

# Report of the Intelligence Services Commissioner for 2014

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 25 June 2015

Laid before the Scottish Parliament by  
the Scottish Ministers 25 June 2015

HC 225  
SG/2015/74



© Crown copyright 2015

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](http://nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk).

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at [www.gov.uk/government/publications](http://www.gov.uk/government/publications)

Any enquiries regarding this publication should be sent to us at [insert contact details]

Print ISBN 9781474121118

Web ISBN 9781474121125

ID 04061503 06/15

Printed on paper containing 75% recycled fibre content minimum

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

# CONTENTS

<b>FOREWORD</b>	<b>2</b>
<b>1. FUNCTIONS OF THE INTELLIGENCE SERVICES COMMISSIONER</b>	<b>7</b>
<b>2. METHOD OF MY REVIEW IN RELATION TO WARRANTS AND AUTHORISATIONS</b>	<b>9</b>
<b>3. STATISTICS</b>	<b>11</b>
<b>4. ASSESSMENT OF MY INSPECTION VISITS</b>	<b>12</b>
i. Intrusive Surveillance	12
ii. Directed Surveillance Authorisation (DSA)	15
iii. Intelligence Services Act (ISA) - Property interference warrants	17
iv. Covert Human Intelligence Source (CHIS)	20
v. Intelligence Services Act (ISA) Section 7 authorisations	23
vi. Consolidated Guidance	27
vii. Bulk Personal Data	32
<b>5. PRODUCT OBTAINED AND HANDLING ARRANGEMENTS</b>	<b>39</b>
<b>6. ERRORS</b>	<b>40</b>
<b>7. BRIEF SUMMARY OF ASSESSMENTS</b>	<b>46</b>
<b>8. CONCLUSIONS</b>	<b>56</b>
<b>APPENDIXES</b>	<b>57</b>
1. The Statutory Functions of the Intelligence Services	58
2. The Regulation of Investigatory Powers Act 2000 (RIPA)	59
3. Warrants and Authorisations under the Regulation of Investigatory Powers Act 2000 (RIPA)	60
4. Warrants and Authorisations under the Intelligence Services Act 1994 (ISA)	64
5. The European Convention on Human Rights (ECHR)	66
6. Necessity and Proportionality	67
7. Bulk Personal Datasets Direction	68
8. Consolidated Guidance Direction	69



The Rt Hon Sir Mark Waller  
Intelligence Services Commissioner  
2 Marsham Street  
London  
SW1P 4DF

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

I enclose my fourth Annual Report covering the discharge of my functions as Intelligence Services Commissioner between 1 January 2014 and 31 December 2014.

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 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 further details including techniques and operational matters which in my view should not be published. I hope you find this convenient.

A handwritten signature in black ink, appearing to read 'Mark Waller'. Below the signature are three short horizontal lines: a longer one on the left, a shorter one in the middle, and another longer one on the right.

The Rt Hon Sir Mark Waller



# INTELLIGENCE SERVICES COMMISSIONER



## FOREWORD

Under section 59 of the Regulation of Investigatory Powers Act 2000 (RIPA) 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. I was appointed by the Prime Minister to the post of the Intelligence Services Commissioner on 1 January 2011. 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.

The UK continues to be a target for groups and gangs, from home and abroad, who would threaten our national security and economic well being. In August 2014, the Joint Terrorism Analysis Centre (JTAC) raised the United Kingdom (UK) threat level from "substantial" to "severe", meaning that an international terror attack on UK soil is highly likely.

In the last 10 years, we have seen a step change in the nature of the threats we face with the tragic events in Paris and Copenhagen early in 2015 being recent examples of how terrorist tactics have evolved and diversified since 9/11 and 7/7.

The police, intelligence and security agencies and the Ministry of Defence (MOD) play a vital role protecting our country and meeting these challenges. They have been given wide ranging powers and capabilities by Parliament (further detail on the intelligence and security agencies and MOD's functions can be found in the appendix to this report) to disrupt the threats to the UK and our interests including powers to intrude upon the privacy of individuals.

## What I oversee

As Intelligence Services Commissioner, I am responsible for auditing the authorisations required by the UK intelligence agencies and their officers enabling them to use lawfully the intrusive powers available to them under RIPA part II and the Intelligence Services Act 1994 (ISA). I also fulfil the same function in relation to the MOD's use of equivalent authorisations. In summary I oversee the granting of warrants and authorisations by Ministers where those are necessary, and internal authorisations where those are necessary.

I also oversee the use by the agencies of bulk personal datasets and compliance by the agencies and MOD with the Consolidated Guidance.<sup>1</sup> See Chapters 4.vi and 4.vii of this report for more detail about how I oversee these activities.

