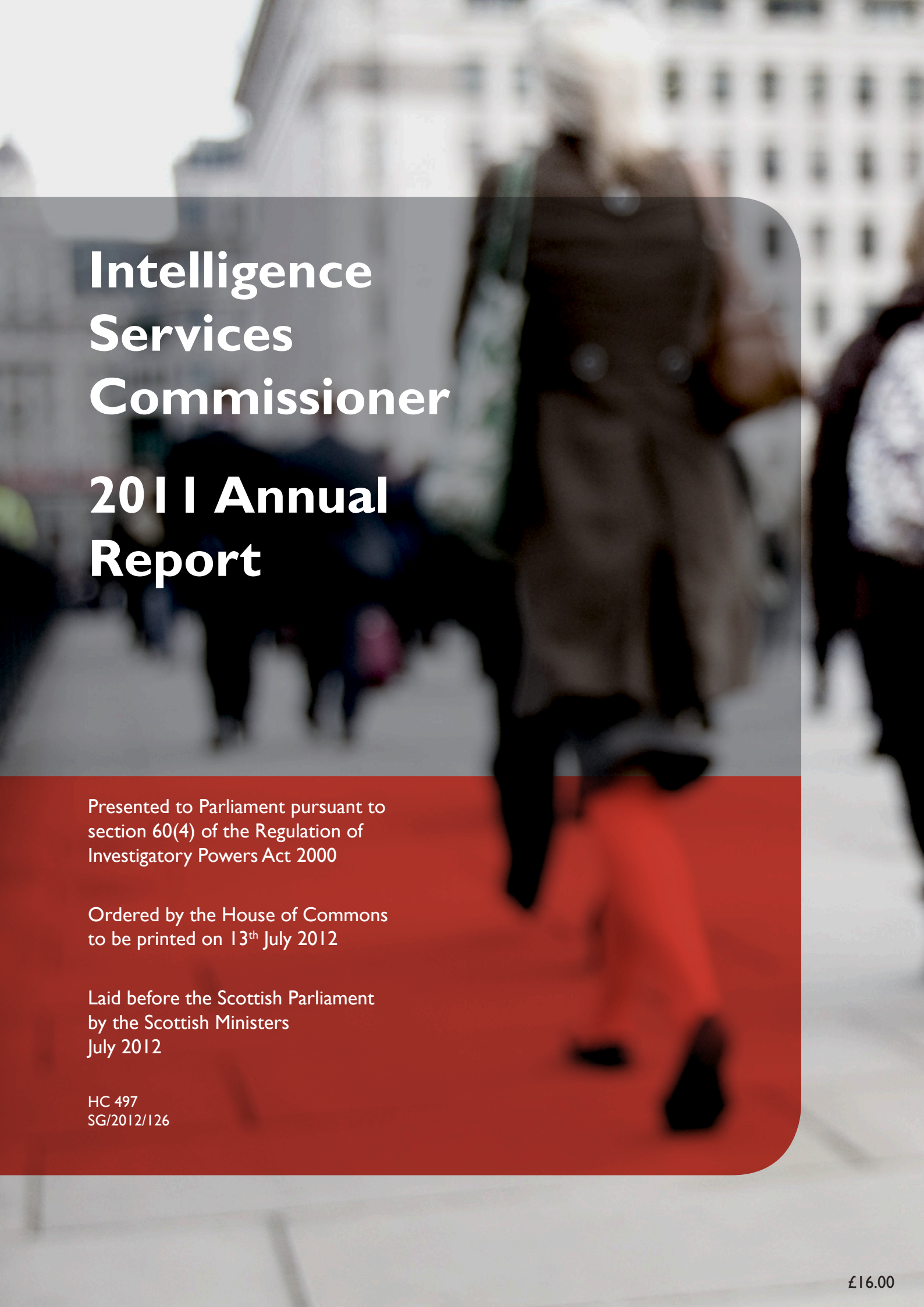


Intelligence Services Commissioner

2011 Annual Report

Presented to Parliament pursuant to section 60(4) of the Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons to be printed on 13th July 2012

Laid before the Scottish Parliament by the Scottish Ministers July 2012

HC 497
SG/2012/126

£16.00

Intelligence Services Commissioner

2011 Annual Report

Presented to Parliament pursuant to section 60(4) of the Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons to be printed on 13th July 2012

Laid before the Scottish Parliament by the Scottish Ministers July 2012

HC 497
SG/2012/126

London: The Stationery Office £16.00

Any enquiries regarding this publication should be sent to us at c/o Intelligence Services Commissioner, 2 Marsham Street, London SW1P 4DF

This publication is available for download at www.official-documents.gov.uk.
This document is also available from our website at www.intelligencecommissioners.com

ISBN: 978-0-10-298033-2

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

ID P0256897 07/12

Printed on paper containing 75% recycled fibre content minimum

INTRODUCTION

Sir Mark Waller: Biography

The Rt. Hon. Sir Mark Waller was appointed Intelligence Services Commissioner on 1st January 2011 by the Prime Minister under s.59 of the Regulation of Investigatory Powers Act (RIPA, 2000). This followed his retirement from the Court of Appeal in summer 2010.

Sir Mark was called to the Bar by Gray's Inn in 1964. He practiced as a Commercial Barrister from 1 Hare Court. He became a QC in 1979. He was appointed a Bencher of Gray's Inn in 1989 and Treasurer in 2009. He was appointed a Judge of the Queen's Bench Division in 1989, serving as Presiding Judge of the North Eastern Circuit between 1992 and 1995. Subsequently he was appointed Judge in charge of the Commercial List between 1995 and 1996. Sir Mark was a Lord Justice of Appeal between 1996-2010, Chairman of the Judicial Studies Board 1999-2003, President of the Council of the Inns of Court 2003-6 and Vice-President of the Court of Appeal Civil Division 2006-2010.

Sir Mark is currently an Arbitrator and Mediator at Serle Court, London.

CONTENTS

CONTENTS

1. INTELLIGENCE SERVICES COMMISSIONER

Commissioner's Foreword

Having been appointed by the Prime Minister to the post of Intelligence Services Commissioner, I am required by section 60(2) of RIPA to report 'as soon as practicable after the end of each calendar year' with respect to the carrying out of my functions. This is therefore my first annual report and covers the period 1st January to 31st December 2011.

During my first year there has been considerable public discussion about the way in which oversight is carried out and /or might be carried out in the future. This public discussion has in many ways been led by the Justice and Security Green Paper and subsequent Bill, which is going through various parliamentary stages as this report is being published. Furthermore, civil society organizations such as Justice published their own views on the future of surveillance reform. These have put under the spotlight the extent of the commissioners' role and the extent to which the public can have confidence in independent oversight.

It has accordingly seemed to me important from the commencement of my role to examine with some care whether these criticisms are justified and if so what could be done to meet them and to see to what extent my report can answer criticisms and be more informative.

Let me start by saying that there are some misconceptions. The role of the commissioner has not always been properly understood. As outlined by my predecessor Sir Peter Gibson in his 2010 Annual Report, some people think that the role is one which has blanket oversight of all the activities of the intelligence agencies. This is simply not the case and, as outlined in the legislative section that follows, the role is quite tightly outlined in RIPA and the Intelligence Services Act (ISA, 1994).

The role is essentially to keep under review the exercise by the Secretaries of State of their powers to issue warrants and authorisations to enable the intelligence agencies to carry out their functions. It is also to keep under review the exercise and performance of the powers and duties imposed on the intelligence agencies and MoD/Armed Forces personnel in relation to those matters which are the subject of an internal authorisation procedure.

The method of review as established by my predecessors has been as a first step to sample randomly i.e. to select a certain number of examples from each area of activity. The next stage has been to obtain all the papers relating to those chosen samples and to ask questions of the persons involved as to the approach adopted by them. Previous commissioners carried out two inspections on the above basis per year with each of the Intelligence agencies and the MoD. In addition however, commissioners have paid visits to in-country stations and areas of MoD activity in various parts of the world to review the work and authorisation process from their own point of view.

The Justice report described the process of review as two 'dip-sample' inspections per year. There is perhaps an unspoken suggestion that the inspection is simply a rather superficial paper-checking exercise at a small number of intelligence agencies, whom one could assume were extremely competent in keeping their paperwork in order. If that is the suggestion then the actuality is very different; the question is how to give confidence that it is very different and how to be able to report so that confidence can best be ensured.

Due to the necessity of keeping many operational details of the warrants and authorisations I oversee secret and out of the annual report, the full extent of the commissioner's review cannot be fully disclosed. Furthermore the absence of details in the open report has caused some members of the public and media to question the extent to which the commissioner has access to the information required to carry out a meaningful review.

I have therefore sought, both in my approach and the drafting of the current report, to address the above points and seek to increase public confidence in the impact of the commissioner role. The current report therefore addresses the 'how' of my oversight in the following ways:

- More information on how I have conducted my scrutiny visits both in the UK and abroad, individuals I have met and broad details of the kinds of cases and issues on which my formal and informal input has been requested throughout the year.
- More detail on the kinds of RIPA and ISA errors and successes reported to me in relation to the warrants and authorisations I oversee. I have also sought to outline where possible in the open report any system changes that have been implemented as a result of my oversight.
- This year I have published in the open report a figure showing the number of RIPA and ISA authorisations which I oversee signed by all Secretaries of State and those authorised internally within the intelligence agencies. I have concluded that is necessary so as to give some indication of the extent of what I oversee. I have inspected what I am advised, and believe, are a sufficient number of authorisations and which, alongside my other investigations, enables me to reach clear conclusions - I have not produced a detailed breakdown of specific numbers related to the different kinds of authorisation overseen in an open report because that could, in my view, be detrimental to national security.
- Details of the system established to oversee the intelligence agencies' and MoD compliance with the Consolidated Guidance on Detainees, which my predecessor agreed to oversee in July 2010.
- Examples of how the commissioners' office has responded to demands for greater transparency around my role, not least through a public-facing website, speeches and wider attempts to establish a greater public profile. Alot of this information can be found by readers on the commissioners' website www.intelligencecommissioners.com launched in 2011.

