appeal against this judgment. Publication of other countries' intelligence material, whether sensitive or otherwise, undermines the key principle of confidentiality on which relations with foreign intelligence services are based and has the potential to cause serious harm to future intelligence co-operation.

55. We have spoken to each of the Agencies in depth this year about the potential harm to our intelligence relationships. The Chief of SIS highlighted his concern about the real possibility that the flow of intelligence from key partners will reduce because of concern about whether SIS could "*keep the secrets that they share with us, or whether we will be forced by our legal systems to release intelligence*".[54]***.

56. On 10 February 2010 the judgment was handed down by the Court of Appeal. The Court dismissed the Foreign Secretary's appeal on the grounds that the substance of the material in question had already been placed in the public domain as a result of a case in the US. However, a number of important points emerged from the judgment, including:

- had the material not been revealed by a US court (a fact which significantly changed the context) the Court would have upheld the appeal; and

---

[52] *We reported in detail on the case of Binyam Mohamed in our 2008–2009 Annual Report, Cm 7807.*

[53] *This was attached to a letter from the Treasury Solicitors to Lord Justice Thomas and Mr Justice Lloyd Jones on 20 July 2009.*

[54] *Oral Evidence – SIS, 19 January 2010.*

- the 'control principle' (i.e. maintaining the confidentially of information supplied by a liaison agency) was recognised as an extremely important principle in intelligence relationships and should not be undermined.

57. Nevertheless, the Office of the Director of National Intelligence issued a statement in response to the Court of Appeal judgment, saying that the decision "*creates additional challenges*" for US/UK intelligence co-operation and that:

> *The protection of confidential information is essential to strong, effective security and intelligence co-operation among allies. The decision by a United Kingdom court to release classified information provided by the United States is not helpful, and we deeply regret it.*[55]

G. The Committee is concerned that the publication of other countries' intelligence material, whether sensitive or otherwise, threatens to undermine the key 'control principle' of confidentiality which underpins relations with foreign intelligence services, and that this may seriously damage future intelligence co-operation. We therefore welcome the Court of Appeal's recognition of the importance of the 'control principle'.

Intercept as evidence

58. Since our last Annual Report, work (led by the Home Office) to examine whether a system could be devised to enable the use of intercepted material in court, which simultaneously satisfied the requirements for a fair trial and safeguard national security, has continued. On 10 December 2009 the Home Secretary published a further update report.[56] The report concluded that the model which had been developed and tested would not be legally viable and that:

> *The collective view of the departments, intercepting agencies and prosecution authorities engaged in the work programme is that despite best efforts to design, build and test the model, it does not provide a viable basis for implementation, without breaching the operational requirements*[57] *set out by the Privy Council.*[58]

59. The report went on to note that the implementation of the original legal model would in fact "*weaken and not enhance our ability to protect the public and to identify and bring the guilty to justice*".[59]

60. However, further work would be done on three areas that were outside the scope of the original programme which might address some of the current failings. These areas are: further enhancing judicial oversight, exploring options for the full retention of interception material, and considering whether advances in technology could make full retention and review more manageable. The results of this additional work are expected to be reported to Parliament before the Easter recess in 2010.

---

[55] *Statement by the Office of the Director of National Intelligence, 10 February 2010.*

[56] *Cm 7760.*

[57] *We reported on these operational requirements in our 2007–2008 Annual Report, Cm 7542.*

[58] *Cm 7760.*

[59] *Cm 7760.*

H. There has now been a comprehensive examination of the issues involved in allowing intercept material to be adduced as evidence in the UK. That it has failed to provide a viable model is unsurprising, given the complexities of the issues involved. We await the outcome of the further work now being done. We recommend that if this too fails to provide a workable solution then the issue should be considered closed.

SCOPE

61. The SCOPE programme was designed as a major inter-departmental IT change programme in order to enable information sharing across the wider intelligence community. It was intended to be delivered in two phases:

- Phase 1: connecting key departments (such as the Home Office and the Serious Organised Crime Agency) to the existing secure communications network used by the intelligence community.
- Phase 2: improving and expanding the secure communications network and extending the system's capabilities.

