

Report of the Intelligence Services Commissioner for 2013

The Rt Hon Sir Mark Waller

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 26 June 2014

Laid before the Scottish Parliament by
the Scottish Ministers June 2014

HC 304
SG/2014/103

Report of the Intelligence Services Commissioner for 2013

The Rt Hon Sir Mark Waller

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 26 June 2014

Laid before the Scottish Parliament by
the Scottish Ministers June 2014

HC 304
SG/2014/103



© Crown copyright 2014

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence v.2. To view this licence visit www.nationalarchives.gov.uk/doc/open-government-licence/version/2/ or email PSI@nationalarchives.gsi.gov.uk

Where third party material has been identified, permission from the respective copyright holder must be sought.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at the office of the Intelligence Services Commissioner via 2 Marsham Street, London, SW1P 4DF.

Print ISBN 9781474101172

Web ISBN 9781474101189

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

ID 2631951 06/14 40707 19585

Printed on paper containing 75% recycled fibre content minimum

CONTENTS

Letter to the Prime Minister	1
FOREWORD	2
1. FUNCTIONS OF THE INTELLIGENCE SERVICES COMMISSIONER	5
My Statutory and Extra-Statutory Functions	5
2. METHOD OF MY REVIEW	9
3. ASSESSMENT OF MY INSPECTION VISITS	13
The Agencies	14
The Warrantry Units	26
The Secretaries of State	30
4. CONFIDENTIAL ANNEX	32
5. MEDIA ALLEGATIONS	33
6. STATISTICS	35
7. SUMMARY OF REPORTABLE ERRORS	36
8. CONSOLIDATED GUIDANCE ON DETENTION AND INTERVIEWING OF DETAINEES BY INTELLIGENCE OFFICERS AND MILITARY PERSONNEL	39
9. INVESTIGATION OF POTENTIAL MISUSE OF DATA	48
10. CONCLUSION	49
APPENDIX	51
The Statutory Functions of the Intelligence Services	52
The Regulation of Investigatory Powers Act 2000 (RIPA)	53
Warrants and Authorisations under the Regulation of Investigatory Powers Act 2000 (RIPA)	54
Warrants and Authorisations under the Intelligence Services Act 1994 (ISA)	57
The European Convention on Human Rights (ECHR)	59
Application Process for Warrants	60
Necessity and Proportionality	61



The Rt Hon Sir Mark Waller
Intelligence Services Commissioner
2 Marsham Street
London
SW1P 4DF
Web: isc.intelligencecommissioners.com

The Rt. Hon. David Cameron MP
10 Downing Street
London
SW1A 2AA

26 June 2014

I enclose my third Annual Report covering the discharge of my functions as Intelligence Services Commissioner between 1 January 2013 and 31 December 2013.

It is for you to decide, after consultation with me, how much of the report should be excluded from publication on the grounds that any such publication would be contrary to the public interest, or prejudicial to national security, to the prevention or detection of serious crime, to the economic well-being of the United Kingdom, or to the continued discharge of the functions of those public authorities subject to my review.

I have continued to write my report in two parts, the Confidential Annex containing those matters which in my view should not be published. I hope that you find this convenient.

A handwritten signature in blue ink, appearing to read 'Mark Waller'. Below the signature are three short horizontal lines.

The Rt Hon Sir Mark Waller

INTELLIGENCE SERVICES COMMISSIONER



FOREWORD

My Appointment

I was appointed by the Prime Minister to the post of Intelligence Services Commissioner on 1 January 2011, under Section 59 of the Regulation of Investigatory Powers Act 2000 (RIPA). Under the Act, the Prime Minister appoints an Intelligence Services Commissioner who must hold, or have held, high judicial office within the meaning of the Constitutional Reform Act 2005. I held office as a Lord Justice of Appeal from 1996 until I retired in

May 2010. After my initial appointment, I accepted the Prime Minister's request to serve as Intelligence Services Commissioner for an additional three years from 1 January 2014.

My Independence, Legislative Responsibility and Statutory Powers

As Commissioner I am appointed by the Prime Minister to provide **independent** external oversight of the use of their intrusive powers by the UK intelligence services and parts of the MOD. I undertake this duty rigorously and entirely independently of government, Parliament and the intelligence agencies themselves.

It is important that the public have confidence in the oversight I provide and I firmly believe that the public should see, as much as is consistent with effective national security and law enforcement, how the intelligence services match up to expectations. The public should have confidence that where there is a shortcoming it is identified and measures taken to prevent it happening again. This report is intended to provide the information and assurances the public are entitled to expect. Of necessity sensitive detail is given in my confidential report to the Prime Minister.

It is also important to understand what my oversight entails. In essence, I act as a retrospective auditor of warrants and authorisations which have been issued. I examine a statistically significant sample of:

- warrants issued by the Secretaries of State authorising intrusive surveillance and interference with property; and
- other authorisations (such as for covert human intelligence sources) which certain designated officials can grant, in order to ensure they were issued properly.

I audit the paperwork and consider how the activity specified in the warrant or authorisation has been put into practice. Details of how I carry out my inspections can be found in Chapter 2 of this report.

I also undertake some extra statutory oversight which I or my predecessors agreed to take on. These extra-statutory roles could soon be placed on a statutory footing now that the Justice and Security Act 2013 has amended my legislative [responsibilities](#), to allow the Prime Minister to direct me to keep under review how the intelligence services carry out any aspect of their functions. So far, the Prime Minister has not published any such direction.

In Chapter 1 of this report, I detail my role, including which of the activities of the intelligence services I am responsible for overseeing.

The intelligence services and the MOD have wide-ranging powers to intrude upon the privacy of individuals. Along with the Interception of Communications Commissioner, I work to ensure these powers are used lawfully and appropriately, to protect the citizens and interests of the United Kingdom. My statutory [powers](#) allow me access to all documents and information I need to carry out my functions, no matter how sensitive or highly classified these may be. More details about my access to information can be found in Chapter 2 of this report. It is my duty, so far as I am able, to satisfy myself that the agencies have acted within the law and applied the test of necessity and proportionality appropriately. You can find more detail on necessity and proportionality in the Appendix to this report.

Other Oversight Mechanisms

The retrospective oversight that I, and the Interception of Communications Commissioner, provide is one link in a chain of internal and external oversight of the activities of the intelligence agencies. Parliament's Intelligence and Security Committee (ISC) provides further external oversight. The Justice and Security Act 2013, strengthened the ISC's ability to hold the intelligence services to account. I, along with the former President of the Investigatory Powers Tribunal, the Interception of Communications Commissioner and the former Interception of Communications Commissioner, met the ISC on 28 February 2013.

Privacy Safeguards

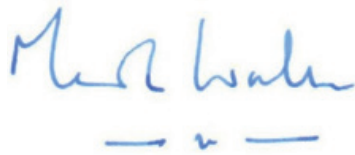
The Human Rights Act 1998 guarantees every person in the UK certain rights and fundamental freedoms. This includes Article 8, the right to respect for private and family life, which is a qualified right and subject to exception; in particular it may be subject to interference in the interest of national security. The full wording of Article 8 can be found in the Appendix to this report but I take as a priority that any intrusion into privacy must be fully justified by the intelligence to be obtained.

Changing World of Technology

There has been debate about whether RIPA, an Act published in 2000, can still apply when technology has advanced significantly since that time. Of the many techniques used which take advantage of technological capabilities now available, some could not have been envisioned when RIPA was drafted. But the Act was written to take account of technological change so as such the wording of the Act is technology neutral. RIPA was also written to reflect Human Rights legislation, which remains current, so it still applies. I am satisfied that the agencies apply the same authorisation process and the same test of necessity and proportionality with these more advanced technologies as they do with simpler, more traditional ones. I have provided a summary of RIPA in the Appendix to this report.

Effective Oversight?

When I first took up my role I was concerned that twice yearly inspections and a sample of warrants might not be sufficient. However, taking into account the method of my review as set out in Chapter 2, the robust and rigorous internal compliance tests and assurances, and the culture and ethos of the intelligence services, I am satisfied that it is sufficient.

A handwritten signature in blue ink, appearing to read 'Mark Waller', with a horizontal line underneath.

The Rt Hon Sir Mark Waller
The Intelligence Services Commissioner

1. FUNCTIONS OF THE INTELLIGENCE SERVICES COMMISSIONER

Statutory Functions

My 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 services to carry out their functions;
- to keep under review the exercise and performance of the powers and duties imposed on the intelligence services and MOD/Armed Forces personnel in relation to covert activities which are the subject of an internal authorisation procedure; and
- to keep under review the carrying out of any aspect of the functions of the Intelligence Services as directed by the Prime Minister.

These functions (which for convenience I summarise under figures 1 & 2 below) are set out in the Regulation of Investigatory Powers Act 2000 (RIPA) as amended by the Justice and Security Act 2013 (figure 4).

Figure 1: Statutory Functions of the Intelligence Services Commissioner

Function	Legislation	Issued by
Checking that warrants for entry on to, or interference with, property (or with wireless telegraphy) are issued in accordance with the law.	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.	The Secretary of State. In practice issued mainly by the Home Secretary or the Secretary of State for Northern Ireland.
Checking that authorisations for acts done outside the United Kingdom are issued in accordance with the law.	Keeping under review the exercise by the Secretary of State of his powers to give, renew and cancel authorisations under section 7 of ISA.	The Secretary of State. In practice issued by the Foreign Secretary.

<p>Overseeing the Secretary of State's powers and duties with regard to the grant of authorisations for:</p> <ul style="list-style-type: none"> • intrusive surveillance and • the investigation of electronic data protected by encryption. 	<p>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 services and (except in Northern Ireland) of MOD officials and members of the armed forces.</p>	<p>The Secretary of State. In practice issued mainly by the Home Secretary or the Secretary of State for Northern Ireland.</p>
<p>Overseeing the grant of authorisations for:</p> <ul style="list-style-type: none"> • directed surveillance • the conduct and use of covert human intelligence sources (CHIS) and • the investigation of electronic data protected by encryption. 	<p>Keeping under review the exercise and performance by members of the intelligence services, and in relation to officials of the MOD and members of the armed forces in places other than Northern Ireland, of their powers and duties under Parts II and III of RIPA.</p>	<p>A Designated Officer through Internal Authorisation.</p>

Further information about the warrants and authorisations that I oversee can be found in the Appendix to this report (page 51).

Figure 2: Statutory Functions Continued:

<p>Keeping under review the adequacy of the Part III safeguards of RIPA arrangements in relation to the members of the intelligence services, and in relation to officials of the MOD and members of the armed forces in places other than Northern Ireland.</p>
<p>Giving the Investigatory Powers Tribunal all such assistance (including my 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.</p>
<p>Making an annual report to the Prime Minister on the discharge of my functions, with such a report to be laid before Parliament.</p>
<p>Advising the Home Office on the propriety of extending the TPIM regime, part of the consultation process under section 21(3) of the Terrorism Prevention and Investigation Measures Act 2011.</p>

Keeping under review any other aspects of the functions of the intelligence services, or any part of HM Forces or the MOD engaging in intelligence activities, excepting interception of communications, when directed to do so by the Prime Minister.

Extra-Statutory Functions

My extra-statutory duties could be put on a statutory footing through a formal direction by the Prime Minister now that the Justice and Security Act 2013 has come into force. I have requested that such a direction is given, but until then, I will continue to provide oversight on an extra-statutory basis (figure 3).

Figure 3: Extra-Statutory Functions:

Overseeing 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 extra-statutory duties that the Prime Minister may from time to time ask me as Commissioner to take on, providing I am willing to undertake these.