I hope this approach contributes to greater public confidence in my eventual conclusion that members of the intelligence agencies and Secretaries of State undertake their authorisations of potentially intrusive activities with the utmost diligence and respect for legalities. I am provided with access to the necessary information around the intelligence, resource and legal cases governing executive actions, and it is often the case that I am provided with more information than is strictly necessary for the purposes of adding context. I can then conclude with some confidence that, as far as those activities I oversee, officials and Secretaries of State do comply with the necessary legislation in relation to the authorisations I oversee, in so far as they are bound to do so.

I have sought to bring as much information about my oversight, authorisation errors and successes into the open report as it is appropriate to do, but it is important that I do not reveal information that could aid hostile states or individuals who may wish to cause harm to the UK.

It has therefore been necessary for me to draft a separate confidential annex to this report containing information not for public disclosure. I can assure readers of two things; firstly, that any reasonable member of the public would be convinced that the operational detail contained in this annex is just that, operational detail, comprising target names and techniques utilised by intelligence agencies, which must be protected in the interests of national security. The principles and impact of my oversight of the intelligence agencies has deliberately been outlined in the open report. Secondly, I have sought to widen the distribution of this annex across Whitehall to ensure that senior officials and Ministers subject to my oversight share successes and learning that may arise through the function of oversight.

2. LEGISLATIVE BASIS

I was appointed the role of Intelligence Services Commissioner on 1st January 2011. My appointment is made by the Prime Minister, initially for a period of three years under s.59 of RIPA. I shall therefore serve until 31st December 2013 whereupon my position is subject to review with the possibility of renewal.

Previous Intelligence Services Commissioners have outlined in their respective annual reports the scope of each part of RIPA, the functions of the intelligence agencies and the functions of the commissioner. In addition, the Interception of Communications Commissioner, in his 2010 annual report, sought to aid understanding of RIPA by presenting its key components in relation to interception in a summary diagram. This has been well-received and made available on the www.intelligencecommissioners.com website.

I have continued with this practice and present in the section that follows:

A. A number of case studies which present in more detail hypothetical but easily-comprehensible examples of when intrusive powers may be used, how they are authorised within the relevant intelligence agency and by whom such acts are signed off and overseen.

B. A brief summary of the statutory objectives under which each of the intelligence agencies conducts its day-to-day work.

C. My remit as set out in the terms and conditions from the Prime Minister upon which I accepted the role of commissioner.

D. Details of my assessment of compliance in relation to my non-statutory oversight of the consolidated detainee guidance.

E. Details of an example where, due to operational reasons, the process set out by RIPA is not fully complied with by the MoD.

F. I also present in the Annex to this report a summary grid which outlines the relevant sections of RIPA and ISA concerning the intelligence agencies and other public authorities; intrusive powers, typical uses of these powers along with details of authorisation and oversight mechanisms.

A. Authorisation case studies

I believe it would add context for readers to be presented with potential scenarios where the intelligence agencies may need to apply for the following:

- Part II RIPA Directed Surveillance Authorisations (DSAs)
- Combined Section 5 ISA Property warrants and Part II RIPA Intrusive surveillance authorisations
- Part II RIPA Covert Human Intelligence Source (CHIS) authorisations.

I would encourage readers to refer to the hypothetical scenarios set out in Annex A to this report. I have drawn heavily in these scenarios on the Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice, both published by the Home Office. The examples given are necessarily simplistic and relate only to covert surveillance and CHIS authorisations applied for by the intelligence agencies in the UK. Such activities are routinely undertaken in partnership between the Police and Security Service and can thus be more complex. I would direct readers to the afore-mentioned Codes of Practice for further information.

Surveillance is defined as being directed if the following are all true:

- It is covert, but not intrusive surveillance
- It is conducted for the purposes of a specific investigation or operation
- It is likely to involve the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation)
- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought.

Intrusive surveillance is defined as covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. It is important to note that, unlike the test in relation to directed surveillance, the definition of surveillance as intrusive relates to the location of the surveillance. There is no consideration necessary in relation to whether or not intrusive surveillance is likely to result in the obtaining of private information.

Only the Secretary of State has powers to authorise the following:

- Intrusive Surveillance under RIPA
- Combined property interference and intrusive surveillance under s.34 (2) of RIPA
- Section 5 ISA property interference
- Section 7 ISA authorisations

Both Directed Surveillance and CHIS authorisations are granted internally by a Designated Person or Authorising Officer, in line with RIPA.

Section 7 authorisations

Under section 7 of ISA the Secretary of State (in practice normally the Foreign Secretary) may authorise SIS or GCHQ to undertake acts outside the United Kingdom which are necessary for the proper discharge of one of its functions. Authorisations may be given for acts of a specified description.

As with section 5 warrants, before the Secretary of State gives any such authority, he must first be satisfied of a number of matters:

- that the acts being authorised (or acts in the course of an authorised operation) will be necessary for the proper discharge of an SIS or GCHQ function (section 7(3)(a)) of ISA)
- that satisfactory arrangements are in force to secure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of an SIS or GCHQ function (section 7(3)(b)(i)) of ISA);
- that satisfactory arrangements are in force to secure that the nature and likely consequences of any acts which may be done in reliance on the authorisation will be reasonable having regard to the purposes for which they are carried out (section 7(3)(b)(ii)) of ISA); and
- that satisfactory arrangements are in force to secure that SIS or GCHQ shall not obtain or disclose information except insofar as is necessary for the proper discharge of one of its functions (section 7(3)(c)).

The purpose of section 7 is to ensure that certain SIS or GCHQ activity overseas, which might otherwise expose its officers or agents to liability for prosecution in the UK, is, where authorised by the Secretary of State, exempted from such liability. I would however emphasise that the Secretary of State, before granting each authorisation, must be satisfied of the necessity and reasonableness of the act authorised.

B. The intelligence agencies' statutory objectives

I have followed the practice of previous commissioners and highlight in this section the statutory functions of the three intelligence agencies. I believe it adds useful context for readers to be aware of functions imposed upon each of the intelligence agencies and certain constraints to which all are subject.

Security Service (SyS)

The functions of SyS are:

- the protection of national security, in particular against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means;
- safeguarding the economic well-being of the UK against threats posed by the actions or intentions of persons outside the British Islands; and
- to act in support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime.

Secret Intelligence Service (SIS)

The functions of SIS are to obtain and provide information and to perform other tasks relating to the actions or intentions of persons outside the British Islands either:

- in the interests of national security, with particular reference to the UK Government's defence and foreign policies, or
- in the interests of the economic well-being of the UK, or
- in support of the prevention or detection of serious crime.

Government Communications Headquarters (GCHQ)

GCHQ's functions are:

- to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material, but only in the interests of national security, with particular reference to the United Kingdom Government's defence and foreign policies, or in the interests of the UK's economic well-being in relation to the actions or intentions of persons outside the British Islands, or in support of the prevention or detection of serious crime;
- to provide advice and assistance about languages (including technical terminology) and cryptography (and other such matters) to the armed services, the Government and other organisations as required.

C. My Remit

I present in this section my remit as set out by the Prime Minister and upon which I accepted the role as Intelligence Services Commissioner. I hope that it will explain to readers the statutory boundaries that define my oversight role as commissioner. Where my predecessors have been asked, and agreed, to perform extra-statutory functions such as oversight of the Consolidated Guidance on the Passing and Receipt of Intelligence Related to Detainees I have continued to provide such oversight on an extra-statutory basis.

As already indicated the commissioner does not have blanket oversight of the intelligence agencies and is not authorised to oversee all of their activities, but that said, one of the strengths of the Office of Commissioner in my view is the challenging but constructive relationship that exists with the intelligence agencies. I have on numerous occasions been consulted by those intelligence agencies and departments I oversee on matters of policy or in relation to legalities. I have given my advice freely and without prejudice. However it is also important to make clear that I am not the adviser of the intelligence agencies.

My functions as commissioner are therefore:

- Keeping under review the exercise by the Secretary of State of his powers to issue, renew and cancel warrants under sections 5 and 6 of ISA, i.e. warrants for entry on or interference with property (or with wireless telegraphy), warrants in practice issued mainly by the Home Secretary or the Secretary of State for Northern Ireland.
- Keeping under review the exercise by the Secretary of State of his powers to give, renew and cancel authorisations under section 7 of ISA i.e. authorisations for acts done outside the United Kingdom, authorisations in practice issued by the Foreign Secretary.
- Keeping under review the exercise and performance by the Secretary of State of his powers and duties under Parts II and III of RIPA in relation to the activities of the intelligence agencies and (except in Northern Ireland) of MoD officials and members of the armed forces, in practice the Secretary of State's powers and duties with regard to the grant of authorisations for intrusive surveillance and the investigation of electronic data protected by encryption.
- Keeping under review the exercise and performance by members of the intelligence agencies of their powers and duties under Parts II and III of RIPA, in particular with regard to the grant of authorisations for directed surveillance and for the conduct and use of covert human intelligence sources and the investigation of electronic data protected by encryption.
- Keeping under review the exercise and performance in places other than Northern Ireland by MoD officials and members of the armed forces of their powers and duties under Parts II and III of RIPA, in particular with regard to the granting of authorisations for directed surveillance and the conduct and use of covert human intelligence sources and the investigation of electronic data protected by encryption.
- Keeping under review the adequacy of the Part III safeguards of RIPA arrangements in relation to the members of the intelligence agencies.

- Keeping under review the adequacy of the Part III safeguards arrangements in relation to officials of the MoD and members of the armed forces in places other than Northern Ireland.
- Giving the Investigatory Powers Tribunal all such assistance (including his opinion on any issue falling to be determined by it) as it may require in connection with its investigation consideration or determination of any matter.
- Making an annual report to the Prime Minister on the discharge of his functions, such report to be laid before Parliament.

Non-Statutory remit

- Overseeing the intelligence agencies' compliance with the Consolidated 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, in accordance with the parameters set out by the Prime-Minister to the Intelligence Services Commissioner.
- Any other non-statutory duties that the Prime Minister may from time to time ask the commissioner to take on and providing the commissioner is willing to undertake these.