<sup>1</sup> 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

I take it as a priority that any intrusion into privacy must be fully justified by the necessity to gain intelligence or carry out the activities in the interests of the UK and I do this by ensuring all activity undertaken by the agencies:

- is necessary for the purpose of protecting national security, the prevention or detection of crime or the economic well-being of the UK;
- falls under one of the statutory functions of the intelligence services;
- is proportionate including that:
  - a) a less intrusive means could not have been used
  - b) intrusion into privacy is limited so far as possible
  - c) in particular any collateral intrusion into privacy is identified and kept to a minimum
  - d) any intrusion is justified by the necessity to gain the intelligence or protect the UK.
- is/was authorised by a relevant senior official or Secretary of State.

### **Structure of oversight relating to warrants and authorisations**

RIPA formally established the oversight mechanisms which Parliament intended for the intelligence services.

The oversight I provide is part of a much broader oversight structure which includes:

#### **Secretaries of State**

Each agency falls under the authority of a Secretary of State who is accountable to Parliament for what agencies do or fail to do. Their personal authorisation is required for more intrusive activities of the agencies.

#### **Parliamentary oversight**

The Intelligence and Security Committee of Parliament (ISC) (a cross party committee which draws its membership from both Houses) primarily examine MI5, MI6 and GCHQ's expenditure, administration and policy. The Committee reports to Parliament annually, and carries out other inquiries on which they produce reports.

#### **Independent judicial oversight**

The Interception of Communications Commissioner and the Intelligence Services Commissioner are appointed by the Prime Minister and are required to be the holder or past holder of high judicial office, ensuring independent, unbiased judgement. The Interception of Communications Commissioner is concerned with interception and communications data and now produces two reports a year, the most recent dated 12th March 2015. I as Intelligence Services Commissioner oversee other matters, as summarised on page (7) below.

It is the Secretary of State who is responsible for taking the relevant decision in the most intrusive areas and who is also accountable to Parliament. I, as Commissioner, have the function of review. The way I carry out my review is set out in Chapter 2. The essential features which I emphasise at this stage are:

1. I carry out two formal inspections a year at each of the agencies and MOD and at the warrantry units at the Foreign Office, the Home Office and the Northern Ireland Office;
2. I get a complete list of all warrants and authorisations current during the period including relevant internal approvals; the lists identify the subjects of the warrants and authorisations;
3. I select certain warrants, authorisations and internal approvals both randomly and by reference to subject matter so that the full paperwork that lies behind those warrants and authorisations can be assembled for my scrutiny;
4. The agencies, the MOD and the warrantry units also bring some warrants or authorisations to my attention which they think I should see and again the full paperwork will be made available;
5. At the agencies and MOD I personally read the warrants and authorisations and the paperwork that lies behind including submissions and supporting documentation; at the Foreign Office, the Home Office and the Northern Ireland Office I spend further time reading the paperwork mostly relating to different warrants and authorisations;
6. At the agencies and MOD I then hold formal interview sessions with those responsible for the documentation and carrying out the activities authorised; at the Foreign Office, the Home Office and the Northern Ireland Office I interview and question those responsible for advising ministers and considering the warrants and authorisations.
7. Once a year I meet each of the ministers – the Foreign Secretary, the Home Secretary, the Northern Ireland Secretary and the Defence Secretary.

A duty of cooperation is imposed on every member of an agency, every departmental official and every member of the armed forces to disclose or provide to me all such documents and information as I may require. I have never had anything but cooperation in this regard.

I emphasise that I do this activity personally and I undertake my duty rigorously and entirely independently of government, Parliament and the intelligence agencies themselves, without political favour or personal bias.



## Review of 2014

Apart from my inspections other matters which occurred in 2014 were as follows.

In January the Prime Minister asked me to report on compliance with the Consolidated Guidance so that the ISC might be properly informed of my views. That Report was produced in February 2014 and provided to the ISC.

In March, I was ordered to give evidence at the Home Affairs Select Committee's Inquiry into Counter-Terrorism. I had taken the view that the appropriate Parliamentary Committee with whom I should discuss my oversight was the ISC. The Home Affairs Committee took a different view and ordered me to attend and thus I did so.

I also appeared before the ISC in October in relation to their Privacy and Security Inquiry.

I was pleased to have had the opportunity to co-host the International Intelligence Review Agency Conference with the ISC in July. The conference focused on the complex balance between protecting an individual's right to privacy and ensuring our collective right to security.

The Home Secretary opened the conference and representatives of the oversight bodies from fifteen different countries attended. Privacy safeguards continue to be my priority so I was particularly interested to exchange views and ideas with my counterparts in other democratic countries. The conference provided an expert forum for legislators and senior office holders working in the field of intelligence oversight to:

- identify current international challenges and drivers;
- consider emerging concerns that impact domestically and internationally;
- exchange ideas and compare models of accountability, including lessons learned and good practice;
- support countries in developing of intelligence oversight mechanisms drawing on the experience of countries with existing structures; and broaden dialogue and expand the expert network towards further international collaboration.