Justice and Security Act 2013

The Justice and Security Act 2013 allows for additions to my statutory functions by a direction from the Prime Minister under section 5 of that Act. The Prime Minister has so far published no such direction. With effect from 25 June 2013, RIPA was amended to insert:

Figure 4: Justice and Security Act 2013:

59A Additional functions of the Intelligence Services Commissioner

- 1) So far as directed to do so by the Prime Minister and subject to subsection (2), the Intelligence Services Commissioner must keep under review the carrying out of any aspect of the functions of –
 - a) the intelligence services
 - b) a head of an intelligence service, or
 - c) any part of Her Majesty's forces, or the Ministry of Defence, so far as engaging in intelligence activity.
- 2) Subsection (1) does not apply in relation to anything which is required to be kept under review by the Interception of Communications Commissioner or under section 59.

- 3) The Prime Minister may give a direction under this section at the request of the Intelligence Services Commissioner or otherwise.
- 4) Directions under this section may, for example, include directions to the Intelligence Services Commissioner to keep under review the implementation or effectiveness of particular policies of the head of an intelligence service regarding the carrying out of any of the functions of the intelligence service.
- 5) The Prime Minister may publish, in a manner which the Prime Minister considers appropriate, any direction under this section (and any revocation of such a direction) except so far as it appears to the Prime Minister that such publication would be contrary to the public interest or prejudicial to –
 - a) national security,
 - b) the prevention or detection of serious crime,
 - c) the economic well-being of the United Kingdom, or
 - d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Intelligence Services Commissioner.
- 6) In this section "head", in relation to an intelligence service, means –
 - a) in relation to the Security Service, the Director-General,
 - b) in relation to the Secret Intelligence Service, the Chief, and
 - c) in relation to GCHQ, the Director.

2. METHOD OF MY REVIEW

Who I Met

During 2013 I undertook two formal oversight and extra-statutory inspections of each of the authorities that apply for and authorise warrants¹ (hereafter “the intelligence agencies”) that I oversee. They are:

The Security Service (MI5)
The Secret Intelligence Service (SIS)
Government Communications Headquarters (GCHQ)
The Ministry of Defence (MOD)

In addition, I inspected the departments processing warrants for each Secretary of State (hereafter “the warrantry units”) in:

The Home Office
The Foreign Office (FCO)
The Northern Ireland Office (NIO)

I also met the respective Secretary of State who signs off warrants at each department. They are:

The Home Secretary
The Foreign Secretary
The Defence Secretary
The Northern Ireland Secretary

¹ Please note that when I make reference to warrants this should be read, where the context demands, to include authorisations under ISA, as well as the internal authorisations under RIPA which are subject to my oversight.

What I Did

During the formal inspections of the areas I oversee, I check that warrants and authorisations have been issued lawfully. I do this over three stages in both the agencies and the warrant issuing departments.

1) The Selection Stage

- I select a number of warrants/authorisations for which I want to inspect the actual warrant/authorisation and the underlying paperwork from full lists of warrants/authorisations provided by the agencies. The lists include brief descriptions of what each is about. I select some warrants/authorisations for inspection on the basis of the information provided to me and I choose the remainder by random sampling.
- As a general rule, most of the warrants/authorisations I choose for inspection will be different in the agency and the government department which processes their applications. On some occasions, however, they will be the same, allowing me to audit the process from both sides.
- I check that the lists I receive from the agency applying for a warrant and the government department which processes their applications correspond. This too allows me to audit the process from both sides.

2) The Pre-Reading Stage

I scrutinise in depth, the warrants/authorisations I selected at 1) above. I fully review all paperwork justifying the issue of the same and identify any further information I need in advance of my inspection visit. In particular, I review whether the case of necessity and proportionality is properly made and whether any invasion of privacy has been justified.

I note points for discussion and questions to be raised during my inspection visit.

3) The Inspection Visit

I undertake my formal oversight inspection, raising points identified at 2) above with the individuals involved. I seek to satisfy myself that all warrants/authorisations are issued lawfully and the intelligence sought to be gathered is of sufficient importance to necessitate any intrusion, and that the least intrusive means of obtaining that intelligence have been used.

Under the Bonnet

I follow up my formal inspections with 'under the bonnet' visits to review how the warrants are put into operation. Because some submissions and warrants contain assurances about the means to be used to limit invasion of privacy, it is important to assess how these assurances are put into practice. These visits are designed to go beyond the paperwork and see the ways in which any assurances have been implemented. I question staff across a range of grades about how they will apply,

or have applied, the tests of necessity and proportionality in the planning stages and when carrying out the acts specified in any warrant or authorisation. I ask challenging questions of operational staff, to ensure they are fully aware of the conditions and understand why they have been applied.

Errors

An important element of my oversight role is examining errors that might have occurred, either during the warrant application and authorisation process, or during the subsequent exercise of these powers by the intelligence services. Under a system introduced by one of my predecessors the agencies are obliged to report to me any error which has resulted in any unauthorised activity where an authorisation should have been in place.

Errors can be divided into different categories:

- a) an administrative error where it is clear on the face of a document that a typing error has occurred, the correction is obvious, and a court would amend it under its 'slip rule';
- b) a situation where there has been an inadvertent failure to renew a warrant or obtain authorisation in time where, if things had been done properly, the renewal or authorisation would clearly have been granted; or
- c) a deliberate decision taken to obtain information without proper authorisation.

Category a)

During 2013 I discovered a number of errors in category a). Although they are not "reportable" errors I have asked that they now be drawn to my attention for the sake of good house-keeping. I have also taken the view that these errors should be corrected to reflect an obvious misspelling or similar. I give details in the errors section of the relevant agency because I believe it is in the public interest to do so.

Category b)

The errors shown in the statistics in Chapter 6 of this report, fall into category b). They are inadvertent but nonetheless important because they will, or may have, involved the invasion of privacy or interference with property when the appropriate authorisation was not in place. In all but rare cases, if any intelligence could have been retrieved it has been discarded. In one or two cases the intelligence was of such importance to the protection of the public that its further use was sanctioned.

Category c)

I have not found a deliberate decision to obtain information without proper authority. It would require dishonesty on the part of more than one person,

including almost inevitably a person of some seniority, for such a situation to take place at all or, crucially, without discovery. If such a deliberate act were to be committed those involved would be subject, not only to disciplinary proceedings, but also to criminal charges. Were I to discover such a deliberate decision I would report it to the Prime Minister immediately and notify the Crown Prosecution Service. I can be confident that deliberate activity as described above does not take place because:

- i) for unlawful warrants or authorisations to be issued it would require considerable ineptitude or conspiracy on a massive scale, involving:
 - the applicant (in setting out a case for necessity and proportionality)
 - the authorising officer (in approving it)
 - the lawyers (in signing off or turning a blind eye to illegal activity)
 - where ministers are involved the relevant government department warantry unit (in presenting the paperwork for signature)
 - the Secretary of State (in signing the warrant)
 - the civil servants (who support and advise the Secretary of State)
- ii) each agency has an internal legal compliance team. These teams work closely with their legal advisers, senior management and their respective minister (mostly through the relevant warantry unit) to help ensure that their organisation is operating lawfully and compliantly;
- iii) the ethos enshrined within the agencies is one of compliance and it is almost impossible for one person to act without others of some seniority knowing.

Access to Information

Every member of an intelligence service is obliged to disclose or provide to me any and all information I require to carry out my duties. There can be no limitations placed on my access to information.

In practice I have access to all information around the intelligence, resource and legal cases governing executive actions. I am provided with more information than is strictly necessary for the purposes of adding context. I can conclude with some confidence that, as far as the authorisations concerning the activities I oversee, officials and Secretaries of State comply with the necessary legislation, in so far as they are bound to do so.

3. ASSESSMENT OF MY INSPECTION VISITS

In the previous chapter I have set out the method of my review and who I inspect. In this section I explain how I undertook my oversight of each organisation and what was discussed, as far as I am able without prejudicing national security.

I have covered this in the following order:

- 1 The Agencies
- 2 The Warranting Units
- 3 The Secretaries of State

And I cover the following where appropriate:

- Dates
- Selection Stage
- Pre-reading Stage
- Inspection Stage
- Under the Bonnet
- Errors (including administrative errors)

I do not rely solely on these visits and also base my assessment on discussions throughout the year, which take place outside of my formal scrutiny visits.

The Agencies

Security Service (MI5)

In 2013 I inspected MI5 as follows:

	Round 1	Round 2
Selection	15 May	4 November
Pre-Reading days	4 July	27 – 28 November
Inspection days	11 July	5 December
Under the bonnet	6 December	

MI5 is tasked to protect the United Kingdom against threats to national security, such as terrorism. The legislation that exists to enable them to do this is set out in the Appendix to this report.

Selection Stage

At my request for each inspection the Legal Compliance Team at MI5 produced a complete list of their warrants and internal authorisations, including a summary of each case, covering all intrusive techniques which fall within my jurisdiction. Each list included every new warrant/authorisation issued since the last list was produced, and all extant or cancelled warrants. Officers from the legal compliance team talked me through their full list bringing to my attention cases they wanted to discuss with me during my inspection visit, in addition to those I selected for inspection.

Where appropriate they also provided me with any lists required to support my extra-statutory oversight.

As described in Chapter 2, I selected 112 directed surveillance, intrusive surveillance, covert human intelligence source (CHIS) authorisations, and/or property interference warrants, which I planned to scrutinise in detail, including whether the case of necessity and proportionality had been made properly.

Pre-Reading Stage

On the pre-reading days I examined the written submissions justifying the issue of the warrants and authorisations, some of which included hundreds of supporting documents. In all cases, I studied in detail the legal test of necessity and proportionality. My assistant scrutinised the same paperwork, focusing on whether the proper administrative procedures had been followed, that the dates were correct and drawing anything else of note to my attention.

The warrant submissions I examined had been reviewed by a senior officer and a lawyer at MI5 before being sent to the warantry unit at the Home Office National

Security Unit or the Northern Ireland Office, where they were considered again. In the Home Office, the warrantry unit processed the applications, and may have asked further questions before they were satisfied. The warrants were then drafted and a synopsis of the submission prepared for the Home Secretary's final consideration and decision. The Home Secretary was satisfied that the warrant was both necessary and proportionate before she signed the warrants. If she had refused, the activity would not take place.

I reviewed all the stages detailed above during my pre-reading and then examined the synopses on my visits to the Home Office. The Northern Ireland Office follows a similar procedure and I examined the warrants in the same way.

Where needed I requested additional documentation, and I raised factual issues with the legal compliance team which were either be dealt with there and then, or answered on my inspection visit.

Inspection Stage

At the beginning of each formal oversight inspection of MI5 the Deputy Director-General (DDG) briefed me on the developments and current threat assessment to provide additional background to the agency's activity. An MI5 lawyer and officers from their legal compliance team were also present.

I then met case officers and senior managers to scrutinise the cases I had selected for further examination. During these meetings the case officers explained to me the operations for which the warrants/authorisations had been issued and I questioned the case officers in detail about any issues which needed clarification or testing and about how they put the same into practice, why they needed to, and what the outcome was. This allowed me to get a clear understanding of the necessity of the activity, and what was done to ensure that intrusion into privacy was limited.

During 2013 we focused on:

- How the legislation applied to modern techniques, and I was satisfied that MI5 applied exactly the same authorisation process and test for necessity and proportionality, and obtained prior authority to undertake the activity in the same way as if, for example, they planned to plant a listening device.
- The impact of the media allegations on MI5's work.
- Further details around the errors reported to me, including efforts to ensure that similar mistakes did not happen again and, in particular, what invasion of privacy occurred.