62. After a two-year delay, Phase 1 was fully implemented in late 2007, and the Committee was assured (in January 2008) that concerted efforts were being made to ensure successful and timely delivery of Phase 2. However, just three months later, as we reported in our 2007–2008 Annual Report[60] the decision had been taken to abandon SCOPE Phase 2. We reported then that we were appalled at what appeared to be a waste of tens of millions of pounds, and said that we would be investigating why this vital project failed, the associated cost implications and the options for a replacement system.

63. SCOPE Phase 2 has been beset by problems and delays. In our 2008–2009 Annual Report we noted that we were continuing with our investigation into the exact circumstances surrounding the Cabinet Office's decision to abandon Phase 2 of SCOPE, and that we would detail our findings in this Annual Report. Although we have taken further evidence on this matter, and were in a position to report our findings, both parties remain engaged in a contractual dispute process[61] and we have been advised to postpone publishing further details until this process is completed. Our findings will be provided to our successor Committee for them to publish at an appropriate time.

---

[60] *Cm 7542.*

[61] *The Cabinet Office informed the Committee in October 2009 that mediation had taken place in September 2009 which had failed to produce a resolution, and that the dispute was about to move to arbitration.*

ANNEX A – COMMITTEE INDEPENDENCE

Principles

1. The Intelligence and Security Committee is a separate legal entity, created by statute to examine the expenditure, administration and policy of the Security Service, the Secret Intelligence Service and the Government Communications Headquarters.

2. The Intelligence and Security Committee is independent of Government. It must be, and must be seen to be, completely independent of those it oversees.

3. The Intelligence and Security Committee has a statutory responsibility to report to the Prime Minister on its work. The ISC can report directly to the Prime Minister on any matter it so chooses, without prior referral or clearance with any other body or individual.

4. In terms of administration, to ensure the above separation and independence:

   4.1 The Intelligence and Security Committee is served by a Secretariat of suitably qualified and security-cleared individuals who report to the Committee.

   4.2 The Intelligence and Security Committee's data and records remain the property of the Committee, and under its responsibility and control.

   4.3 The Intelligence and Security Committee determines its own procedures.

Intelligence and Security Committee
November 2009

Policies

The following policies flow from the principles governing the work of the Intelligence and Security Committee.

Remit

1.1 Following on from principle 1 above, the remit of the Intelligence and Security Committee ('the Committee') has evolved since the original legislation. The Committee has developed its oversight remit, with the Government's agreement, to include examination of other intelligence and security related areas within Government.

1.2 These include:

1.2.a the Joint Intelligence Committee in the Cabinet Office;

1.2.b the work of the Intelligence Security and Resilience Group, in the Cabinet Office;

1.2.c the Defence Intelligence Staff in the Ministry of Defence; and

1.2.d any other work in a department or agency that is relevant to a Committee Report (such as the Office for Security and Counter-Terrorism in the Home Office).

Separation

2.1 Given principle 2 above, the Committee must ensure that no undue influence is brought to bear on its work. As a matter of principle it must be clearly independent and separate from all bodies within Government which have an intelligence or security role.

2.2 The Committee can not therefore be hosted – in terms of its administration, pay and rations – by any organisation with an intelligence or security function. Given the considerable changes in the central security and intelligence functions within Government over the past 16 years, the current arrangements are now out of date and require changing as a matter of priority.

2.3 The Committee's funding must be similarly separated and ring-fenced as a fixed percentage of the Single Intelligence Account (or its equivalent, should the SIA structure be changed). This will allow the Committee's activity and capability to grow or shrink in accordance with those it oversees.

Reports

3.1 Following on from principle 3 above, the Prime Minister appoints the Committee Members after considering nominations from Parliament and consulting with the leaders of the two main opposition parties. The Committee consists of nine Members drawn from both Houses. (Traditionally there has only been one representative of the House of Lords, but this is not laid down in statute.) The Committee reports directly to the Prime Minister and through him to Parliament, by the publication of the Committee's reports.