D. Consolidated Guidance on Detention and Interviewing of Detainees by Intelligence Officers and Military Personnel.

My predecessor agreed to monitor the intelligence agencies' and MoD compliance with the Consolidated Guidance on the Passing and Receipt of Intelligence Relating to Detainees, which was published on 6th July 2010. In his last report as commissioner, Sir Peter Gibson outlined in Paragraph 45 that

> *'...satisfying the Commissioner of due compliance (with the guidance) is a new burden on agencies and the MoD, and I do not doubt that my successor as Commissioner will wish to develop, in co-operation with the agencies and the MoD, better ways whereby the Commissioner will be provided with and can check on the information he needs to be able to report on such compliance'*

I have therefore, throughout 2011, worked with the intelligence agencies and the MoD to develop a methodology through which the monitoring of such compliance can satisfactorily be achieved and provide details of the outcome of this process later on in this report. I present relevant statistics on the number of occasions the guidance was engaged in discussions with liaison services in the confidential annex to this report. I have attempted, however, to present as many details as possible in the open report about the establishment of the compliance process in relation to the detainee guidance.

E. RIPA process

There exists, in my view, a situation in relation to the MoD where the process set out in RIPA is not fully complied with, for reasons which I have been briefed on and understand. The situation in question relates to the sub-delegation of intrusive surveillance authorisations at the MoD from the level of Secretary of State to members of the Armed Forces. I have seen the internal MoD directives that set out this authorisation process. This delegation of responsibility has been made for operational reasons in relation to intrusive surveillance operations.

I must emphasise, however, that it is not a question of whether the correct legal tests are being applied to the act authorised outside of the RIPA process. I can confirm that undoubtedly the correct tests are being applied i.e. that authorisations are only being given on the basis that they are necessary and proportionate.

3. DISCHARGE OF MY FUNCTIONS

A. Pre-appointment briefings

Although I formally took up the role of Commissioner on 1st January 2011 I did prior to this attend a number of introductory briefing meetings with the intelligence agencies and departments whose conduct I was to oversee. The purpose of these meetings was to provide me with background briefing to the role, the range of intelligence agency operations and authorisations, alongside other contextual briefing. To the extent allowed by national security restrictions, I present further details of what was discussed during these meetings in Figure 1 below

Figure 1: Details of Pre appointment briefings

Agency	Dates	Items discussed
Security Service	18/11/2010 26/11/2010 10/12/2010 14/1/2011	• Introduction with both Director-General and Deputy Director General of Security Service • Threat briefing covering key Counter terrorism/ counter intelligence and counter-proliferation threats to UK • Briefing on current investigations, resources and prioritisation • Briefing on the SyS authorisations, including role of Home Office and ultimately Secretary of State • Policy discussion on Thresholds for Reporting Errors to commissioners and Data Protection Act • Discussion of establishing compliance mechanism and methods of working with international partners on detainee related issues • Discussion on non-statutory oversight
GCHQ	01/12/2010 06/12/2010 and 01/03/2011	• Introductions to GCHQ business and authorisations • Threat briefing provided by Director-General Operations • Visits to various operational teams who rely on authorisations overseen by the commissioner • Meetings with working-level operational staff • Briefing on non-statutory oversight • Shadowing previous commissioner on non-statutory inspection
SIS	30/11/2010 1/12/2010	• Introduction to SIS business and authorisations • Threat briefing • Non-statutory oversight (including development of detainee guidance oversight framework) • Shadowing previous commissioner on formal inspection of authorisations

Northern Ireland Office	6/01/2011	• Northern Ireland Related Terrorism (NIRT) briefing • Briefing on specific aspects of NI related oversight
Cabinet Office	17/12/2010	• Meeting with Deputy National Security Adviser on Green Paper
MOD	02/02/2011	• Pan-MoD scene setting • Global theatres of MoD operations • MoD authorisations and Defence Human Intelligence training • Theatre visits

I found it beneficial to attend these briefings and thank those involved and Sir Peter Gibson for allowing me to observe how inspection visits were conducted prior to my formally taking up the role of commissioner.

B. My Inspection visits

My role is essentially that of a retrospective auditor of authorisations. I am provided with lists of all RIPA and ISA authorisations extant, modified or cancelled some weeks before each bi-annual inspection visit. The intelligence agencies also provide me with any lists required to support my non-statutory oversight at the same time. I am satisfied that the intelligence agencies provide me with a full list of authorisations, and they often highlight particularly challenging warrants for review, in addition to making available paperwork related to errors if required.

Readers of previous commissioners' reports have also asked which legal tests and principles are applied when scrutinising authorisations and engaging in discussions with those officers responsible for planning and executing operations. In essence, I seek to satisfy myself that the intelligence case is sufficiently strong to warrant the undertaking of what is often a significant intrusion into the private life of a citizen, for example interfering in their private dwelling in order to listen to their conversations. I check whether the tests of necessity and proportionality have been applied in constructing the case for this intrusion, the act is necessary to meet one of the statutory aims of the intelligence agency and crucially that there are no other less intrusive means to gather the intelligence the agency seeks to gather. I test these principles by scrutinising the paperwork, which I check for accuracy and the presence where necessary of a signature of the Secretary of State or where appropriate the correctly designated person. I also check whether authorisations have been renewed on time or cancelled when the intelligence dividend does not match the intrusion into the target's private life.

In addition, it has also been my intention to meet with as broad a cross-section of staff as possible, from Director-General to desk officer level. In doing so I wished to test the ethos of the intelligence agencies and, at a working level, both their knowledge of, and compliance with, the authorisations under which they commit potentially intrusive acts in

pursuit of their statutory objectives. I have therefore initiated a series of random, 'under the bonnet' visits, giving only one week's notice of my arrival, which were completed at GCHQ and Security Service in winter 2011. During these visits, I questioned staff across a range of grades as to how they applied the tests of necessity and proportionality when carrying out the acts specified under any authorisation.

I also scrutinise the care officers take to comply with the terms contained within the authorisations. For example, assurances may be given as to the way in which authorisations will be used. Many authorisations are clearly worded with certain conditions which set out which kinds of material and during which times surveillance product can be seen or listened to. I am keen during the scrutiny visits to check whether operational staff are aware of these conditions and are adhering to them. For example, the focus of one of my 'under-the-bonnet' visits to the Security Service assessed how conditions relating to when audio eavesdropping product could be accessed were adhered to by officers within the relevant audio-analysis section. Adherence I should say was complete, and not in doubt.

FIGURE 2: A typical inspection visit

Stage	Purpose
Selection Stage Intelligence agency provide list of extant, expired and modifications to authorisations since last Inspection visit Intelligence agencies also commonly refer commissioner to specific cases of interest concerning either errors or legal issues Commissioner selects at random a number of warrants and authorisations for further scrutiny on inspection day	To provide commissioner with full list of authorisations for selection purposes. Commissioner may raise specific cases for subsequent reading day prior to Inspection day itself To ensure the random nature of Inspections and ensure all warrants have an equal chance of being selected for review
Inspection Day (approx 1 month later) Brief by senior officials on threat and emerging policy issues. Reading through and scrutinising authorisations. Pre-reading time is set aside to ensure commissioner has had time to review all paperwork related to authorisations prior to inspection visit. Where necessary, oral briefings by case officers to detail intelligence case behind the submissions and answer commissioner's questions on any errors	To provide commissioner with a general operational overview as to the nature of the threat in relation to which applications for authorisations Commissioner seeks to reassure himself that throughout authorisation process principles of necessity, proportionality and other safeguards being applied. Specific focus on ensuring renewals are being submitted in good time and that urgent oral applications really are urgent

Follow-up stage	
Meetings with Secretary of State	Feeding back any issues to Secretary of State
Report of Inspections within Annual Report	Ensure getting best value from commissioners' expertise
Potential informal consultation between Intelligence agency and commissioner on challenging legal or policy issues	Characteristic of an effective relationship between commissioner and Intelligence agencies
Discussions with officials at Department of State through whom submissions go before reaching Secretary of State.	

C. Assessment of 2011 Inspection visits

Readers will find details of my 2011 Inspection visits broken down by intelligence agency or government department in the section that follows. I have disclosed, as far as is not detrimental to national security, matters discussed during the inspections themselves.

It is important to note that my overall assessment of compliance in those I oversee is only partially informed by the scrutiny of warrants. As indicated I undertake random visits to discuss compliance, in addition to following up when necessary on errors reported to me during and outside of formal scrutiny visits.

There has been some questioning in the past as to why the commissioner rarely picks up errors within his selection of warrants for review. The answer to this is that during inspections I have available to me should I wish to see them authorisations related to the errors reported to me by each respective intelligence agency since the last inspection visit. All errors identified by the agencies are fully disclosed to the Commissioner upon discovery of the error, and as a result it is unlikely I will identify a new error, although this is not impossible. In essence, I am given the opportunity to scrutinise all erroneous authorisations. This enables me to explore during the formal inspection days why errors occurred and what measures have been taken to minimise the risk of errors being repeated in the future.

Pre-reading days are also important components of my scrutiny function. Here I am able to spend some days, in the SyS case in Thames House, working through files of signed authorisations, intelligence cases, examples of Ministerial submissions on detainee guidance and other matters. Each reading day is set up to enable relevant officers to be questioned in some depth on various matters related to authorisations, errors and legalities in a more constructive manner. Key matters of legal and policy significance are then consolidated from the reading day and presented at the inspection day itself.

Security Service (SyS)

Key dates related to my inspection visits to SyS over 2011 were as follows

Selection Days:	*30th March and 18th August*
Pre-reading days:	*27/28th April and 26th August*
Inspection Days:	*4/5 May and 29/30th September*
'Under-the-bonnet' visits:	*29th November and 2nd December*

During my formal Inspection visits to SyS, the following matters were discussed:

- Introductory meetings with Deputy Director-General and Director-General alongside the heads of various divisions focussed on counter-terrorism, counter-proliferation, counter-intelligence and with legal advisers.
- International Counter-terrorism briefing
- State-led threats briefing
- Northern Ireland Related Terrorist (NIRT) briefing
- Presentations related to specific authorisations
- Olympics planning
- Compliance frameworks for my oversight of Consolidated Guidance on detainees.

I also attended SyS on 29th November and 2nd December to undertake 'under-the-bonnet' visits. During these days I took the opportunity to question technical and operational staff from across grades as to their understanding of the legal framework underpinning the authorisations under which they conducted operations. I used these opportunities to speak to less senior staff than during formal inspections about the ethos of the organization and those steps taken to ensure no more than the absolutely necessary and authorised intrusion into the private lives of targets was being undertaken. I was impressed by the attitude of all staff I spoke to on these occasions.