From the range of officers I met and questioned during my inspections I was left with the clear impression that my external oversight was welcome and that compliance with the legislation is an integral part of the organisation.

Under the Bonnet

During this stage, among other things, I observed a surveillance team being briefed prior to mobilisation for a live operation. I saw how officers sought assurance that the operation was lawful and clarified the limits of their remit and was impressed with how the pre-mobilisation briefings were designed to ensure compliance with the legislation.

Operational Examples

Part of my under the bonnet work involves seeing how warrants are put into practice. In the past I have included examples of operational successes to illustrate this in my annual report. However, given that I cannot give specific examples in equal detail across the organisations I inspect, I have taken the decision to drop these sections from my report this year.

Errors Reported to Me

In 2013, the DDG reported to me 19 errors made by MI5. I discovered one administrative error in an MI5 warrant, although this error originated in the Home Office warranting unit.

Of the 19 errors:

- all were caused by human error and all resulted in intrusion into privacy to some degree;
- none were deliberately caused by those involved;
- 11 occurred because the correct authorisation was not applied for or renewed;
- 6 were a result of procedural errors;
- 1 arose from data being incorrectly inputted into electronic systems;
- 1 was because an authorisation had been prematurely cancelled before extraction of equipment could be completed.

The reports notifying me of the errors contained details of the operation, how the error occurred, the intrusion into privacy that resulted, and what steps had been taken to prevent a reoccurrence. In most instances I was satisfied with the answers but still discussed the errors during my inspection and made clear that any error, but especially those which led to intrusion into privacy, were not acceptable.

On two occasions when a lapse had been missed for a long period of time I requested further explanation and made clear that this was unacceptable. The DDG explained the circumstances to me during my inspection visit and assured me that the MI5 officers responsible had been informed that the lapses were unacceptable.

Administrative Error

During my pre-reading stage I spotted an anomaly in the date on a warrant (the warrant said that it was issued on 25/3/12 when it should have said 25/3/13). This warrant was drafted by the Home Office and the mistake was therefore theirs. It was evident that this was an administrative slip and that no unauthorised intrusion into privacy had occurred, but I reiterated that any error was unacceptable. To correct this slip I asked that the Home Secretary amend the date on the original warrant to 2013 and then sign and date when this took place.

I also raised this with the DDG during my formal inspection at MI5. Although this slip was made by the Home Office it is the responsibility of the officer who might be planting a device or undertaking surveillance to check that they have a proper authorisation before undertaking any intrusive activity. I told the DDG that although this type of error is not a "reportable error" under the system set up by my predecessors and continued by me, I would like to be notified of such slips, and I would reflect them in my report.

Secret Intelligence Service (SIS)

In 2013 I inspected SIS as follows:

	Round 1	Round 2
Selection	15 April	4 November
Pre-Reading days	30 May	25 November
Inspection Days	7 June, 18 June	29 November, 2 December
Station Visits	7 – 8 May 2013 (Western Asia)	10 – 13 November (Europe)
Under the bonnet	2, 11 and 12 December 2013	

SIS is tasked with protecting the United Kingdom (UK) and UK interests. It operates overseas, dealing with threats and gathering intelligence. The legislation which enables SIS to do this is set out in the Appendix to this report.

Selection Stage

For each inspection I required SIS to provide me with a complete list of their warrants and authorisations, including a summary of each case, covering all activities which fall within my jurisdiction. This list included all new warrants issued since the last list was produced and all extant or cancelled warrants. An officer from their legal compliance team talked me through their full list bringing to my attention cases they wanted to discuss with me during my inspection visit, in addition to those I selected for inspection.

As described in Chapter 2, I selected 46 RIPA and ISA warrants and authorisations to scrutinise in detail, including the necessity and proportionality in the underlying paperwork of each case.

Where appropriate, their legal compliance team also provided me with any lists to support my extra-statutory oversight.

Pre-Reading Stage

During the pre-reading stage I scrutinised the written submissions justifying the issue of the warrants and authorisations, including the warrants and all supporting documents. In all cases, I studied in detail the legal test of necessity and proportionality. My assistant again scrutinised the paperwork, focusing on whether the proper administrative procedures had been followed and drawing anything else of note to my attention.

All the warrants and ISA section 7 authorisation submissions I examined had been drafted by SIS and reviewed by a lawyer before they were submitted to the Foreign Office for their warrantry unit to consider. The Foreign Office reviewed the cases again and may have asked further questions of SIS before they were satisfied. The warrantry unit added their own comments and prepared a synopsis of each case for the Foreign Secretary's final consideration and decision. If the Foreign Secretary was satisfied that the activity was both necessary and proportionate he signed the warrant (or section 7 authorisation). If he refused, the activity did not take place.

I requested any further documentation I needed, and I raised factual issues which were either dealt with there and then, or answered on my formal inspection visit.

Inspection Stage

My formal oversight visits of SIS began with a briefing of operations taking place across the world under the warrants and authorisations I oversee. The SIS legal compliance team and an SIS lawyer were present.

I then met desk officers to scrutinise the cases I had selected for further examination. During these meetings the desk officers briefed me on the background to their particular operation and I questioned and challenged them on the operational activity to ensure I got behind the paperwork and understood how the legislation was translated into practice. I required clarification if something needed further testing. Again this allowed me a better understanding of the necessity of the activity and how intrusion into privacy is limited.

During 2013 we focused on:

- how the written assurances contained in submissions which set out how SIS planned to limit intrusion into privacy are put into practice;

- the errors reported to me, and what had been done to mitigate against similar errors happening again;
- we also discussed, as I have elsewhere, the importance for SIS to evidence how any invasion into privacy is justified by the intelligence to be gained.

I saw a wide range of SIS officers and spent more time than before at SIS getting “beneath the bonnet” of their work. I am confident that the staff at SIS work to comply with the legislation and have no desire to operate unlawfully. Legal compliance is an integral part of the culture of the organisation.

Under the Bonnet

As part of my under the bonnet work, on 2 December I was shown, in detail, how SIS systems identify and prevent unauthorised or inappropriate intrusion into privacy.

I also participated in training courses for SIS staff, to ensure those receiving the training were properly aware of their legal obligations in the areas under my jurisdiction:

- On 11 December I gave a presentation to staff, about their responsibilities under ISA, my priorities, and what I am looking out for in my inspection visits. I emphasised the importance of using intrusive techniques only as a last resort, and ensuring the intrusion into privacy is justified by the intelligence to be gained.
- On 12 December I observed how new recruits to SIS are trained and participated in the training as part of an exercise where trainees had the opportunity to present a case about an operation to me as the Intelligence Services Commissioner.

Station Visits

An important element of my oversight of SIS is to scrutinise the overseas stations in which they operate and undertake the activity authorised by the Foreign Secretary through an ISA section 7 authorisations. On these visits I have two main priorities:

- to check that legal requirements set out in the authorisations are complied with; and
- to see how staff operate in-country, and the ethics they apply.

During my station visits, I was briefed on current operations so that I could get a full and detailed picture of the activity authorised by the Foreign Secretary. I questioned the stations about activity that had been authorised, and what might be required as an operation progressed. We covered the necessity of an operation and I probed and challenged in more detail the reasonableness and proportionality, with a particular focus on privacy. Because I look at ongoing operational matters

and discuss these with the officers in the field undertaking the activity, I am not able to give further detail about the issues covered.

However, for each operation there was a controlling officer at SIS Head Office in London who was in constant communication with the station about that operation. SIS Head Office in London set out in writing the necessity and reasonableness or proportionality of the operation, but I test how this works in country in stations I visit. Staff overseas may have to operate alone but not without authorisation of their manager in country who will, in relation to anything of substance, communicate with Head Office before acting. This ensures unauthorised activity does not take place.

Station teams are often small and they appear to value the opportunity to discuss what they are doing and to explain how they seek to operate in accordance with UK law and UK standards. The same ethos of honesty and integrity run through the service whether at Head Office or overseas. Having interviewed officers posted to these stations I was satisfied that they had no desire to act otherwise than in accordance with UK law and standards.

Errors Reported to Me

In 2013 I was made aware of 10 “reportable” errors by SIS. Three of these errors were reported to me late, having actually occurred in 2012. I also discovered three administrative errors during my inspections and a fourth was brought to my attention.

Of the 10 reportable errors:

- all were caused by human error and all resulted in intrusions into privacy to some degree;
- none of these errors were deliberately caused by those involved;
- 3 occurred because the correct authorisation was not applied for or renewed;
- 6 were as a result of procedural errors; and
- 1 arose from data being incorrectly inputted into electronic systems.

In most cases it was clear from the errors reported to me: what the error was; when it occurred; what intrusion into privacy took place and; what steps had been taken to avoid a reoccurrence. But in a few cases I had to request follow up information and to remind SIS of the importance of and requirement to report errors to me promptly.

During a formal inspection visit I re-emphasised that individual officers in SIS must check, and be able to check, that an authorisation is in place before they engage in any intrusive activity. In one case a manager had not been alerted and so did not

electronically sign the form until the activity had already taken place. To prevent this happening again, the applying officer now speaks to the authorising officer and checks that the form is authorised. I recommended that this safeguard be put in place across the organisation.

Administrative Errors

During my pre-reading I discovered an authorisation for the use and conduct of a CHIS which had expired on 11 October 2012, but the renewal had not been signed until 12 November 2012. No activity with the CHIS took place between 11 October and 12 November. However, SIS should have made an application for a new authorisation instead of completing a “renewal” application.

I was also informed of an error in SIS internal procedure where the authorising officer for an internal RIPA authorisation had failed to complete the correct section of an electronic form. This form is automatically locked down after it is approved and cannot be amended subsequently. However, it is clear from electronic tracing that the authorising officer had taken the necessary corrective action.

During my inspection I also discovered that two internal authorisations had been approved late, but no action had taken place before this was realised and corrected.

Government Communications Headquarters (GCHQ)

GCHQ produces intelligence from communications and takes the lead on cyber issues, including cyber defence, to protect the UK and UK interests overseas. I have set out their statutory purpose in full in the Appendix to this report.

In 2013 my oversight of GCHQ in 2013 took place as follows:

	Round 1	Round 2
Selection	29 April	7 November
Pre-Reading and Inspection Days	4 – 5 June	10 – 11 December
Under the bonnet	10 July	

I also visited on 13 June 2013 following media allegations about the legality of some of GCHQ’s work, and asked for a further update prior to a pre-arranged under the bonnet visit on 10 July 2013.

Selection Stage

I required GCHQ to provide me with a complete list of all warrants and internal authorisations, including a summary of each case, covering all intrusive techniques which fall within my jurisdiction. This included all new warrants issued since the last list was produced and all extant or cancelled warrants. Where appropriate their

legal compliance team also provided me with any lists required to support my extra-statutory oversight.

As described in Chapter 2 I selected 33 RIPA and ISA warrants, which I planned to scrutinise in detail, including whether the case of necessity and proportionality had been made properly.

Pre-Reading Stage

On my pre-reading days in GCHQ prior to starting my formal oversight, I examined the written submissions justifying the issue of warrants and authorisations. In each case I scrutinised in detail the legal test of necessity and proportionality. My assistant scrutinised the same paperwork, focusing on whether the proper administrative procedures had been followed, that the dates were correct and drawing anything else of note to my attention.