3.2 The Members are subject to section 1(1)(b) of the Official Secrets Act 1989 and have access to highly classified material in carrying out their duties. The Committee's access to information is set out in the Intelligence Services Act 1994. The Committee takes evidence from Cabinet ministers and senior officials – all of which is used to formulate its reports. It also considers written evidence from the intelligence and security Agencies and relevant Government departments. This evidence may be drawn from operational records, source reporting and other sensitive intelligence (including original records when relevant), or it may be memoranda specifically written.

3.3 The Committee is required by the Intelligence Services Act to produce an Annual Report on the discharge of its functions, which the Prime Minister is required to lay before Parliament. The Committee can produce other reports on specific topics. It has no obligation to report to, and is not answerable to, any other minister or Government official.

3.4 Under the terms of the Intelligence Services Act, material can be redacted if it is determined "*after consultation with the Committee, that the publication of any matter in a report would be prejudicial to the continued discharge of the functions of either of the Services or, as the case may be, GCHQ*". In practice this is a process of considerable negotiation between Government and the Committee, with the aim of agreeing a text that can be published without damage to national security. To date, no material has been redacted without the Committee's consent.

3.5 The Committee sends its reports directly to the Prime Minister, and meets him to discuss the report prior to it being published. When the report is published it is debated in both Houses, with the debate in the Commons opened by the Chairman of the Committee, and the debate in the Lords opened by the Lords Member.

Staff

4.1 Following on from principle 4.1 above, the Secretariat is responsible to the Committee and must not be put under undue pressure or have its work interfered with by others. All members of the Secretariat have a duty of confidentiality to the Committee, and this continues beyond the period of their service.

4.2 All members of the Secretariat will conduct themselves in accordance with the Civil Service Code.

4.3 The Committee's Clerk will be selected by and appointed to the Committee itself, with the Chairman of the Committee acting as the Clerk's line manager. For the purposes of Civil Service procedures, a senior 'mentor' may be appointed. This must be a Director or Director-General level official outwith those departments which the Committee oversees (i.e. with no intelligence role) and will be agreed formally with the Chairman and one opposition Member.

Records and data

5.1 All records and data – while rightly remaining the property of the originator – are controlled by the Committee, and maintained in accordance with the relevant security accreditation procedures.

5.2 Individuals outside of the Committee or its Secretariat must not attempt to control, administer or access the Committee's records or data.

Procedures

6.1 The Committee sets its own procedures, as set out in Schedule 3 of the Intelligence Services Act 1994. These are not subject to review, challenge or interference by others, other than in accordance with the law.

6.2 The current procedures that the Committee follow in relation to its meetings, visits, reports and correspondence will be set out for the information of those with whom the Committee deals.

Intelligence and Security Committee
November 2009

GLOSSARY

CESG	Communications-Electronics Security Group
CIA	Central Intelligence Agency (US)
CONTEST	UK Counter-Terrorism Strategy
CPNI	Centre for the Protection of National Infrastructure
CSOC	Cyber Security Operations Centre
CSR07	Comprehensive Spending Review 2007
DIGINT	Digital Intelligence
DIS	Defence Intelligence Staff
GCHQ	Government Communications Headquarters
IA	Information Assurance
ICT	International Counter-Terrorism
INOC	Internet Operations Centre
ISC	Intelligence and Security Committee
IT	Information Technology
JIC	Joint Intelligence Committee
JTAC	Joint Terrorism Analysis Centre
NDIST	Network Defence Intelligence and Security Team
OCS	Office of Cyber Security
SIA	Single Intelligence Account
SIGMOD	GCHQ's SIGINT Modernisation Programme
SIS	Secret Intelligence Service

LIST OF WITNESSES

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Mr Iain Lobban – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Sawers – Chief, SIS

Other officials

SECURITY SERVICE

Mr Jonathan Evans – Director General, Security Service

Other officials

CABINET OFFICE

Sir Gus O'Donnell KCB – Cabinet Secretary

Mr Robert Hannigan – Security Adviser to the Prime Minister and Head, Intelligence, Security and Resilience

Other officials

TSO
information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone Fax & E-Mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

TSO@Blackwell and other Accredited Agents

Customers can also order publications from
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-178442-9
9 780101 784429