Home Office

Security Service authorisations must pass through the National Security Unit at the Home Office prior to reaching the Home Secretary. Previous commissioners have therefore undertaken inspection visits to the Home Office as an extra check on such authorisations. I have continued with this practice and undertook formal visits to the Home Office on 2nd September and 20th December. Lists of authorisations current, extant and expired were provided to my office in good time for these review visits. The visits took place in the Home Office, London.

Meeting with Home Secretary

I met with the Home Secretary in early 2012 to discuss my perceptions of the discharge of my functions in 2011. We discussed in broad terms, whether she felt she was supplied with sufficient information when signing property warrants and surveillance authorisations, my views on the intelligence agencies' compliance with RIPA, any specific errors of note I was concerned with, the structure of my upcoming Annual Report, detainee guidance compliance and other relevant policy matters. These matters are discussed in more detail in the confidential annex that accompanies this report and will be distributed to senior intelligence officials across Whitehall.

I am satisfied that the Home Secretary takes a significant amount of care before signing warrants and authorisations that potentially infringe on the private lives of citizens. It was apparent that she took significant time to read submissions, often requesting further information and updates from officials in relation to certain warrants. The Secretary of State does not 'rubber-stamp' authorisations.

Secret Intelligence Service (SIS)

The chronology of my scrutiny visits to SIS over 2011 was as follows:

Selection Days: *18th February and 10th November*

Pre-reading days: *23rd February*

Inspection Days: *22nd /30th March and 30th November.*

Station visits: *23-25th June 2011 (Europe) and 15th-18th November 2011 (South Asia)*

Apart from visits to SIS stations, all inspections were held at SIS HQ, Vauxhall Cross, London.

I believe that my scrutiny of selected authorisations, combined with the level of discussion I was able to have with a cross-section of staff on the subject of legalities during my inspection and wider briefing visits, is sufficient for me to conclude that compliance at SIS was robust. I was again impressed by the attitude of all those that I have spoken who work for SIS.

I discussed the following during my inspection visits:

- Threat briefing

- ISA and RIPA authorisations (ISA s.5 Property warrants, s.7 authorisations and internal RIPA DSAs and CHIS authorisations)
- Non-statutory oversight (including development of detainee guidance oversight framework)

During the non-statutory portion of my oversight visits I explored in some depth with SIS the levels of compliance at desk officer level in relation to sensitive intelligence techniques. Once again, I was assured that officers working for the SIS were conducting themselves in accordance with high levels of ethical and legal compliance.

Government Communications Headquarters (GCHQ)

In relation to GCHQ, lists of relevant material were sent to my office by early March 2011 and late September 2011. My formal inspection visits to GCHQ were on 29th March and 17/18th October respectively. All inspection visits took place at the GCHQ site in Cheltenham. I scrutinised those RIPA and ISA authorisations I had previously selected. In addition, I scrutinised the internal approval documents supporting operations authorised under Section 7 ISA. I also discussed matters related to the development of my non-statutory oversight function in relation to GCHQ.

During December 2011 I also undertook an 'under the bonnet' inspection at GCHQ where I sat in on operational planning meetings. I was able, as with other intelligence agencies, to question a cross-section of staff involved in the day-to-day planning of GCHQ technical operations. In addition, GCHQ legal advisers have taken the opportunity to discuss emerging capabilities with me outside the inspection visits. Once again, it is my belief that based on my scrutiny of GCHQ authorisations, in addition to what I have seen at both Inspection and 'under the bonnet' visits, GCHQ staff conduct themselves with the highest levels of integrity and legal compliance.

Foreign and Commonwealth Office (FCO)

As mentioned previously, as an integral part of the oversight process the commissioner also undertakes an inspection visit to the FCO. The purpose of this visit is to meet with those senior officials at the Department of State (Head of Intelligence Policy Department, Director of National Security and Director-General Defence and Intelligence) who advise the Secretary of State on matters related to his signing of GCHQ and SIS authorisations. I have also used the opportunity to undertake an additional scrutiny of GCHQ submissions.

In relation to the FCO, lists of relevant material were sent to my office by early February 2011 and early November 2011. My formal inspection visits were on 9th March and 29th November respectively. Once again, I was satisfied with both the information provided to me at the FCO and the levels of oversight and compliance shown by those officials I met.

Meeting with Foreign Secretary

I met with the Foreign Secretary on 15th December to discuss the discharge of my oversight role in relation to the intelligence agencies (GCHQ and SIS) for whom he is responsible. In broad terms we were able to have a fruitful discussion on SIS and GCHQ compliance with RIPA and ISA, his views on the level and depth of information outlined within submissions he signs and my development compliance frameworks in relation to detainee guidance. We were also able to discuss the proposed structure of my inaugural annual report, the Justice and Security Green Paper, state-level threats and human rights concerns in relation to liaison services. It was clear to me that the Secretary of State and his staff take their responsibilities extremely seriously. The Secretary of State does not 'rubber-stamp' authorisations.

Northern Ireland Office (NIO)

As part of my oversight function I also visit the Northern Ireland Office in order to inspect authorisations signed by the Secretary of State for Northern Ireland. In relation to NIO therefore, lists of relevant material were sent to my office by mid May and late November respectively. My formal inspection visits took place on 10th June and 13th December in, Belfast.

In broad terms I was briefed on the following during the inspection visits

- Policy and legal matters in relation to selected authorisations
- National Security and Political Update from Senior NIO Officials
- Technical demonstrations
- Discussion on elements of my non-statutory oversight

Meeting with Secretary of State for Northern Ireland

I met with the Northern Ireland Secretary on 23rd November 2011. We covered a wide range of topics during the discussion, including the NI political and security situation, his assessment of the quality of authorisations submitted to him for signature, Olympics planning, my annual report and whether there were occasions when he refused to sign authorisations. It was clear to me that the Secretary of State took his responsibilities for authorising potentially intrusive acts seriously. Although outright refusal to sign authorisations was rare, the Secretary of State did send submissions back for further information on occasion.

Ministry of Defence (MoD)

Lists of authorisations were provided to my office for my selection in good time by early March and October. I undertook reading days on 2nd March and 11th October in preparation for formal inspection visits on 17th March and 10th November respectively. In addition to formal scrutiny of MoD authorisations, I was briefed on the following during the inspection visits:

- Overview of military operations
- Planning for visits to MoD areas of operation
- MoD compliance mechanisms in relation to oversight of consolidated detainee guidance.

I also undertook a theatre visit in July 2011 and met with the Defence Secretary on 21st December 2011.

4 STATISTICS

Readers will be aware that previous Intelligence Services Commissioners have not disclosed in their public reports details of the number of RIPA and ISA authorisations signed by Secretaries of State and information on numbers and types of errors reported to them. My fellow commissioner, Sir Paul Kennedy, did include in his 2010 annual report more details on the numbers and kinds of errors reported to him by those public authorities he oversees. He was also able to include an operational success case study which drew on interception techniques. His previous annual reports have also routinely disclosed the numbers of interception warrants signed by the Home Secretary and Scottish Justice Secretary. Disclosure of both these statistics and error details has been well-received by members of the media and the public alike as contributing to increasing public confidence in the independent oversight provided by the commissioners.

Both Sir Paul and I have worked with those public authorities we oversee to agree how the number of RIPA and additionally in my case ISA authorisations granted could be disclosed in our 2011 open reports without compromising national security. Our starting position was a desire to disclose as fully as possible the numbers of authorisations, in addition to error details, constrained only by being convinced by those we oversee that certain information could not be disclosed due to national security concerns. I have applied an identical approach to Sir Paul last year in relation to the disclosure of total numbers of each kind of authorisations.

Our rationale for the inclusion of such details is that in an era of increased transparency we believe it would aid public confidence in our oversight if readers could discern the volume of RIPA and ISA authorisations the Commissioner must oversee and from which he selects cases for further review during inspection visits.

In relation to errors, it is my belief that disclosing in the open report numbers and details of errors reported to me by those intelligence agencies and departments I oversee is necessary to give confidence in my oversight, it also helps to increase compliance and minimise the risk of such errors being reported in the future. It is clear from the section describing errors that the majority of errors reported to me occur due to human error. I am also able to disclose in this section and the Confidential Annex accompanying this report details of system-changes that are implemented in the intelligence agencies and departments I oversee as a result of these errors. The task has been to balance this desire for disclosure with relevant national security concerns and ensure that neither hostile foreign intelligence agencies nor other targets use the information disclosed to harm the UK. I believe that the correct balance has been struck.

A. Statistics

The total number of RIPA and ISA authorisations I oversee that were approved across the intelligence agencies and MoD in 2011 was 2142. I am confident that such disclosure gives an indication of the total number of authorisations from which the commissioner could potentially sample during inspection visits, whilst not disclosing information that could be detrimental to national security.

B. Operational successes

In the next section I disclose numbers and broad details of errors reported to me by the intelligence agencies. Prior to doing so, however, I feel it would add context for the reader to be made aware of the kinds of operational successes achieved by the intelligence agencies. Only by seeing such examples can the reader conclude, as do I, that the use of potentially intrusive acts is central to intelligence agencies achieving their national security, serious crime or economic wellbeing statutory objectives. I am grateful to the intelligence agency concerned for providing me with an unclassified case study for inclusion in my open report. Details of further operational successes will be made available in the confidential annex to accompany this report.

In late 2010, a large-scale joint Security Service and Police operation investigated a network of individuals, comprised of groups in Stoke-on-Trent, Cardiff and London, some of whom in late 2010 were plotting terrorist attacks against various symbolic targets in London, including through the potential use of IEDs. The network also had longer term plans for a further period of training.

Following the investigation, in December 2010, nine individuals were charged under the Terrorism Act (TACT) with conspiracy to cause an explosion and preparing for acts of terrorism; five of these were also charged with possessing documents of use to a person committing an act of terrorism.

On February 1st 2012, all nine members of the network charged in December 2010 pleaded guilty to offences relating to the plot and were sentenced on 9th February 2012. Eight individuals pleaded guilty to engaging in conduct in preparation for acts of terrorism, contrary to Section 5 of the Terrorism Act 2006. One individual pleaded guilty to possessing an article for a terrorist purpose, contrary to Section 57 of the Terrorism Act 2000.

The majority of the case against the individuals, and the resulting guilty verdicts, was heavily reliant upon warranted material surveillance and eavesdropping against the various members of the network. This focused on the monitoring of conversations in various properties and vehicles in London, Cardiff and Stoke and in providing surveillance coverage of several key meetings between network members.