GCHQ's activity can be highly technical but their submissions and supporting documents are set out clearly. An officer from the compliance team was available to me at all times during my pre-read to clarify any technical points or acronyms.

The warrant issuing process at GCHQ is the same as that in SIS. All the warrants and ISA section 7 authorisation submissions I examined had been drafted by GCHQ and reviewed by a lawyer before they were submitted to the Foreign Office for their warrantry unit to consider. The Foreign Office reviewed the cases again and may have asked further questions of GCHQ before they were satisfied. The warrantry unit added their own comments and prepared a synopsis of each case for the Foreign Secretary's final consideration and decision. The Foreign Secretary was satisfied in all cases that the activity was both necessary and proportionate before he signed the warrant (or section 7 authorisation).

Inspection Stage

At the beginning of my formal inspections at GCHQ the Director-General for Intelligence and Strategy (DGIS) briefed me on operational activities since my last visit, and current operational priorities to provide background for the individual warrants and authorisations that I inspected. At least one GCHQ lawyer was present for the whole of my inspection, along with a number of other officers from their legal compliance and policy team.

Separate from my formal inspections, I visited GCHQ to discuss allegations made in the media that GCHQ had acted unlawfully. The detail of those visits and my assessment of GCHQ activity in areas of my jurisdiction subject to the allegations are set out in Chapter 5 of this report. However, on inspection day DGIS also briefed me on the operational impact on the effectiveness of GCHQ following the media allegations. GCHQ staff were forthcoming in response to my questions and I was told that there had been an adverse impact. As Sir Iain Lobban confirmed to me and stated in his evidence before the Intelligence and Security Committee

on 7 November 2013, GCHQ do not conduct activities outside the UK legal framework. I have found no evidence to the contrary.

At the inspections I discussed the warrants and authorisations I had selected for detailed scrutiny with the individuals involved, both those who drafted the submissions and those who carried out the activities. As on other inspections I questioned and challenged them with particular focus on the legal test of necessity and proportionality. We also discussed errors, and how the same errors could be prevented in future. From my work it is clear to me that GCHQ apply the same human rights considerations and the same privacy considerations, checks and balances to the virtual world as they do to the real world. From my scrutiny of GCHQ authorisations, inspection visits and my under the bonnet work, it is my view that GCHQ staff continue to conduct themselves with the highest level of integrity and legal compliance.

Under the Bonnet

In July 2013, as part of my under the bonnet work I observed a mandatory training course which operational managers at GCHQ in particular roles are required to attend. There was strong emphasis on ethics during the training and an “ethical principles” section which I set out here:

- Necessity: there must be a strong business case, framed in terms of HMG policies and desired outcomes, for our activity.
- Proportionality: the impact and/or intrusion of our activity must be justifiable in relation to the threat posed and the benefit to be gained.
- Objectivity: our activity is not subject to inappropriate influence or bias.
- Professionalism: we understand the responsibility invested in us by virtue of our unique role, and act accordingly.

Errors Reported to Me

In 2013 I was made aware of 3 reportable errors by GCHQ.

All of the errors reported to me were caused by human error and all resulted in intrusions into privacy to some degree. However, none of these errors were deliberately caused by those involved.

I can report that:

- 2 out of 3 errors were procedural errors.
- 1 arose from data being incorrectly inputted into electronic systems.

This last was a situation in which GCHQ was supplied with the wrong intelligence or data by a third party, which informed the subsequent conduct of an operation. In my view this constituted a “reportable” error because there was the potential for unnecessary intrusion into privacy to have taken place, even though it was not an error made by GCHQ. The intrusion was not deliberate or intentional criminal activity, and did not require referral to the Crown Prosecution Service.

Administrative Error

While at GCHQ I reviewed a clerical slip that I had earlier picked up at the FCO and which is set out in that section of my report. GCHQ hold the original warrant, which displayed a clearly incorrect date. I noted that the Foreign Secretary had amended the original warrant.

I made it clear that GCHQ must check that an authorisation is in place before undertaking intrusive activity. GCHQ have a check list that they follow when producing warrants for the Foreign Secretary to sign, and this has been updated since I discovered this error. I reviewed this checklist and recommended that there should be a further check when the warrant was returned to GCHQ from the FCO.

Ministry of Defence (MOD)

In 2013 my oversight of the MOD was as follows:

	Round 1	Round 2
Selection	8 April	8 November
Pre-Reading and Inspection	18 April	15 November, 3 December

The Ministry of Defence protects the security, independence and interests of the UK at home and overseas.

In order to do this, the Armed Forces are able to use intrusive techniques and this is coordinated by the MOD under the guidance of the Defence Secretary. It is not accepted by HMG that RIPA Part II applies to all relevant activities outside the United Kingdom, but the MOD seeks to apply RIPA to surveillance and CHIS operations outside the UK as a matter of policy. So for directed surveillance, intrusive surveillance and agent running, MOD authorisations are issued only on the basis that necessity is established and any intrusion into privacy is justified.

Selection Stage

I required the MOD to provide me with a complete list of authorisations in relation to the intrusive techniques falling within my jurisdiction. This included any new authorisations since the last list was produced and all extant or cancelled authorisations. Lists of authorisations were provided to my office for my selection in good time.

Where appropriate the MOD also provided me with any lists to support my extra-statutory oversight.

As described in Chapter 2, I selected 21 authorisations I planned to scrutinise in detail, including whether the case of necessity and proportionality had been made properly.

Pre-Reading and Inspection Stage

My first inspection round in April took place in one location but by the latter part of the year the MOD was storing paperwork in two separate locations so I carried out two separate inspection visits.

During my formal oversight inspections I pre-read written submissions justifying the authorisation, with particular focus on whether the necessity and proportionality case had been made. My assistant scrutinised the same paperwork, focusing on whether the proper administrative procedures had been followed, that the dates were correct and drawing anything else of note to my attention.

The paperwork I scrutinised was first applied for and authorised in theatre overseas. Staff overseas had access to both legal and political advisers and the paperwork was then made available to MOD head office. The Defence Secretary was regularly briefed on such operations.

I discussed the particular military operations with the relevant UK based personnel who obtained further documentation and information from theatre when I required it.

Errors Reported to Me

It is not accepted by HMG that RIPA Part II applies to all relevant activity outside the UK, but one formal breach of the RIPA process occurred in relation to the areas I oversee. The failure was a human, procedural error and was not deliberate. Corrective action was taken immediately.

Administrative Errors

In 2013 I became aware of 2 administrative errors relating to the MOD authorisations I scrutinise. First, during an inspection visit I noticed that a CHIS authorisation² had a different written justification to the original urgent oral authorisation. I also noticed an error where the end date for surveillance had originally been set more than three months after commencement, although the MOD had identified and corrected this error well before the three month point. In both cases the MOD issued corrective instructions immediately. I was satisfied these were strictly administrative errors and therefore no unauthorised invasion of privacy had taken place.

² The authorising officer must give authorisations in writing, except in urgent cases, where they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant (or the person with whom the authorising officer spoke) as a priority.

All of the errors reported to me by the MOD were caused by human error and although some resulted in unauthorised intrusions into privacy to some degree this was a breach of MOD policy and not of RIPA. None of these errors were deliberately caused by those involved.

It is clear to me that those responsible for authorising surveillance, whether directed or intrusive, only do so if they are satisfied necessity has been established and any intrusion into privacy has been justified. I am also satisfied that procedures are being put in place to prevent the administrative errors I found.

The Warrantry Units

Home Office

In 2013 my inspection of the Home Office was carried out as follows:

	Round 1	Round 2
Selection	14 May	4 December
Pre-Reading and Inspection	22 May	16 December

The Home Office National Security Unit processes applications from MI5 for warrants to allow use of property interference or intrusive surveillance. The team first satisfy themselves that the applications are necessary and proportionate before drafting and presenting warrants to the Home Secretary for her consideration. If the Home Secretary is satisfied that a warrant is both necessary and proportionate, she will sign it, if she is not satisfied, then the activity does not take place.

Selection Stage

I required the Home Office to provide me with a list of every new warrant issued since the last list was produced, and all extant or cancelled warrants, as well as any warrants which may have been refused by the Home Secretary. The list set out the type of operation with notes on each case. The list of warrants issued by the Home Office and the list I received from MI5 corresponded. I was satisfied that both had provided a full and complete list.

As described in Chapter 2, I selected 21 intrusive surveillance and/or property interference warrants, which I planned to scrutinise in detail, including whether the case of necessity and proportionality had been made properly. As a general rule, most of those I chose will have been different from those I inspected at MI5.

Inspection Stage

During my inspections I studied: the paperwork which had been submitted to the Home Office by MI5 for presentation to the Home Secretary; any additional background documents on each operation; and the synopsis of the submission prepared by the Home Office for the Home Secretary's consideration.

While the Home Secretary personally considers a large number of warrant requests, the nature of the synopses prepared by the Home Office reassured me that she could give each application appropriate consideration and make a properly informed decision.

I raised a number of points with the Home Office and discussed these with the senior official responsible for the team. They also raised a number of points that they wished to discuss with me. I was fully satisfied with explanations I received and the willingness to take forward my recommendations.

Administrative Error

I raised the slip I had discovered at MI5 and told them to report it to me formally. The Home Office followed up in writing, explaining that the typed date on the warrant referred to the incorrect year, and apologising for not detecting this at the time. I accepted that this did not make the warrant unlawful, because it was plain from the document itself that a slip had been made. However, I requested that the Home Secretary be asked to correct and initial the correction.

Foreign and Commonwealth Office (FCO)

I undertook inspection visits to the FCO on:

SIS	Round 1	Round 2
Selection	15 April	4 November
Pre-Reading and Inspection	25 April	12 December

GCHQ	Round 1	Round 2
Selection	12 April	21 October
Pre-Reading and Inspection	25 April	7 November

I carried out separate inspections of SIS and GCHQ paperwork with the FCO because they are stored in separate locations.

The FCO processes applications from SIS and GCHQ for warrants and authorisations to allow use of intrusive surveillance and activities under ISA

sections 5 and 7. The team first satisfy themselves that the applications are necessary and proportionate and may have had further questions for either agency, before drafting and presenting warrants to the Foreign Secretary for his consideration. If the Foreign Secretary is satisfied that the warrant is both necessary and proportionate, he will sign the warrant but if he refuses, the activity does not take place.

Selection Stage

I required the FCO to provide me with lists of every new warrant and ISA section 7 authorisations issued since the last lists were produced, and all extant or cancelled warrants, as well as any warrants which may have been refused by the Foreign Secretary. The lists of warrants issued by the FCO and the lists I received from SIS and GCHQ corresponded. I was satisfied that both agencies and the FCO had provided full and complete lists.

As described in Chapter 2, I selected 55 cases, which I planned to scrutinise in detail, including whether the case of necessity and proportionality had been made properly. As a general rule, most of those I chose will have been different from those I inspected at SIS and GCHQ.

Inspection Stage

During my inspections I scrutinised: the paperwork which had been submitted to the FCO by SIS and GCHQ for presentation to the Foreign Secretary; the warrants (which had been pre-prepared by SIS or GCHQ) any additional background documents on each case including FCO advice on the political and legal risk for the Foreign Secretary and whether the necessity and proportionality cases have been properly made.

During my inspections I met the Head of Intelligence Policy Department, Director of National Security and Director-General Defence and Intelligence who advise the Foreign Secretary. I raised with senior officials the importance of proper justification and, in particular, that necessity justifies intrusion into privacy. They are fully aware of those factors.

Administrative Error

At the FCO I discovered an administrative error. The warrant was drafted by GCHQ and the mistake was therefore theirs. A renewal warrant signed by the Foreign Secretary stated that it was valid for six months but then gave an end date of 25 May 2013, only a few weeks away. It was evident that this was the expiry date for the previous renewal and the wording of the warrant was clear and unqualified in stating that the renewal remained valid for six months. It was evident that a slip had been made on the face of the document. I required the Foreign Secretary to correct the date on the original warrant to 25 November 2013 and then sign and date when this took place.

Although this error was made by GCHQ I instructed the FCO that it is their responsibility to check that the warrant is accurate before placing it before the Foreign Secretary for his consideration.

Northern Ireland Office (NIO)

My oversight of NIO occurred as follows:

	Round 1	Round 2
Selection	10 April	21 November
Pre-Reading and Inspection	16 May	19 December

The Northern Ireland Office processes applications from MI5 for warrants to allow use of property interference or intrusive surveillance in Northern Ireland. The NIO first satisfy themselves that the applications are necessary and proportionate, and may have further questions for the agency, before drafting and presenting warrants to the Northern Ireland Secretary for her consideration. If the Northern Ireland Secretary is satisfied that a warrant is both necessary and proportionate, she will sign it, if she is not, then the activity does not take place.

Selection Stage

For each inspection I required the NIO to provide me with a list of every new warrant issued since the last list was produced, and all extant or cancelled warrants, as well as any warrants which may have been refused by the Northern Ireland Secretary. The list set out the type of operation with notes on each case. The list of warrants issued by the NIO and the list I received from MI5 corresponded. I was satisfied that both had provided a full and complete list.

As described in Chapter 2, I selected 24 intrusive surveillance and/or property interference warrants, which I planned to scrutinise in detail, including whether the case of necessity and proportionality had been made properly. As a general rule, most of those I chose will have been different from those I inspected at MI5. The NIO also brought to my attention any cases where they had concerns or where there were special restrictions which I scrutinised in addition to those I had already selected for inspection. I approved of this practice and recommended that it is followed elsewhere.

Inspection Stage

During my inspections I scrutinised:

- the paperwork which had been submitted to the NIO by MI5 for presentation to the Northern Ireland Secretary;
- the warrants prepared by the NIO; any additional background documents on each operation; and

- the advice on the political or legal risk given to the Northern Ireland Secretary by her senior officials.

During my inspection visits in Belfast senior officials briefed me on the current political and terrorism situation in Northern Ireland to provide more context to the activity I oversee. They were available to me throughout my inspection and answered all questions I had.

During my reading it became apparent that an administrative error concerning an incorrect grid reference in a warrant had been made and picked up by the NIO. The NIO legal advice was that the warrant was still valid and I agreed, because the grid reference specified was not a valid reference for any location, and all of the other information made clear which property was intended. I advised that the Secretary of State should normally amend, initial and date the original warrant where a slip had been made but in this case, the warrant was too old. I recommended the NIO cancel the old warrant and obtain a new one, but record that the original warrant was valid and that I, as Commissioner, agreed with this assessment.

The Secretaries of State

As part of my formal oversight I met:

The Rt Hon. Theresa May, Home Secretary, on 26 November

The Rt Hon. William Hague, Foreign Secretary, on 18 December

The Rt Hon. Phillip Hammond, Defence Secretary, on 18 December

The Rt Hon. Theresa Villiers, Northern Ireland Secretary, on 6 November

The Secretaries of State above have the power to sign warrants authorising activity by the relevant agencies under the applicable legislation, including intrusive surveillance and property interference. They take responsibility for ensuring that the warrants they sign are necessary and proportionate and the Home and Foreign Secretaries are responsible in Parliament for the three intelligence services.

During my meetings with the Home Secretary, Foreign Secretary and Northern Ireland Secretary, I wanted to satisfy myself that they made well informed assessments and decisions about the warrants they were called upon to approve. I questioned them in some detail about this and was fully satisfied that the each Secretary of State had taken the time to study the submissions, request additional information and updates from officials where needed, taken into consideration the potential infringement on the private lives of citizens and made their own informed decision.

Separate issues

During my meeting with the Foreign Secretary I raised the administrative error contained in a warrant signed by him, of which he was aware, and had been asked to correct and initial the original document.

I also spoke to the Foreign Secretary about ISA section 7 authorisations. (Detail of the legislative framework, strict criteria and authorisation procedure can be found in the Appendix to this report.) I raised with him the parameters of one particular authorisation. The Foreign Secretary sought urgent advice about it, and subsequently provided me with further information which clarified the limitations of the activity specified and the assurances that had been put in place. Having now reviewed a number of authorisations at GCHQ and SIS, and discussed this with the Foreign Secretary, I am satisfied that he has properly exercised his statutory powers under section 7.

During my meeting with the Northern Ireland Secretary we discussed one warrant she had refused to issue and which I followed up during my inspection at the Northern Ireland Office. The Northern Ireland Secretary has the power to sign warrants authorising MI5 to undertake intrusive surveillance and property interference in Northern Ireland, and she takes responsibility for ensuring that the warrant is necessary and proportionate.

The Defence Secretary has responsibility for the Ministry of Defence. During my meeting with him we had an in depth discussion about my role in examining authorisations and the challenge faced by those involved in military operations.

4. CONFIDENTIAL ANNEX

As I said in the forward to this report, I am committed to providing as much information and assurance as I can in my open report so that the public can have confidence in my oversight of the intelligence services. I must do this within the constraints of my Office and without prejudice to effective national security and law enforcement. There are, therefore, sensitive points I cannot publish in my open report, because it would not be in the public interest to do so.

Under section 60(5) of RIPA, the Prime Minister, in consultation with me, can decide that certain matters should not be published in my open report. I have prepared a confidential annex covering the issues I suggest should not be disclosed. Nothing contained in the confidential annex detracts from or changes in any way what I have said in my open report.

5. MEDIA ALLEGATIONS

Throughout 2013 there were allegations in the media that GCHQ had been conducting activities unlawfully. The first allegation suggested that GCHQ had circumvented UK law. When I read about it, I was extremely concerned, as many other people were. However, as the Intelligence Services Commissioner, I was able to visit GCHQ immediately and confront them about the allegations. I first did so on 13 June 2013, and again on 10 July during a pre-arranged visit. In my annual report for 2012 I said:

This report is being finalised at a time of considerable media comment about the legality of GCHQ's activities. The Intelligence and Security Committee are, quite properly, investigating and it is for them to comment further if they wish to do so.

In so far as matters related to my areas of oversight, which is the only area where it is appropriate for me to comment, I have discussed matters further with senior officials within GCHQ and I am satisfied that they are not circumventing the legal framework under which they operate.

During these two visits, I was first briefed in depth about the agency's activities and the allegations. I then met and questioned a number of senior GCHQ officials, including a GCHQ lawyer. My questions were probing and challenging. I also questioned Sir Iain Lobban, the Director of GCHQ. The results of this questioning and briefing allowed me to conclude that GCHQ were not circumventing the law in the UK. Everyone I spoke to was forthcoming and answered all my questions fully and willingly.

Since my second visit on 10 July, GCHQ have been in regular contact with me on further allegations made in the media.

Because these allegations primarily relate to the interception of communications they fall within the remit of the Interception of Communications Commissioner, Sir Anthony May. Sir Anthony conducted an investigation and reported on it to the Prime Minister in his Annual Report for 2013, confirming that GCHQ had not acted unlawfully so far as matters within his remit were concerned.

The Intelligence and Security Committee, having taken evidence from GCHQ, concluded that the allegations they investigated on circumvention of UK law were unfounded, and that GCHQ's activities conformed to the requirements contained

in the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000. They announced in October 2013:

Although we have concluded that GCHQ has not circumvented or attempted to circumvent UK law, it is proper to consider further whether the statutory framework governing access to private communications remains adequate.

My views have not changed from those I set out in my 2012 Report but a further allegation comes within my jurisdiction and I therefore consider it. The allegation is that GCHQ does not have the statutory power to conduct activities under Part II of RIPA, specifically Covert Human Intelligence Source operations (CHIS).

GCHQ's statutory 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; and

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.

Therefore, if GCHQ were to conduct activity which falls under Part II of RIPA (such as CHIS) it would be lawful if it were conducted through electronic means. They could not, for example, physically conduct surveillance but they could monitor activity online, which constitutes surveillance. They would need, of course, proper authorisation. I can therefore repeat that I am satisfied that GCHQ are not circumventing the legal framework under which they operate.

I have discussed with all three intelligence services the impact of the revelations made by Edward Snowden. The heads of each agency clearly set out during the public evidence session before the Intelligence and Security Committee (ISC) on 7 November 2013 how alerting targets and adversaries to UK capabilities means that it becomes more difficult to acquire the intelligence that this country needs. The agencies provided me with clear evidence to substantiate this. In the interests of national security, I am not in a position to give further detail in my open report.

6. STATISTICS

In previous reports I have published the total number of RIPA and ISA authorisations I oversee. Doing so is helpful to public confidence and gives an idea of the number of authorisations that I could potentially sample during my inspection visits. However, it is my view that disclosing details beyond this could be detrimental to national security, and for this reason a further breakdown is provided only in my confidential annex.

The total number of warrants and authorisations approved across the intelligence services and the MOD in 2013 was **1887**. Provided with details of all warrants, I scrutinised **318** warrants extant and paperwork during 2013, **16.8%** of the total.

Although this total figure is for the number of approved warrants and authorisations in 2013, the list of warrants and authorisations presented to me to make my selection from may have included some issued in late 2012. Warrants and authorisations have a finite duration, expiring after 3, 6 or 12 months. As a result, the 1887 warrants and authorisations approved in 2013 should not be interpreted as adding to a cumulative total of warrants and authorisations over preceding years.

The total number of new warrants and authorisations for 2013 was a reduction from the total approved in 2012, which was 2838. However, the 2012 total was not a true representation: because of a migration onto a new electronic system, a number of authorisations were cancelled and then re-authorised. In 2012 I scrutinised 242 warrants and authorisations, or 8.53% of the total.

7. SUMMARY OF REPORTABLE ERRORS

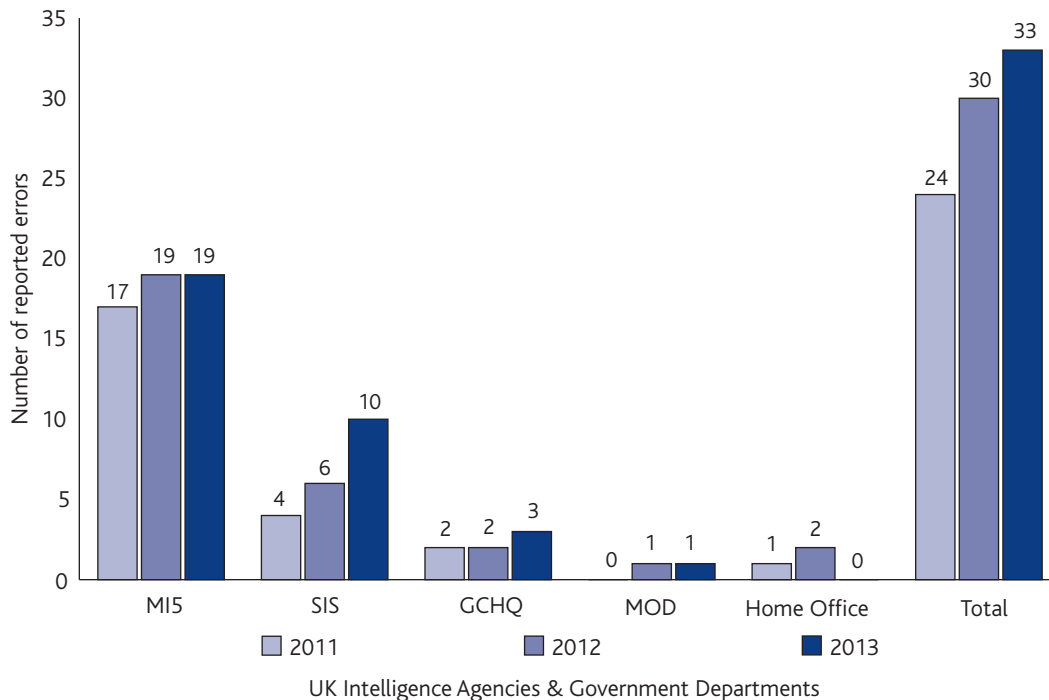
In 2013 I was made aware of **33 reportable errors**. Two of these errors were reported to me late, having happened in 2012. Those responsible for these reports have apologised and undertaken to report in a timely manner in future.