C. Errors

24 errors were reported to me during the course of 2011, this is a reduction of 14% in comparison to the 28 errors reported by my predecessor Sir Peter Gibson in his 2010 Annual Report. Details of the reporting intelligence agency and, where possible, sanitised elements of how selected errors occurred are also presented in this section. However,

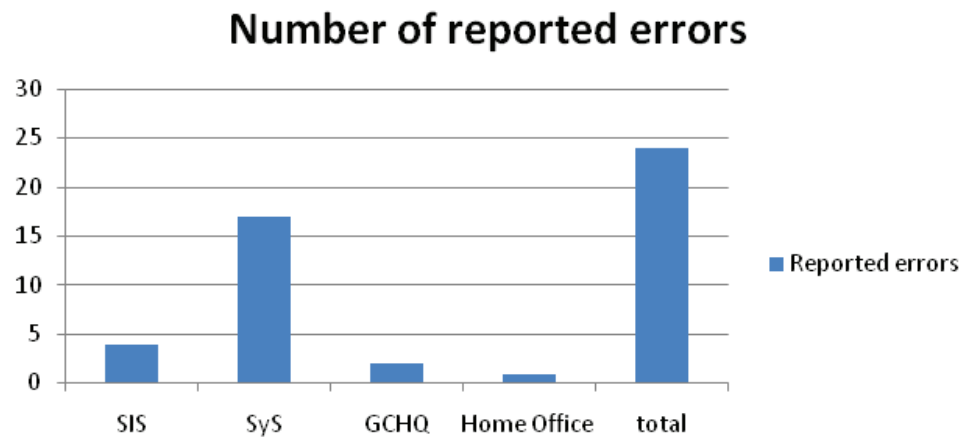
it is crucial to set out from the offset that none of the reported errors or breaches was deliberate. Every single one was caused by human or procedural error, failures to renew authorisations or technical glitches. In relation to SyS who reported the most errors, as a proportion of the total number of authorisations (and as the holder of the highest number of authorisations) the error rate was very low.

It remains my view that the intelligence agencies undertake potentially intrusive acts only when strictly necessary in order to meet intelligence requirements. I believe the chain of authorising these acts, which begins with a desk officer and ends with the Secretary of State or Authorising Officer signature, involves significant consideration at each stage of ethics and compliance. It would therefore take a huge conspiracy if any deliberately unlawful activity was being carried out. At each stage there is due consideration of legalities, collateral intrusion and whether the intelligence dividend proposed can be reaped from other, less intrusive means.

That is not to say, however, that errors cannot occur in fast-paced, complex investigations. It is in my opinion the learning from these errors that is crucial to ensure such mistakes are not repeated in the future. The confidential annex contains details of the most common kinds of errors that have been reported to me and details of system changes that have been implemented as a result of my oversight.

The breakdown of errors by reporting intelligence agency or department is shown in Figure 3 below

Figure 3: Errors broken down by reporting intelligence agency or department



Readers will discern from Figure 3 that the total number of errors reported across all those intelligence agencies and departments I oversee represents 1.1% of the total number of RIPA/ISA authorisations approved throughout the year. In my opinion, this low percentage is illustrative of two things; firstly, that human error is likely to occur in any fast-paced, complex and evolving investigation the likes of which the intelligence agencies engage with on a daily basis. Secondly, that the intelligence agencies conduct their business with high levels of ethical and legal compliance.

My assessment, having reviewed reports, policies and practice related to errors throughout 2011, is that in all cases errors were due to human oversight or administrative shortcomings. As far as I am able to reveal without prejudicing national security, I can report that 15 out of 24 errors (63%) were due to the correct authorisation not being applied for or being renewed, 5 out of 24 errors due to a failure to remove equipment (20%), 3 out of 24 (12.5%) were procedural errors and 1 error (4.2%) due to an incorrect transposition of digits onto a collection system

I too have followed the practice of my fellow commissioner Sir Paul Kennedy and have attempted in this year's annual report to set out, as far as security restrictions allow, broad details of kinds of errors reported to me. Figure 4 is the product of this approach. There are however, certain errors details of which I am unable to give without prejudicing safeguards around national security and techniques of the intelligence agencies. Therefore, some of the generic examples I outline in the grid are typical of the whole and anonymous as far as the targets are concerned.

Figure 4: Details of selected reported errors

Agency	Date/ period of error	Date/period of error
SyS	March 2011	A DSA was obtained to operate against a long-standing target. However, due to human error, renewal paperwork for the DSA did not reference a type of surveillance activity taking place. The correct paperwork was subsequently completed upon discovery of the omission and it was reported an IT system change would minimise the risk of such an error being repeated.
SIS	February 2011	The error concerned a lack of authorisation under Part 2 RIPA. An officer had approached an individual to determine whether they were suitable to work as a potential CHIS without completing the requisite authorisation. The officer realised his error immediately and reported it to the compliance team. The officer's team leader, once informed of the error, stated that he would have granted the authorisation had it been requested. The team leader reviewed RIPA obligations with the officer to ensure future compliance.
GCHQ	September 2011	This error related to an operation authorised under ISA. Successful testing of techniques had been completed satisfactorily prior to the operation commencing. During the operational phase, an error was identified. An investigation was mounted, which identified the cause of the error as a software bug that had arisen during a transfer of systems in Summer 2011. This transfer of systems had involved much re-writing of software code and despite careful review of systems and testing, it was likely the software bug had been introduced during this stage. The investigation team checked for other instances of the technique not functioning properly- none were found. A review of the operation revealed no further instances of the error having occurred.

5. CONCLUSION

In conclusion, I can report that I am satisfied that the intelligence agencies and MoD are fully aware of their legal obligations. In particular, they are aware of the need for the object in obtaining the intelligence being sought to be in discharge of one or more of their statutory functions; secondly, that the action in question has appeared to be both necessary for obtaining information which could not be obtained by less intrusive means and also proportionate to what is sought to be achieved. Naturally human errors can occur, and have occurred. However, such errors are few in number and almost without exception relate to failures to renew an authorisation which was then properly obtained but where for the period unauthorised the information obtained was not used except where deemed necessary for the pursuit of agency statutory objectives. The second most common class of error relates to the failure to cancel an authorisation where no material was actually obtained. I have set out in this report details of which intelligence agencies reported authorisation errors to me throughout the year, and where possible details of such errors. I am clear that all take any error very seriously and take steps to prevent it recurring.

I have also met with the Secretaries of State who normally issue warrants and authorisations. They of course rely to a great extent on the accuracy of the information supplied. By the time submissions reach the Secretaries of State I am satisfied they have been scrutinised by a number of persons in the intelligence agencies and in the office of the Secretaries of State. I have spoken with those persons and am satisfied they are persons of the highest integrity and ability. It is also clear to me that even then the Secretaries of State do not simply accept and sign what is put in front of them, but take their obligations seriously. I conclude that the respective Secretaries of State have properly exercised their statutory powers. I am also satisfied that in 2011 the various members of the intelligence agencies have properly exercised their powers. I am satisfied that the MoD and armed forces in so far as they come within my remit have properly exercised their powers.

In the introduction to this report I discussed certain misconceptions and criticisms which may have cast doubt on the effectiveness of the oversight of the commissioner. I hope that public confidence will be increased by three key changes to this report; further clarification of the commissioner's remit, greater transparency in the oversight process and finally my reasoning behind why operational details behind those warrants I oversee must remain secret.

To this end, I have set out once again in my report the legislative basis underpinning my oversight as commissioner. I have also disclosed the Prime Minister's expectation of my role: readers will, I hope, observe that I do not have blanket oversight of the intelligence agencies. Indeed my role is tightly defined as overseeing the powers granted to Secretaries of State, and on occasion internally within the intelligence agencies, to authorise certain acts which may intrude into the private lives of citizens in the pursuit of intelligence agency objectives.

I have sought to disclose more details than ever before of those compliance processes upon which I base my conclusions that the intelligence agencies and departments I oversee are compliant with the relevant legislation. I am grateful therefore to both the intelligence

agencies themselves and Secretaries of State for facilitating the disclosure of total numbers of authorisations signed or approved, and details of errors reported to me. Such details are naturally of interest to readers, as they reflect the extent and impact of my oversight. I have therefore based my assessment that the number of warrants I scrutinise is appropriate on two key reasons. Firstly, although the number is small the selection is random and the number I believe to be significant.

Secondly, and for me most importantly, I have been able to make a number of extra checks throughout the year that support the formal warrantry inspections themselves. I have taken into account the discussions I have had with a cross-section of staff during these meetings and formed the judgement that the intelligence agencies conduct themselves with proper regard for legalities and good ethical judgement.

One of the key areas of interest previously has been the lack of faulty warrants selected by the commissioner during his inspection visits. In my opinion, the likelihood, as shown this year, of my randomly selecting a warrant and finding it to be erroneous is decreased by the fact that the intelligence agencies themselves make available details of erroneous authorisations during my inspection visits. The error reports received are in-depth, clear and focus on system-changes undertaken within the intelligence agencies to reduce the likelihood of similar errors being repeated. I am then able to observe the relevant paperwork or speak to the officers involved should I wish to. This is reflective of the mutually constructive relationship that I enjoy with those intelligence agencies and departments I oversee.

Finally, during a period of potential reform, driven not least through the emerging Justice and Security Bill and wider world events, there must however be an acceptance that operational details within the authorisations I oversee should remain secret. I can with some confidence state that, although I have sought to bring as much information about my oversight, surveillance errors and successes into the open report, revealing further operational information about intelligence agency investigations could aid hostile states and individuals who may wish to cause harm to the UK.

It has therefore been necessary for me to draft a separate confidential annex to this report containing information not for public disclosure. I can assure readers of two things; firstly, that any reasonable member of the public would be convinced that the operational detail contained in this annex is just that-operational detail, comprising target names and techniques utilised by intelligence agencies, which must be protected in the interests of national security. Secondly, I have sought to widen the distribution of this annex across Whitehall to ensure that senior officials and Ministers subject to my oversight share successes and learning that may arise through the function of oversight.

6. EXTRA-STATUTORY OVERSIGHT

CONSOLIDATED 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

My predecessor, Sir Peter Gibson, agreed to monitor compliance by intelligence agency officers and military personnel on the standards to be followed during the detention and interviewing of detainees as set out by the Consolidated Guidance published in July 2010. I have been content to follow this practice.