All of the errors reported to me were caused by human error and all resulted in intrusions into privacy to some degree. However, none of these errors were deliberately caused by those involved.

14 out of 33 errors occurred because the correct authorisation was not applied for or renewed, 15 out of 33 were as a result of procedural errors, 3 out of 33 arose from data being incorrectly inputted into electronic systems, and 1 out of 33 was due to prematurely cancelling an authorisation before extraction of equipment could take place.

A breakdown of the reported errors in 2011, 2012 and 2013 can be seen in Figure 1. I should emphasise that MI5 obtain a larger number of warrants and authorisations than other agencies, so although their number of errors appears high it is actually in proportion.

Figure 1: Number of Reported Errors in 2011, 2012 & 2013



Sources: Intelligence Service Commissioner, 2011 Annual Report; 2012 Annual Report

I cannot give detail in my open report about many of these errors without prejudicing national security and the operational techniques of the intelligence services and details are thus set out in the confidential annex. However, I have provided below examples of errors typical of those reported to me in 2013.

Examples of Reportable Errors

Security Service

A renewal authorisation for an MI5 agent to act as a Covert Human Intelligence Source (CHIS) expired because of an administrative oversight. The CHIS was not re-authorised until nine days after expiry of the previous authorisation. This error in procedure was not identified in the interim period because the authorising officer was overseas, absent from the office. The CHIS did not engage in any covert activity against individuals of intelligence interest during this period so any unauthorised invasion of privacy was minimal. As a result of this error all staff involved in CHIS operations were reminded of their responsibility to ensure that CHIS authorisations are renewed in time, and that lapsed authorisations cannot be renewed.

Secret Intelligence Service (SIS)

SIS reported an internal policy error in the implementation of an internal authorisation issued under an ISA section 7 authorisation. A desk officer mistakenly thought that 'internal authorisation' meant that the form only needed to be signed off by an SIS Director. In fact, the form needed to be signed by both an SIS Director and a senior FCO official. The operational activity was therefore carried out without the senior FCO official's approval. The error was only discovered after the activity had taken place. The activity itself was still lawful, and on presentation of the case the senior FCO official gave his approval retrospectively. I recommended that staff be reminded of this requirement and SIS have since amended the wording on the operational authorisation form to make it clear that the senior FCO official must also be consulted.

SIS reported another error relating to the implementation of a RIPA Part II authorisation. This occurred when an officer discussed issuing a RIPA Covert Human Intelligence Source (CHIS) authorisation with his line manager, but failed to ensure that the authorisation paperwork was completed by the line manager before meeting the target. One unauthorised meeting took place with the source. The team in question have since received refresher training on the RIPA authorisation process, and tightened up their signatory process to ensure that such an error is not repeated.

Government Communications Headquarters (GCHQ)

GCHQ made an error relating to a technical operation authorised under ISA. It occurred when an analyst failed to update the parameters of an operation in a tasking document, with the result that the operation was not properly limited to the minimum parameters necessary. The error was detected some days later when

another analyst noticed that the results did not correspond with those expected; an investigation was launched immediately. Unwanted and unauthorised information collected was destroyed without further examination.

As a consequence of this error, GCHQ have revised and tightened their internal processes. This includes making sure that tasking documents are always checked by suitably qualified individuals, who have a good awareness of the elements of an operation that need particular focus and attention to detail.

8. CONSOLIDATED GUIDANCE ON DETENTION AND INTERVIEWING OF DETAINEES BY INTELLIGENCE OFFICERS AND MILITARY PERSONNEL

The Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, on the Passing and Receipt of Intelligence Relating to Detainees (hereafter, “the Consolidated Guidance”) was published on 6 July 2010. Also published at that time was a Note of Additional Information from the Foreign Secretary, the Home Secretary and the Defence Secretary.

On 18 March 2009, prior to publication of the Consolidated Guidance, the then Prime Minister informed Parliament that he had asked, and obtained agreement from the Intelligence Services Commissioner (then the Rt Hon. Sir Peter Gibson) to monitor compliance by intelligence officers and military personnel with the Consolidated Guidance on the standards to be applied during the detention and interviewing of detainees, and to report to the Prime Minister annually.

As the Note of Additional Information said, the standards and approach outlined in the Consolidated Guidance are consistent with the internal guidelines under which each of the intelligence services and the armed forces were already operating. The novelty of the Consolidated Guidance lay in the publication of those standards and approach.

In a statement to Parliament on 19 December 2013, Kenneth Clarke announced that the Prime Minister had asked me, as Intelligence Services Commissioner, to provide my views on current compliance with those aspects of the Consolidated Guidance which I monitor. This report was to be made available to the Intelligence and Security Committee in full by the end of February 2014.

In my report to the Prime Minister I set out the history of my oversight of the Consolidated Guidance. I began by explaining what was said in my first Annual Report covering 2011 which, although it is in that Report, I set it out here in full for convenience:

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 which I would 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 advisers 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.

By my 2012 Annual Report matters had been taken a little further. I said this:

During 2012, I developed my methodology further in the belief that compliance with the guidance must:

1. Provide auditable evidence that operational staff engaged on detainee matters are following the guidance to which their respective intelligence service or government department has signed up.
2. Provide appropriate levels of assurance, including to the Commissioner and Ministers, that the guidance is being followed.
3. Seek to achieve 1 and 2 without placing significant additional administrative or resource burden on those subject to oversight.

My office undertook a "health-check" of my methodology and I am assured that (a) the detainee grid provides me with the range of information necessary for me to oversee the guidance and (b) those responsible for compiling the grids are providing full and frank information to the extent to which it is available or provided to them by relevant colleagues within their organisation. I am grateful for information provided by the intelligence services and MOD to enable this health-check to take place.

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 1 January and 31 December 2012.

The Consolidated Guidance is clear that there is an absolute prohibition of torture in international law and a clear definition of what constitutes torture. There is also an absolute prohibition on cruel, inhuman or degrading treatment or punishment (CIDT). The UK policy on such conduct is clear – we do not participate in, solicit, encourage or condone the use of torture or CIDT for any purpose.

The Consolidated Guidance and my oversight role relates to circumstances in which a decision has to be taken which concerns a detainee or the detention of an individual by a liaison service where there is a risk of torture or CIDT occurring at the hands of that third party.

It is important to emphasise that what I am seeking to monitor is whether the guidance is being followed so that when a detainee of a third party is involved, people immediately appreciate the Guidance applies and that decisions are then taken at the correct level. When I come to the statistics on page 46 it is vital to appreciate that what I am supplied with, and what I am checking, are cases where it is being properly registered that a detainee is involved and therefore the Consolidated Guidance applies, and not simply cases where it is contemplated that a detainee will be mistreated in detention.

The areas subject to my oversight are as follows:

Cases where a detainee is interviewed by UK personnel whilst under the custody of a third party
Cases where information is sought by HMG from a detainee in the custody of a third party
Cases where information is passed from HMG to a liaison service in relation to a detainee held by a third party
Cases where unsolicited intelligence related to a detainee is received from the third party
Soliciting the detention of an individual by a third party

Security Service (MI5)

The Security Service has adopted an internal policy that governs those aspects of international engagement which must be considered under the Consolidated Guidance.

The internal policy, which is fully consistent with the Consolidated Guidance, applies to the categories of detainee cases referred to in the Consolidated Guidance and helps to manage the risks inherent in dealing with liaison partners who may have very different approaches to human rights. The policy provides a decision making framework for officers and sets out who should be consulted (internally and externally) to reach a decision. The internal policy follows the Consolidated Guidance in the thresholds it sets for whether authorisation can be provided internally, or whether ministerial authorisation is required.

The internal guidance provides additional clarity for MI5 staff on the procedure around interviewing detainees in the custody of overseas liaison. It is their policy to consult ministers prior to all interviews of detainees in the custody of a liaison service. I am clear that MI5 and its staff are acutely conscious of the Consolidated Guidance and adhere to it.

Secret Intelligence Service (SIS)

SIS issue detailed policy guidance to all their staff in relation to the Consolidated Guidance. This ensures that all staff have access to details of the Consolidated Guidance itself, in what circumstances it applies and instructions on how they must record correspondence on issues relating to the guidance to ensure an effective record is maintained and can be retrieved. Directors regularly issue reminders to staff of the importance of the Consolidated Guidance. Central Policy and Legal staff Oversee and govern all compliance with the Consolidated Guidance by SIS officers.

For my first inspection in June 2013, SIS still produced a grid as before but by December, following my recommendation, they had changed their system. Their system now ensures that all correspondence is readily retrievable, thereby giving me visibility of compliance processes and the decision making underpinning them. This includes records of conversations where no exchange on detainees with liaison partners eventually transpired.

Under this new system I can also see evidence that consideration has taken place but where the decision not to proceed has been made without reference to higher authority simply because it is obvious that the risk of CIDT was too high. During my inspection visits I speak to the individual officers who explain the background to the operations in more detail.

With the sample I inspected, plus the discussions held at stations I visited where I discussed liaison relationships within the geographic region, I am confident that SIS and its personnel are very conscious of the Consolidated Guidance and adhere to it.

Government Communications Headquarters (GCHQ)

GCHQ have maintained an internal policy specifically in support of the Consolidated Guidance since it was first published in 2010.

GCHQ's policy has been kept under review throughout the period, and updated where appropriate. The policy, along with associated guidance documents, provides detailed advice to GCHQ staff on how to handle cases which may need to be considered under the Consolidated Guidance, who in GCHQ must be alerted to cases and when, what needs to be considered when assessing Consolidated Guidance-related risk, possible appropriate ways to mitigate any risk, and direction on record keeping to ensure I can oversee their work effectively. Their policy is, and will continue to be, that where there is a serious risk of CIDT, GCHQ will act to mitigate that risk, and seek ministerial authorisation as necessary. Where the risk is too high they will not proceed.

I am satisfied that GCHQ and those who work there are acutely aware of the Consolidated Guidance. I am clear that GCHQ make careful assessment of whether their activities need to be considered under the Consolidated Guidance, and I believe that GCHQ take proper care to comply with it.

Ministry of Defence (MOD)

During 2013 the MOD improved the guidance available to its staff and has put in place a robust scrutiny process, with accompanying proforma records that clearly set out the necessary decision-making steps. They maintain a "grid" of cases for my inspection from which I select cases for closer examination. Wherever a detainee of a third party might be involved a proforma has been developed that must be completed. The form is clear and works people through the process of using the guidance and concentrates the mind on the relevant points.

Prior to my inspections the MOD submitted the grid of Consolidated Guidance cases for me to make my selection to examine in more detail. All MOD Consolidated Guidance paperwork is available to me.

From my inspections I would conclude that the grid was accurately completed. I am clear from this sampling and from discussions I have had with MOD personnel that the MOD are conscious of the need to comply with the Guidance.

Training

Part of ensuring all personnel are aware of the Consolidated Guidance is down to the training provided. I have familiarised myself with the training and I set out what I understand the position to be.

Security Service (MI5)

MI5 produces a range of guidance documents for staff, and offers specific training for those most likely to be affected by the issues raised by both the Consolidated Guidance and their own parallel internal policy and guidance to staff.

The principal document is the official guidance which includes detail about how the Consolidated Guidance applies to MI5 staff, the processes to be used in such circumstances and relevant background material. MI5 review this regularly. The principles of both the Consolidated Guidance and internal policy are also covered in some detail on the training courses for investigative practitioners and managers. Training is mandatory for operational members of staff travelling overseas to participate in an interview of a detainee and ensures they are aware of relevant legislation and MI5 policy.

Central legal and policy teams are always available to investigative staff and managers as an independent source of advice.

Secret Intelligence Service (SIS)

SIS understanding of and compliance with the Consolidated Guidance is an embedded part of their training for operational officers and all officers posted overseas are required, as an integral part of their pre-posting preparation, to have training on the Consolidated Guidance which is delivered by SIS's operational policy teams. For those officers operating in parts of the world where engaging with liaison partners on detainee issues routinely gives rise to questions as to possible mistreatment or lack of due process, these courses extend to four day scenario based exercises that test advanced understanding of the operational, legal and policy challenges associated with compliance with the Guidance.

There are also online Consolidated Guidance training modules which all staff are strongly encouraged to make use of. These training modules are compulsory for officers undergoing further training in operational compliance.

More routinely, officers across the agency are encouraged to take the on-line Consolidated Guidance self-learning modules, and they are a pre-requisite for some posts and courses. I am told that there is comprehensive policy advice on the SIS intranet which details their obligations under the Guidance and how to comply and that Directors' notices regularly remind staff of the importance of the Guidance and refer them through hyperlinks to the relevant policy pages.

Government Communications Headquarters (GCHQ)

As most GCHQ staff have no direct involvement in detention operations, detailed support is targeted at deployed staff, staff with military support or counter terrorism roles, and staff in decision-making positions on intelligence release.

GCHQ runs bespoke briefing sessions for staff involved in work that might involve intelligence support to detention operations, and all staff deploying forward in support of military, SIS or MI5 customers receive a structured pre-deployment briefing before they depart.

Since last year GCHQ has also launched an e-Learning package which covers the core principles for working with liaison services on detentions and detainees, government policy, unacceptable acts, relevant laws and policies, and responsibilities of individuals and line managers. They run a round of briefings for staff in particularly relevant roles, principally those working on counter terrorism and military support. They will also be providing additional training for team leaders on the key legal principles involved in work that may involve support to detention operations, to ensure they are able to provide first line advice on detention matters to their teams.

Because of the relatively low level of detention-related reporting, GCHQ's processes are designed to funnel any issues where there is any complexity to central staff for fuller consideration of the risks, even below the thresholds described within the Consolidated Guidance.

Ministry of Defence (MOD)

The MOD has disseminated widely a guidance document for all personnel, both military and civilian, to ensure that the safeguards within the Consolidated Guidance are applied appropriately in the types of situations in which MOD personnel might become involved in intelligence sharing. It covers the decision making process and the record keeping requirements and is intended to cover both active military operations and more conventional intelligence-sharing relationships. This document is widely accessible to department personnel.

Additional support is targeted at those members of staff likely to be actively involved in sharing or receiving intelligence as part of their duties. For example, the departmental guidance has been supplemented with specific operating instructions for UK personnel operating in Afghanistan, where an inherent part of their mission is to work closely with and develop Afghan National Security Forces. Training provision has been developed over the course of 2013 and Armed Forces and civilian personnel working with intelligence now routinely receive briefings on Consolidated Guidance requirements before deploying to Afghanistan. Those personnel expected to be regularly involved in work which could engage the Consolidated Guidance, such as policy advisers, military lawyers and some commanders, are exercised on the process during their pre-deployment training. The Army Legal Service also provides more in-depth legally-tailored training to military lawyers.

Statistics

I have not in previous reports published any statistics indicating the number of occasions when the Consolidated Guidance has been applied, and the extent of my checking. That is because the figures can easily be misinterpreted by the public and misused by those who might wish to do this country harm, or make false

allegations against it. I have decided that it is in the public interest to disclose these figures, but I caution strongly against any misinterpretation.

The total number of cases where the Consolidate Guidance was applied during 2013 was 418. It is important to understand what this means. It means that there were 418 cases where consideration had to be given as to whether there was a serious risk of an individual being subject to unacceptable conduct either because they were in the detention of a liaison service, or if intelligence was supplied to solicit detention and they were then detained. This does not show the number of individuals subject to unacceptable conduct; only that proper consideration was being given to that risk in this number of cases.

I have full details of all 418 including what decision was taken and by whom, including instances when a decision is taken where there was no serious risk, and action could be taken on that basis, and decisions when it is assessed there was a serious risk that could not be mitigated and that (for example) no intelligence should be shared so as to solicit detention.

I took a random sample to cross-check that the information with which I was supplied was accurate and for the purpose of checking the underlying paperwork: that sample was 65, or over **15%** of the 418 cases.

Conclusion

The high number of cases in which the Consolidated Guidance is applied demonstrates how seriously it is taken when detainees of third party countries are concerned. The fact that my sampling of over 15% of those cases shows that what is being reported to me is accurate indicates again that the guidance is being applied properly and well.

9. INVESTIGATION OF POTENTIAL MISUSE OF DATA

Although an area outside of my statutory remit, I have sought and been provided with:

- details of the procedures in place to detect potential inappropriate use of, or access to, operational data by staff in the intelligence services; and
- details of any actions taken where appropriate, including disciplinary action.

I made it clear to the agencies that any inappropriate use of, or access to, operational data is unacceptable. This is an area covered during my oversight visits and I am satisfied that the agencies have robust systems in place to detect wrongdoing and strict procedures for disciplining staff if wrongdoing has occurred.

A member of the Home Affairs Select Committee asked for the number of disciplinary findings I had been shown during 2013. I said I would try to provide the figure in this report. However, without the benefit of full context, which I cannot give in an open report, to provide such detail could be both inaccurate and misleading. Therefore I do not believe it is in the public interest to do so at this time. However, I have given full details in my confidential annex.

10. CONCLUSION

As part of my ongoing commitment to openness and transparency, I have sought to disclose more detail than I did in 2012 because it is important that the public have confidence in the way in which the agencies conduct their activities and in how those activities are regulated. I should like to emphasise, as I hope this report shows, that my scrutiny is the final stage in a robust process starting with the agencies themselves and their compliance departments, including lawyers, through which authorisations and warrants must be processed. The warrant applications must then be considered by personnel advising a minister and then by the minister him or herself. All involved know that a Commissioner can scrutinise any and all of the documentation to check whether the necessity and proportionality case has been properly made and that any warrant or authorisation has been issued lawfully.

In conclusion I can report that:

- i) the secretaries of state authorising warrants for intrusive surveillance and interference with property are doing so lawfully;
- ii) other authorisations (such as for directed surveillance or covert human intelligence sources) are being issued on a proper basis;
- iii) section 7 of ISA authorisations are being issued on a proper basis;
- iv) authorisations granted by the MOD are being granted on a basis that would comply with RIPA Part II, if RIPA Part II applied.

In particular I can report that proper cases were made as to the necessity of the intelligence being obtained, and as to the proportionality of the activities authorised.

Of the 318 warrant and authorisations I reviewed in 2013, eight contained administrative errors which is a marked increase since last year when I discovered only one. Although these are correctable slips they are still unacceptable. I have recommended that the agencies put in place procedures to prevent further re-occurrence and I will continue to monitor this. One of these slips was made by a warrantry unit but I informed the relevant agency that it is their responsibility to ensure that they have proper authorisation for their activities.

I have recommended to all the agencies that separate consideration be given to the individual privacy being invaded as part of the test for proportionality. In all

cases I want to see this set out separately in the application for these intrusive techniques and to see this wording reflected in the warrants.

I have also recommended that the agencies bring to my attention any cases where special restrictions apply or where they have concerns.

As regards the Consolidated Guidance, this is taken seriously by all the agencies and the MOD and decisions are being taken by the appropriate people where a detainee of a third party or detention by a third party of an individual is involved. Looking forward I have tasked the agencies to find ways to capture instances where the Consolidated Guidance has been discussed or considered at an early stage but a decision has been taken not to proceed.

Overall I believe the agencies act within the constraints imposed upon them by law and the public should have confidence that they do so.

APPENDIX

Useful Background Information

As background to the oversight I provide, it is helpful to be aware of the statutory functions each of the intelligence services fulfils and certain constraints to which all are subject.

In this appendix I set out:

- The statutory functions of the Intelligence Services
- A summary of the Regulation of Investigatory Powers Act 2000 (RIPA)
- A summary of Warrants and Authorisations under the Regulation of Investigatory Powers Act 2000
- A summary of Warrants and Authorisations under the Intelligence Services Act 1994 (ISA)
- Article 8 of the European Convention on Human Rights
- The authorisation process for warrants and section 7 authorisations
- Definitions of Necessity and Proportionality

The Statutory Functions of the Intelligence Services

Security Service (MI5)

The functions of MI5 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;

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; and

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.

The Regulation of Investigatory Powers Act 2000 (RIPA)

The commencement of the Regulation of Investigatory Powers Act 2000 (RIPA) introduced a number of changes to existing legislation. The most significant of these was the incorporation into surveillance powers of the fundamental protections afforded to individuals by the Human Rights Act 1998. RIPA was also designed to remain relevant in the face of future technological change through technologically neutral provisions. The full text of RIPA is available at www.legislation.gov.uk

Part I	Part I of RIPA is concerned with the interception of communications (the content of a communication), and the acquisition and disclosure of communications data (the who, when and where of a communication). Oversight of Part I activities, including the Secretary of State's role in interception warrantry and the regime for acquiring communications data, is provided by the Interception of Communications Commissioner, Sir Anthony May. He produces his own report on Part I activities and this area is therefore not included in my oversight.
Part II	Part II of RIPA provides a statutory basis for the authorisation and use of covert surveillance (both directed and intrusive) and covert human intelligence sources (undercover officers, informants etc.) by the intelligence agencies and certain other public authorities. Part II regulates the use of these intelligence-gathering techniques and safeguards the public from unnecessary and disproportionate invasions of their privacy.
Part III	Part III of RIPA contains powers designed to maintain the effectiveness of existing law enforcement capabilities in the face of the increasing use of data encryption by criminals and hostile intelligence agencies. It contains provisions to require the disclosure of protected or encrypted data, including encryption keys. Part III came into force on 1 October 2007, after Parliament approved a Code of Practice for the investigation of protected electronic information.
Part IV	Part IV of RIPA provides for the independent judicial oversight of the exercise of the various investigatory powers. This includes provisions for the appointment of Commissioners, and the establishment of the Investigatory Powers Tribunal as a means of redress for those who complain about the use of investigatory powers against them. This section was amended by the Justice and Security Act 2013 to extend the powers of the Intelligence Services Commissioner so that the Prime Minister may direct me to keep under review the carrying out of any aspect of the functions of the Intelligence Services. Part IV also provides for the issue and revision of the codes of practice relating to the exercise and performance of the various powers set out in Parts I to III, as well as section 5 of the Intelligence Services Act 1994.