When I inherited the responsibility to oversee compliance with the Consolidated Guidance I had some anxiety in relation to the broad scope of the guidance and thus what I would be required to oversee. I therefore discussed with the Cabinet Office, the MoD and the intelligence agencies which areas would fall under my remit, and in broad terms the mechanisms that would be needed to be established to enable my monitoring of the guidance.

As a result of these discussions it was agreed that my oversight would be limited to occasions where members of the intelligence agencies or MoD;

- had been involved in the interviewing of a detainee held overseas by a third party (this may include feeding in questions or requesting the detention of an individual)
- had received information from a liaison service (solicited or not) where there is reason to believe it originated from a detainee.
- had passed information in relation to a detainee to a liaison service

Most importantly, it was agreed that my remit would not include oversight of adherence to the consolidated guidance in relation to MoD detention operations or the subsequent handing over of detainees by the MoD to a host nation for prosecution.

A. Compliance framework

I now set out the framework I have developed in conjunction with the intelligence agencies and MoD to allow me to satisfy myself as to levels of compliance with the guidance, to the extent set out by my remit above. I thus received correspondence from the Cabinet Office in June 2011 which set out the process by which the intelligence agencies and MoD would provide the necessary information for me to fulfil my remit. This outlined that the process through would I monitor compliance would be as follows:

1. Intelligence agencies and MoD would be required to compile separate lists of all cases in which their staff have been involved in the interviewing of a detainee held overseas by a third party, or where they had fed in questions or solicited the detention of such an individual. The lists would note key details of each case.

2. It was recognised that liaison services did not often disclose the sources of their intelligence. Therefore it was agreed that the lists outlined in (1) would also contain cases where personnel had received unsolicited intelligence from a liaison service that they knew or believed had originated from a detainee, and which caused them to believe that the standards to which the detainee had been or would have been subject were unacceptable. In such cases senior personnel would always be expected to be informed.

3. I would then inspect randomly-selected cases for further review and discussion during my formal Inspection visits to each intelligence agency or the MoD.

4. It was also agreed that the examination of such cases in isolation was unlikely to provide the full context necessary to report to the Prime Minister on the discharge of this element of my oversight. It would also be beneficial for me to receive wider briefing on the context of liaison relationships with challenging partners to take a view on whether the assessments about individual cases, for example in relation to the obtaining of assurances, were being made sensibly. It was agreed therefore that I would receive more contextual, in-country and UK-based briefings from the intelligence agencies and MoD on their relationship with relevant liaison partners.

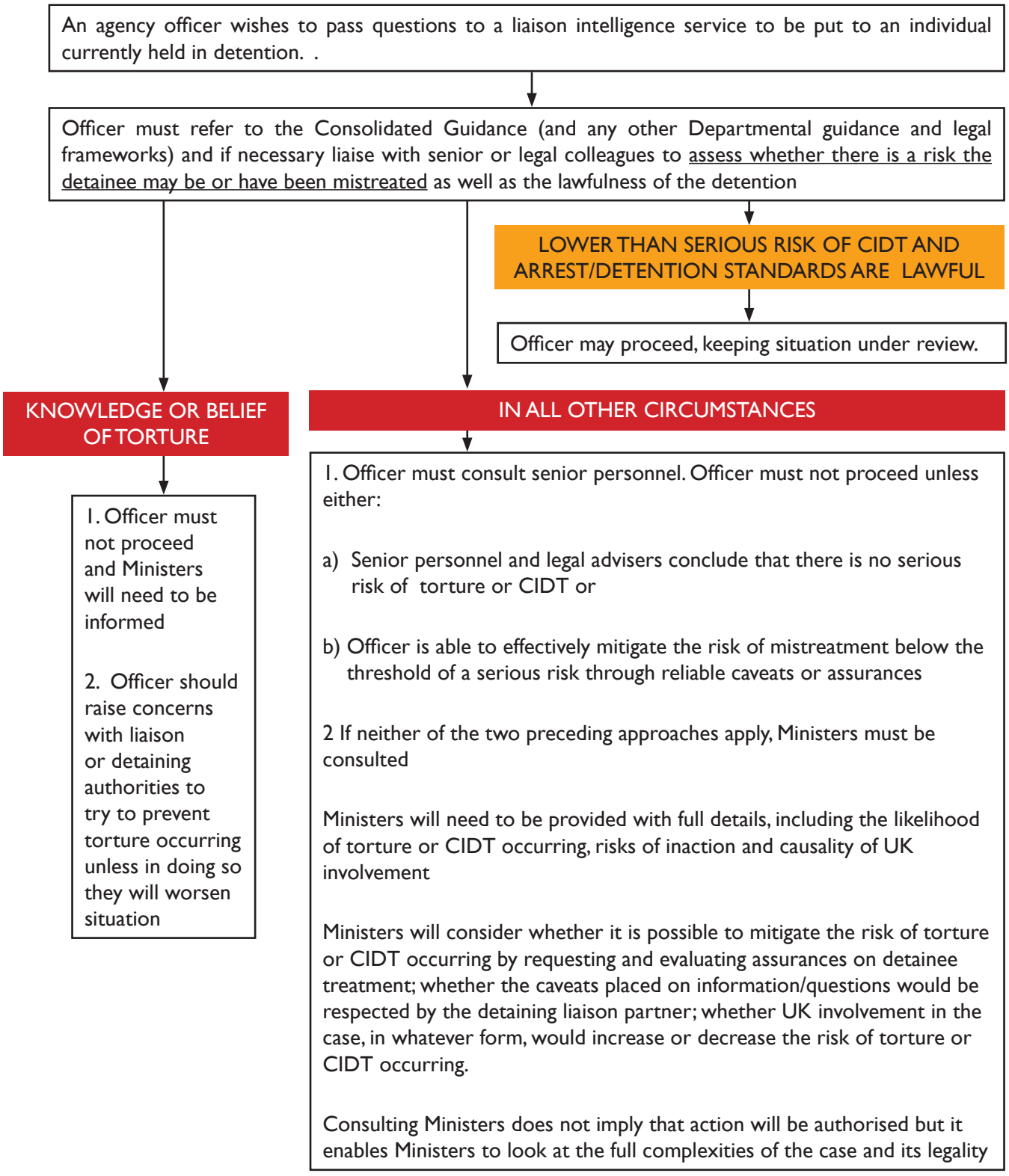
I have attempted to ensure that the intelligence agencies and MoD (where applicable) follow a consistent process in presenting detainee cases for my selection and subsequent in-depth review. I have therefore developed in conjunction with relevant intelligence agencies and MoD a 'detainee grid' which sets out cases which fall within my remit for selection and potential subsequent review. The detainee grid, presented as a spreadsheet, lists the following information;

- Date of request
- Details of the operation or overarching submission (if any) under which liaison service is being engaged
- Details of liaison service and if available detainee or objective that is subject of intelligence request or detention
- Assessment of risk of mistreatment i.e. whether risk of torture, serious or lower than serious risk of Cruel or Inhuman Degrading Treatment (CIDT)
- Details of reference to senior personnel, legal advisors or Ministers
- Level at which decision taken.

I am then able during the selection stages preceding my inspection visits to review these lists and identify cases to examine further, for which the intelligence agencies and MoD provide fuller details, including access to relevant personnel and supporting Ministerial submissions.

The process for me to receive in-country briefings in relation to challenging partners is much more qualitative in nature. However, I have received throughout the year during my station visits a number of such briefings. I have spoken to intelligence agency officers stationed overseas in some depth about the nature of their interaction with liaison services in relation to detainees. I am under no illusions that this is a highly sensitive and complex area in which to operate and to seek those assurances upon which, for example, decisions around the passing and receipt of intelligence in relation to detainees are often based.

Figure 5: Steps to be taken by officers when considering whether to pass intelligence or solicit detention from an overseas liaison service



B. Principles

I have drawn upon the following principles when working with others to set up the oversight mechanism for monitoring compliance with the detainee guidance:

- UK intelligence agencies do not have powers of detention either in the UK or overseas. They must work with liaison services, referring where necessary to steps set out in the detainee guidance, when seeking to pass or receive intelligence related to detainees, or requesting the detention or interviewing of detainees held by liaison services.
- UK armed forces may need to detain and question detainees in support of mission objectives. In such cases 'interviewing' also includes tactical questioning, interrogation or debriefing. It was agreed between myself, Sir Peter Gibson and the Cabinet Office/ MoD that oversight of detention operations and interviewing by military personnel of detainees does not fall within the scope of the commissioner's oversight role. The commissioner will oversee in relation to the MoD, however, compliance with the guidance in relation to occasions where MoD personnel interview, or pass or receive intelligence relating to, detainees in the custody of another nation.
- Where intelligence agencies and the MoD have set up their own internal guidelines governing interaction with liaison services in relation to detainees, it is important that the principles of the guidance are embedded fully within such guidelines. These internal guidelines do not replace the consolidated guidance which must be adhered to by all intelligence agencies and MoD personnel. The principles of the consolidated guidance also need to be reflected in any internal training that may be given to intelligence agency staff and military personnel who may come across detainee issues in their day-to-day work.
- Officers and military personnel should consider whether a detainee may be or have been mistreated on each occasion they seek to pass or receive intelligence related to a detainee or solicit the detention of a detainee by a third party. The role of the guidance specifically is to set out the process that should be followed on occasions where officers assess that there is a risk of torture or CIDT. My oversight is confined to checking whether the process set out in the guidance is being followed, and it is upon this that I make those statements of compliance set out below.
- If reliance is placed upon assurances then it falls within my remit to assess the existence of these assurances.

C. Assessment of compliance

I am thankful to those involved in setting up the relevant procedures. I will follow the practice of my predecessor in not disclosing publicly statistics or details of the number of occasions in 2011 each intelligence agency submitted to Ministers in accordance with the Guidance. I feel such details, and the subject matter of my contextual briefing in overseas stations, are better disclosed in the Confidential Annex to be shared across senior intelligence officials in Whitehall. That said I do present in the sections that follow my assessment of compliance in relation to the detainee guidance in each intelligence agency I am charged with overseeing.