Part V	Finally, Part V of RIPA deals with miscellaneous and supplementary matters. Perhaps the most relevant to my functions is section 74, which amended section 5 of the Intelligence Services Act 1994. This relates to the circumstances in which the Secretary of State may issue property warrants, in particular by introducing a criterion of proportionality.
---------------	---

Warrants and Authorisations under the Regulation of Investigatory Powers Act 2000 (RIPA)

Part II of RIPA provides a statutory basis for the authorisation of covert surveillance and covert human intelligence sources, and their use by the intelligence agencies and other designated public authorities. Part II regulates the use of these techniques and safeguards the public from unnecessary and disproportionate invasions of their privacy.

Directed Surveillance Authorisation (DSA)

What is directed surveillance?

Surveillance is defined as being directed if all of the following criteria are met:

It is covert, but not intrusive surveillance;
It is conducted for the purposes of a specific investigation or operation;
It is likely to result in 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 in circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

How is directed surveillance authorised?

Under section 28 of RIPA designated persons within each of the intelligence services and the armed services may authorise surveillance. The authoriser must believe:

That the DSA is necessary for a specific human rights purpose (for the intelligence agencies this is in the interests of national security, for the purpose of preventing or detecting crime or disorder, or in the interests of the economic well-being of the UK; for the armed services it is, in addition, for the purpose of protecting public health or in the interests of public safety);
That surveillance is undertaken for the purposes of a specific investigation or operation; and

That it is proportionate to what it seeks to achieve and cannot be achieved by other (less intrusive) means.

How is directed surveillance used in practice?

An example of directed surveillance could include surveillance of a terrorist suspect's movements in public, in order to establish information about their pattern of life.

Covert Human Intelligence Source (CHIS)

What is CHIS?

A CHIS is essentially a person who is a member of, or acting on behalf of, one of the intelligence services and who is authorised to obtain information from people who do not know that this information will reach the intelligence or armed services. A CHIS may be a member of the public or an undercover officer.

A person is a CHIS if:

a) He establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

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.

How is CHIS authorised?

Under section 29 of RIPA designated persons within the relevant intelligence service or the armed services may authorise the use or conduct of a CHIS provided that the authoriser believes:

That it is necessary for a specific human rights purpose (for the intelligence agencies this is in the interests of national security, for the purpose of preventing or detecting crime or disorder, or in the interests of the economic well-being of the UK; for the armed services it is, in addition, for the purpose of protecting public health or in the interests of public safety);

That the conduct or use of the source is proportionate to what it seeks to achieve; and

That the information cannot be obtained by other (less intrusive) means.

The legislation requires a clear definition of the specific task given to a CHIS, and the limits of that tasking. It also requires that the CHIS is closely managed,

including having regard to his or her security and welfare. All of this must be recorded for accountability purposes and managers are required to ensure that their staff comply with the legislation.

How is CHIS used in practice?

This could include the authorisation of the conduct of an informant tasked with developing a relationship with a suspected terrorist, in order to provide information to an intelligence agency.

Intrusive Surveillance

What is intrusive surveillance?

Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and involving the presence of an individual on the premises or in the vehicle, or the deployment of a surveillance device. The definition of surveillance as intrusive relates to the location of the surveillance, as it is likely to reveal private information.

How is intrusive surveillance authorised?

Under section 42 of RIPA, the Secretary of State may authorise a warrant to undertake intrusive surveillance which is necessary for the proper discharge of one of the functions of the intelligence services or the armed services.

Before the Secretary of State can authorise such action he must believe;

That it is necessary in the interests of national security, the purpose of preventing or detecting crime or disorder, or in the interests of the economic well-being of the UK;
That the authorised surveillance is necessary and proportionate to what it seeks to achieve; and
That the information cannot be obtained by other (less intrusive) means.

As a result of the naturally heightened expectation of privacy in the locations in which intrusive surveillance takes place, it is not necessary to separately consider whether the surveillance is likely to lead to private information being obtained.

How is intrusive surveillance used in practice?

Typically this would involve planting a surveillance device in a target's house or car, normally combined with a property warrant under section 5 of ISA.

Warrants and Authorisations under the Intelligence Services Act 1994 (ISA)

The Intelligence Services Act 1994 was introduced to make provisions for the issue of warrants and authorisations to enable MI5, SIS and GCHQ to carry out certain actions in connection with their functions. The Act also made provisions for the establishment of an Intelligence and Security Committee to scrutinise the intelligence services, and set out procedures for the investigation of complaints made about them. The Act is available in full at www.legislation.gov.uk

Section 5 Warrants

What is a section 5 warrant?

Under section 5 of ISA the Secretary of State may issue warrants authorising MI5, SIS or GCHQ to enter on to, or interfere with, property, or to interfere with wireless telegraphy. Often referred to as property warrants, their use must be necessary for the proper discharge of one of the functions of the applying agency.

How are section 5 warrants authorised?

Before the Secretary of State gives any such authority, he must first be satisfied of a number of matters:

That the acts being authorised are necessary for the purpose of assisting the particular intelligence agency to carry out any of its statutory functions;

That the activity is necessary and proportionate to what it seeks to achieve and it could not reasonably be achieved by other (less intrusive) means; and

That satisfactory arrangements are in place to ensure that the agency shall not obtain or disclose information except insofar as necessary for the proper discharge of one of its functions.

How are section 5 warrants used in practice?

A section 5 warrant might be used to authorise entry to a property and concealment of a listening device within it. In such cases, a section 5 warrant will be used in conjunction with an intrusive surveillance warrant.

Section 7 Authorisations

What is a section 7 authorisation?

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.

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 exempted from such liability where authorised by the Secretary of State. A section 7 authorisation would of course have no effect on the law in the country where the act is to be performed. The Secretary of State, before granting each authorisation, must be satisfied of the necessity and reasonableness of the acts authorised. Reasonableness will include a requirement to act so as not to intrude on privacy any further than justified by the necessity to achieve what is authorised.

How are section 7 authorisations authorised?

Before the Secretary of State gives any such authority, he must first be satisfied:

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;
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;
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; 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.

How are section 7 authorisations used in practice?

These authorisations may be given for acts of a specified description, in which case they are referred to as class authorisations. In practice this could mean obtaining intelligence by way of agent operations overseas.

The European Convention on Human Rights (ECHR)

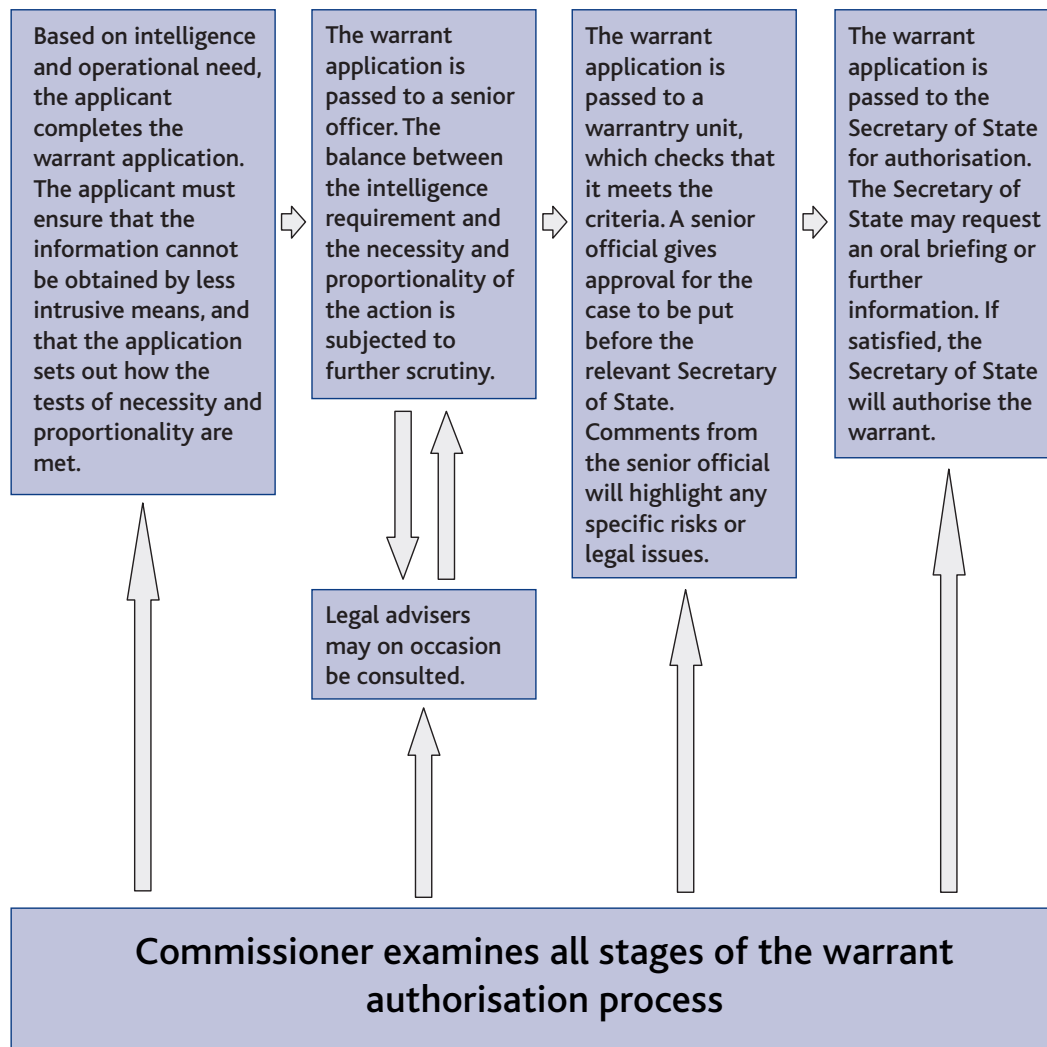
The ECHR was introduced into UK law on 1 October 2000 when the Human Rights Act came into force.

Article 8

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Application Process for Warrants



As detailed above, the role of the Secretaries of State as democratically elected individuals signing off acts which may involve intrusion into the private lives of citizens is important. Secretaries of State spend a substantial amount of time and effort considering operational merits, necessity, proportionality and wider implications before signing off warrants and authorisations.

Necessity and Proportionality

When deploying intelligence gathering techniques, the intelligence services always aim to take courses of action that are effective, minimally intrusive into privacy, and proportional to the identified threat. Before intrusive methods of intelligence gathering are used, the intelligence services must justify to the relevant Secretary of State that what they propose to do is both:

Necessary for the protection of national security, or for the purpose of safeguarding the economic well-being of the UK against threats from overseas, or in order to prevent or detect serious crime, or, additionally in the case of the armed services, protecting public health or in the interests of public safety; and

Proportionate to what the activity seeks to achieve, i.e. that the intelligence gain will be sufficiently great to justify the intrusion into the privacy of the target, and any unavoidable collateral intrusion into the privacy of individuals other than the target.

The relevant Secretary of State also needs to be satisfied that the information that is expected to be obtained could not reasonably be obtained by other, less intrusive, means.

These are important tests, and the intelligence services apply for warrants only where they believe the threshold is clearly met.

ISBN 978-1-4741-0117-2



9 781474 101172