SyS

The Security Service played a significant role in the development of the early drafts of the detainee grid which subsequently became the blueprint for the other intelligence agencies. They should be commended for this early work; I am fully content that, as far as I am able to discern, I have been fully availed of all cases where officers have either submitted to Ministers or to senior personnel/legal advisors in relation to detainee-related business. SyS submitted on a number of cases to Ministers and senior management in relation to the passing and receipt of intelligence related to detainees or soliciting of a detainee's detention by a liaison service. I have noted that the Home Secretary takes her responsibilities as set out in the detainee guidance seriously. There have been occasions when either Ministers or senior management decided not to proceed and I have been given opportunities to review associated paperwork during my scrutiny visits. SyS have encouraged staff to take a cautious view of the guidance and refer cases to senior management when in any doubt so that risks and mitigations can be fully considered.

SIS

SIS clearly operates in a much more complex environment than any of the other intelligence agencies or the MoD in relation to detainees. I am currently working with SIS to develop a detainee grid that is to my full satisfaction, however, in relation to those cases I have scrutinised in detail, I am confident that SIS have provided me with full details of cases and are compliant with the process set out in the guidance. I have seen the SIS internal policy on detainees. I have observed during my inspection visits that it is SIS policy, furthermore, to be more cautious than is strictly necessary in relation to consulting the Foreign Secretary in situations where there may be a risk of CIDT.

In addition, I have formed the clear view from my station visits, which have included in-depth conversations with officers involved on a daily basis in complex decisions related to detainees, that adherence to the standards set out in the consolidated guidance is at the forefront of officers' minds in any interaction undertaken with liaison services in relation to detainees.

GCHQ

GCHQ have also been fully compliant in relation to the process established to support my oversight of the consolidated guidance. The grids supplied in support of my formal oversight visits have been fully populated and relevant officers have been available during inspection visits to discuss those cases I have selected for further review. GCHQ does not solicit the detention of detainees through liaison services. I am convinced that GCHQ is more likely to play a supporting role to the other intelligence agencies and MoD in relation to soliciting the detention of detainees through liaison services or the passing and receipt of intelligence related to detainees. GCHQ have consulted senior personnel in 2011 in relation to detainee cases and from the cases I have seen are fully compliant with the consolidated guidance on such occasions and in relation to their internal policies and practices.

MoD

The majority of MoD business related to detainees is concerned with MoD-led detention operations, which, as set out earlier on in this section, falls outside of my remit. In relation to cases which fall within my remit, MoD have reported that on no occasion in 2011 have they solicited the detention of an individual by a liaison service, interviewed a detainee held overseas by a third party nor received from a third party any unsolicited information believed to originate from a detainee. There have been occasions where MoD personnel have sought information from detainees held by coalition partners. I refer to these in more detail in the confidential annex to this report.

Conclusion

Based on the information provided to me, and to the extent set out in my remit, I am not aware of any failure by a military or intelligence officer to comply with the Consolidated Guidance in the period between 1st January and December 31st 2011. I have received assurances from the relevant departments and intelligence agencies that they have disclosed fully relevant information about cases within the detainee grid. I am also assured that I have been given full access to both information and officers to discuss particular cases both in the UK and during Station visits. I therefore have no reason to doubt that the guidance is being complied with based on the information that has been provided to me in 2011.

I can report that from what I have seen the intelligence agencies and MoD take their human rights and legal obligations towards detainees seriously. I shall be particularly keen to develop additional processes in future to help me in overseeing this complex element of my non-statutory remit.

ANNEX A
CASE STUDY 1 - DIRECTED SURVEILLANCE AUTHORISATION (DSA)

A reliable source (authorised CHIS) puts forward a target name during a debriefing session. As a potential threat to national security this falls within one of the functions of the Security Service. The name is corroborated with other intelligence sources.

Applicant officer assesses whether the resource, intelligence and wider operational case behind whether the previously unknown individual should be placed under directed surveillance. The applicant may begin to draft a written DSA or request urgent oral authorisation to commence the surveillance

ROUTINE

The application is passed to an authorising officer who may only grant the DSA in writing. The application should include;

- Description of conduct to be authorised and purpose of investigation
- Reasons why authorisation is necessary in the particular case and on the grounds listed in s.28 (3) of RIPA
- Nature of the surveillance
- The identities where known of those to be subject of the surveillance
- Summary of intelligence underpinning application and information it is desired to obtain as a result of the surveillance
- Details of potential collateral intrusion and justification
- Details of any potential confidential information that may be obtained
- Reasons why the surveillance is considered proportionate
- The level of authority required for the surveillance
- Record of whether the authorisation was given or refused, by whom, and the time and date of when this happened.

URGENT

Authorisation may be given by the authorising officer to the applicant officer orally in urgent cases (occasions when any delay in authorising the directed surveillance may endanger life or a specific operation), however the action must be recorded in writing by the authorising officer and applicant as soon as practicable. In such cases the authorising officer and applicant, where applicable, should record the following information in writing as soon as practicable

- Identities of those subject to surveillance
- Nature of the surveillance
- Reasons why authorising officer consider the case so urgent as to require an oral authorisation

Where the officer entitled to act in urgent cases has given written authority, reasons must be given as to why it was not practicable for the application to be considered by the authorising officer. Authorising officers should not typically be involved in authorising operations in which they are directly involved, however this may sometimes be unavoidable. Centrally retrievable records should be kept in all cases and made available for review by me.

DURATION:

A written DSA will be valid for three months beginning from the time it took effect

An urgent oral authorisation will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation was granted.

Highly skilled specialist surveillance officers carry out the directed surveillance producing high-quality intelligence on the target, which facilitates their identification along with a preliminary assessment of their pattern-of-life.

RENEWAL:

If a member of the intelligence agencies entitled to grant DSAs considers it necessary the authorisation should continue on the grounds of national security or in the interests of the economic well-being of the UK, he may renew it for six months beginning on the day the original DSA would have ceased to have effect.

If the original authorising officer considers the authorisation necessary for continuation for the purpose it was originally granted, he may renew it in writing for a further period of three months.

In all renewal cases the applicant should consider and record

- No. of occasions the DSA has been renewed if any
- Significant changes to information in the original application
- Why the DSA should continue
- The intelligence dividend reaped by the surveillance
- Results of regular reviews of the operation

Authorisations may be renewed more than once if necessary and provided they continue to meet the relevant criteria

Using results gleaned from this period of furrther surveillance, officers conclude that the indvidiual's visits to the premises of interest and interaction with other potnetial targets has diminished significantly. It is decided the DSA should be cancelled.

CANCELLATION:

An authorising officer must cancel a DSA if satisfied the directed surveillance as a whole no longer meets the criteria upon which it was authorised. If the authorising officer is not longer available, the current incumbent of the position must undertake this duty.

Instructions must be given to operational staff to cease any surveillance activity- the date of cancellation must be centrally recorded and any relevant documentation kept for review.

Extant, cancelled and refused DSAs may be subject to review by the Intelligence Services Commissioner during his inspection visit.

For the organisations over whom I have oversight, an authorisation for intrusive surveillance in the UK may only be granted by the Secretary of State.

In many cases, operations involve both intrusive surveillance and entry on, or interference with, property or wireless telegraphy. On such occasions a combined authorisation (s.5 ISA property interference warrant and pt 2 RIPA intrusive surveillance warrant) may need to be sought from the Secretary of State. However, the criteria for the authorisation of each activity must be considered separately.

CASE STUDY 2 - COMBINED PROPERTY INTERFERENCE AND INTRUSIVE SURVEILLANCE WARRANTS

An intelligence agency wishes to place a listening device into a private motor vehicle to record for intelligence purposes conversations between suspected targets of concern for national security.

Applicant officer will work closely with operational, management and legal colleagues to ascertain the case behind the potential deployment of the equipment. Decisions will often be made on the basis of dividends from earlier DSA s, interception warrants and other intelligence sources.

ROUTINE

An application for a combined property and intrusive surveillance warrant may be commenced by the officer, in writing (unless urgent) and should describe the;

- Conduct to be authorised and purpose of investigation
- Reasons why authorisation is necessary in the particular case and on the grounds listed in s.32 (3) of RIPA
- Nature of the surveillance
- Residential premises or private vehicle in relation to which interference and surveillance will take place, where known
- The identities where known of those to be subject of the surveillance
- Summary of information it is desired to obtain as a result of the surveillance
- Details of potential collateral intrusion and justification
- Details of any potential confidential information that may be obtained
- Reasons why the surveillance is considered proportionate to what it seeks to achieve

URGENT

In urgent cases, information that forms the basis of a written intrusive surveillance application can be supplied orally to the Secretary of State. In such cases the applicant should also record the following in writing as soon as is reasonably practicable:

- The identities where known of those to be subject of the surveillance
- Nature and location of the surveillance
- Reasons why and urgent instead of written authorisation is necessary

In such cases, a warrant may be signed (but not renewed) by a senior official with the express authorisation of the Secretary of State.

The combined application then passes from the officer to the Secretary of State through the Department of State for authorisation. Before granting a warrant, the Secretary of State must be satisfied that the property interference and intrusive surveillance are;

- Necessary for the agency to carry out its functions
- Proportionate to what it seeks to achieve

The Secretary of State must also consider whether;

- Any intelligence being sought could be obtained through less intrusive means and that
- Satisfactory arrangements are in force in respect of the disclosure of any material obtained by means of the warrant

DURATION:

If granted by the Secretary of State, a combined warrant will cease to have effect, unless renewed, after six months beginning with the day of issue (if issued under the hand of the Secretary of State) or at the end of the fifth working day following the day on which it was issued (in any other case)

The agency wish to renew the combined warrant as despite it taking time to identify an opportunity to deploy the device, the intelligence yield from the device has been significant to the ongoing investigation.

The Secretary of State may renew such a warrant if necessary for a period of a further six months beginning from the day it would have ceased to have effect. In order to support the case for renewal, the agency should supply the Secretary of State with information on the intelligence yield produced by the surveillance and property interference authorised.

The investigation reaches a successful conclusion and it is decided to cancel the combined warrant and remove the device when practicable.

The original applicant must apply to the Secretary of State for the warrant to be cancelled, if he is satisfied the warrant no longer meets the criteria for which it was authorised. If this person is no longer available, the current incumbent of the position of the original application should draft the cancellation application. The Secretary of State must cancel the application.

Under RIPA, a person is a CHIS if

a. he establishes or maintains a personal relationship with a person for the covert purpose of facilitating the doing of anything falling within b) and c) below

b. he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c. he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

It is important to note that, as alluded to in Paragraph 2.9 of the Home Office CHIS Code of Practice, the intelligence agencies and indeed public authorities more widely are not required by RIPA to obtain an authorisation just because one is available. The use or conduct of a CHIS can be a particularly intrusive and high-risk covert technique. It requires dedicated and sufficient resources, oversight and management. Agencies must ensure that all use or conduct of CHIS is necessary and proportionate to any potential intelligence dividend and in compliance with relevant Articles of the ECHR, in particular Articles 6 & 8. A number of further complexities exist in relation to the use of CHIS, including issues around when a human source becomes a CHIS, tasking, covert surveillance of a CHIS, welfare issues, use of technical equipment and special considerations. Once again I would draw readers' attention to the relevant sections of the Home Office CHIS Code of Practice for further information.

CASE STUDY 3 CHIS AUTHORISATION

An intelligence agency, working with the Police, wish to obtain details of the travel plans of an individual Mr X, in the interests of national security. The agency is aware of Mr Y, a close associate of Mr X, who would be able to provide the necessary information. Mr Y is however not of direct security interest. The agency therefore wishes to authorise the use of Mr Y, known to an operational officer, as a CHIS.

An application is commenced to authorise the use or conduct of a CHIS. This should be in writing and record:

- Why the authorisation is necessary in order to pursue one of the agency's statutory objectives
- The purpose for which the CHIS will be tasked or deployed
- The nature of any wider investigation or operation
- The nature of what the CHIS conduct will be
- Details of any potential collateral intrusion
- Details of any confidential or legally privileged information that may be obtained
- Reasons why the authorisation is considered proportionate to what it seeks to achieve
- The level of authorisation required

The application is then passed to an authorising officer

The authorising officer in the agency may grant an authorisation for the use or conduct of a CHIS, under Part II of RIPA if he believes that the authorisation is necessary and proportionate. Authorising officers should not be responsible for authorising their own activities and be independent of the operation. Records should be kept for review by the Commissioner when this occurs.

In urgent cases oral authorisation can be given for the use or conduct of a CHIS. A statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant. The full information pertaining to the authorisation should be recorded in writing when reasonably practicable (generally the next working day). Cases should only be considered urgent if the time that may lapse before the authorising officer is available to grant the authorisation is likely to endanger life or jeopardise the operation.

DURATION:

A written authorisation will be valid for twelve months beginning with the day it took effect.

Urgent oral authorisations will unless renewed be valid for seventy-two hours, beginning with the time the authorisation was granted.

The initial phases of the CHIS engagement and tasking are successful. The CHIS provides valuable intelligence in relation to the ongoing investigation into Mr X. The authorising officer and handler rightly engage in regular reviews of the authorisation.

REVIEW

Each regular review should consider whether it remains necessary and proportionate to use the CHIS and thus justified to continue the conduct. The review should also consider

- The use made of the CHIS during the period authorised
- Details of any tasking given to the CHIS
- Any information gained from the CHIS
- Results of a review should be retained for at least three years. Reviews should be more regular in cases that involve access to confidential information, use of a juvenile or significant collateral intrusion.

↓

The CHIS handler and authorising officer decide to renew the CHIS authorisation and continue to task the CHIS

↓

RENEWAL

Prior to renewing an authorisation, the authorising officer must be satisfied that a review has been carried out of the CHIS and its results considered. The authorising officer may renew the CHIS authorisation for a further period of twelve months in writing. This begins to take effect from the time the authorisation would have expired but for the renewal. Urgent oral renewals may be granted for a period of seventy-two hours. Any person entitled to grant an authorisation may renew one. Authorisations may be renewed more than once. Documentation relating to renewals should be kept for at least three years and record

- Whether this is the first renewal or details of previous renewals
- Significant changes to information in the original application
- Reasons why it is necessary for the authorisation to continue
- Tasking of the CHIS since the last review
- Information obtained from tasking since last renewal
- Results of regular reviews on use of CHIS

↓

Results of the next review meeting reveal the original target Mr X has moved overseas and thus it is not necessary to continue to task Mr Y as a CHIS. The CHIS handler and authorising officer agree to cancel the authorisation.

↓

CANCELLATION

The authorising officer who granted or renewed the CHIS authorisation must cancel it if it is no longer deemed necessary or proportionate to continue the conduct or use of the CHIS. Where the authorising officer is not available the task falls to the current incumbent of that original authorising officer's position. The safety and welfare of the CHIS should be taken into account after the authorisation has been cancelled.

ANNEX B
SUMMARY OF RIPA AND ISA

Readers will find below a summary of the relevant sections of RIPA and ISA relating to the oversight provided by the Intelligence Services Commissioner.

Regulation of Investigatory Powers Act (RIPA, 2000)

Which section of RIPA?	What is the power?	What is a typical use of this power?	When can this power be used?	Who can use the power?	Who authorises and who oversees the responsible use of power?
Pt 3	The investigation of electronic data protected by encryption	Request for encryption password or key pertaining to criminal suspect's computer	• Interests of national security • Prevention/ detection of crime • Interests of economic well-being of United Kingdom; or For the purpose of securing the effective exercise or proper performance by any public authority of any identified statutory power or statutory duty	Any public authority	Authorisation is most frequently by a Judge. Except when authorised by a judicial authority, oversight is conducted by the Interception of Communications, Intelligence Services and Surveillance Commissioners

Directed surveillance, intrusive surveillance, Covert human intelligence sources					
Which section of RIPA?	**What is the power?**	**What is a typical use of this power?**	**When can this power be used?**	**Who can use the power?**	**Who authorises and who oversees the responsible use of power?**
Pt .2	Intrusive Surveillance	Gaining access to a suspect's private home or vehicle and gathering private information	In the interests of National Security The economic well being of the United Kingdom Preventing or Detecting Serious Crime	Intelligence Agencies MoD and Armed Forces A full list of senior authorising officers for intrusive surveillance is set out in s.32 (6) of RIPA.	Warrant signed by One of her Majesty's principal secretaries of state Oversight of intelligence agencies' and MoD use of powers provided by Intelligence Services Commissioner Oversight of Police use of powers provided by Chief Surveillance Commissioner.

Pt. 2	Directed Surveillance	Undertaking authorised surveillance of an individual terrorist suspect's movement to establish pattern of life information	• In the interests of national security • Prevention and detection of serious crime • Safeguarding the economic well-being of the UK • In the interests of public safety, • For the purpose of protecting public health, • For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department	Intelligence Agencies (SyS, SIS, GCHQ) Police Forces (HO, Met, City, Scotland, PSNI) Military Police Forces (Army, Navy, Air Force) Armed Forces (Army, Navy, Air Force) Serious Organised Crime Agency HM Revenue and Customs For a full list of authorising officers for directed surveillance refer to Regulation of Investigatory Powers (DS and CHIS) Order 2010 SI 2010/521.	A senior member of that authority Surveillance Commissioner oversees authorisations by Law Enforcement Authorities, Chief Officers of Police, SOCA and HMRC Intelligence Services Commissioner has oversight of authorisations by Intelligence Agencies.
Which section of RIPA?	**What is the power?**	**What is a typical use of this power?**	**When can this power be used?**	**Who can use the power?**	**Who authorises and who oversees the responsible use of power?**

Pt. 2	Covert Human Intelligence Sources (CHIS)	Authorisation of the conduct of an informant or 'agent' developing a relationship with a counter-proliferation target	• In the interests of national security • Prevention and detection of serious crime or of preventing disorder • Safeguarding the economic well-being of the UK • In the interests of public safety • In the purpose of protecting public health • For the purpose of assessing or collecting any tax, duty, levy or other imposition , charge or contribution payable to a government department	Intelligence Agencies (SyS, SIS, GCHQ) Police Forces (HO, Met, City, Scotland, PSNI) Military Police Forces (Army, Navy, Air Force) Armed Forces (Army, Navy, Air Force) Serious Organised Crime Agency HM Revenue and Customs For a full list of authorising officers for CHIS refer to Regulation of Investigatory Powers (DS and CHIS) Order 2010 SI 2010/521.	Surveillance Commissioner oversees authorisations by Police/ Law Enforcement Authorities, Chief Officers of Police, SOCA and HMRC Intelligence Services Commissioner has oversight of authorisations by Intelligence Agencies. CHIS authorisations are made by a senior member of that authority

Intelligence Services Act (1994)

Enacted on 26th May 1994

Placed the Intelligence Agencies on a statutory footing

Established the Intelligence and Security Committee (ISC) to provide parliamentary oversight of the intelligence agencies.

Which section of ISA	What is the power?	What is a typical use of this power?	When can this power be used?	Who can use the power?	Who authorises and who oversees the responsible use of power?
Section 5 (Property Warrants)	Entry or interference with property or with wireless telegraphy	Entering a premises to implant a recording device	If Secretary of State is persuaded the action is: • necessary for the applying Agency to carry out one of its statutory functions, • proportionate to what it seeks to achieve • satisfactory arrangements are in place with respect to the disclosure of information that may be obtained • Intelligence cannot be obtained through less intrusive means	Security Service, SIS or GCHQ	Authorisation through signature by Secretary of State (most commonly Foreign, Home or Northern Ireland Secretary) Exercise of powers to grant authorisations overseen by the Intelligence Services Commissioner

Section 7 ISA and amended by s.116 of Anti-terrorism Crime and Security Act	Secretary of State may authorise SIS or GCHQ to carry out acts abroad for which they may be liable in the UK including activities taking place in the UK but intended to relate to apparatus overseas.	Agent operations overseas	If Secretary of State is persuaded the action is: • necessary for proper discharge of an agency function • arrangements are in place that nothing will be done in reliance of the authorisation beyond what is necessary… • consequences of act reasonable as to what is sought to be achieved • satisfactory arrangements in place to ensure agency does not obtain or disclose information except insofar as it is necessary for the proper discharge of its functions	SIS and GCHQ	Authorisation through signature by Secretary of State (most commonly Foreign Secretary) Exercise of powers to grant authorisations overseen by the Intelligence Services Commissioner

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

Online www.tsoshop.co.uk

Mail, telephone, fax and email
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
Email: 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

ISBN 978-0-10-298033-2

9 780102 980332

HO_01054_G