Finally, I was pleased to welcome the Prime Minister's decision to put my oversight of the Consolidated Guidance and bulk personal datasets onto a statutory footing. All of my oversight is now on a statutory footing and I have no extra- statutory responsibilities.

In particular I welcome that the agencies' use of bulk personal datasets and my independent oversight has been avowed. I have had non-statutory oversight since my appointment that oversight having been accepted by my predecessor just

before his appointment ended. In his announcement of 12 March 2015 the Prime Minister said:

*"The Intelligence Services Commissioner, the Rt Hon Sir Mark Waller, currently provides non-statutory oversight of the Security and Intelligence Agencies' use of bulk bulk personal datasets. Sir Mark has previously recommended that this be put on a statutory footing."*

I reported on this aspect in the confidential annex to my Annual Reports. In my Annual Report for 2013 I reported in my confidential annex for example on the agencies' acquisition, retention, storage and deletion of bulk personal datasets as well as access to and use of such data. In doing so I considered the related privacy issues and safeguards, particularly the possibility of data being misused and how this is prevented. I consider this to be a key part of my oversight as it is critical that access to bulk personal data is properly controlled and the risk that some individuals may misuse their powers to access private data is carefully guarded against. I report on this further in chapter 4.vii of this report.

## **Structure of my report**

I am committed to being as open and transparent with the public as I possibly can be within the constraints of my office and of the subject matter I deal with. To this end as part of my continued drive for greater openness I have restructured my report and dealt with issues thematically including, for example, sections on Intrusive Surveillance, Directed Surveillance, Covert Human Intelligence Sources and Intelligence Services Act section 7 authorisations. There is also a section on my recently publically avowed Bulk Personal Data oversight. These sections highlight privacy considerations and provide my overall assessment during 2014 including some of the recommendations I have made to help ensure continued compliance.

My office also re-launched my website last October which now contains more detail about my functions, the legislative framework under which I operate and how I carry out my inspections.

# 1. FUNCTIONS OF THE INTELLIGENCE SERVICES COMMISSIONER

My statutory functions are set out in full on my website, but in summary my primary role as Intelligence Services Commissioner is to ensure the UK intelligence agencies and parts of the Ministry of Defence lawfully and appropriately use the intrusive powers available to them including:

**Figure 1: Oversight of warrants and authorisations issued by Secretaries of State**

Function	Legislation
Oversight of the Secretary of State's powers to issue, renew and cancel warrants authorising entry on to or interference with property (eg the planting or installing of a listening device) or with wireless telegraphy	Section 5 and 6 of the Intelligence Services Act 1994
Oversight of the Secretary of State's powers to issue, renew and cancel authorisations for acts done outside the United Kingdom	Section 7 of the Intelligence Services Act 1994
Oversight of the Secretary of State's powers to grant authorisations for intrusive surveillance(e.g. monitoring through a listening device)	Regulation of Investigatory Powers Act 2000 (RIPA) Part II
Oversight of the Secretary of State's powers to grant authorisations to investigate electronic data protected by encryption	Regulation of Investigatory Powers Act 2000 (RIPA) Part III



**Figure 2: Oversight of internal authorisations issued by a Designated Officer**

Function	Legislation
Oversight of powers to grant authorisations for directed surveillance (DSA)	Regulation of Investigatory Powers Act 2000 (RIPA) Part II
Oversight of powers to grant authorisations for the conduct and use of covert human intelligence (CHIS)	Regulation of Investigatory Powers Act 2000 (RIPA) Part II

In the last year, under section 59A of the Regulation of Investigatory Powers Act 2000 (as amended by section 5 of the Justice and Security Act 2013), the Prime Minister published two directions which put on a statutory footing my oversight of:

- the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets including the misuse of data and how this is prevented
- compliance with the Consolidated Guidance

Both directions can be found in the appendix to my report.

My other statutory functions include:

- Assisting the Investigatory Powers Tribunal when required;
- Reporting to the Prime Minister annually on the discharge of my duties;
- Overseeing the adequacy of the Part III safeguards of RIPA arrangements;
- Advising the Home Office on the propriety of extending the TPIM regime;
- Overseeing any other aspects of the functions of the intelligence services, HM Forces or the MOD when directed by the Prime Minister.

## 2. METHOD OF MY REVIEW IN RELATION TO WARRANTS AND AUTHORISATIONS

It is my duty, as far as I am able, to satisfy myself that the agencies have acted within the law and that the test of necessity and proportionality has been correctly applied.

I do this through my formal four stage inspection regime (a summary of my method can be seen on the right) where I audit warrants and authorisations.

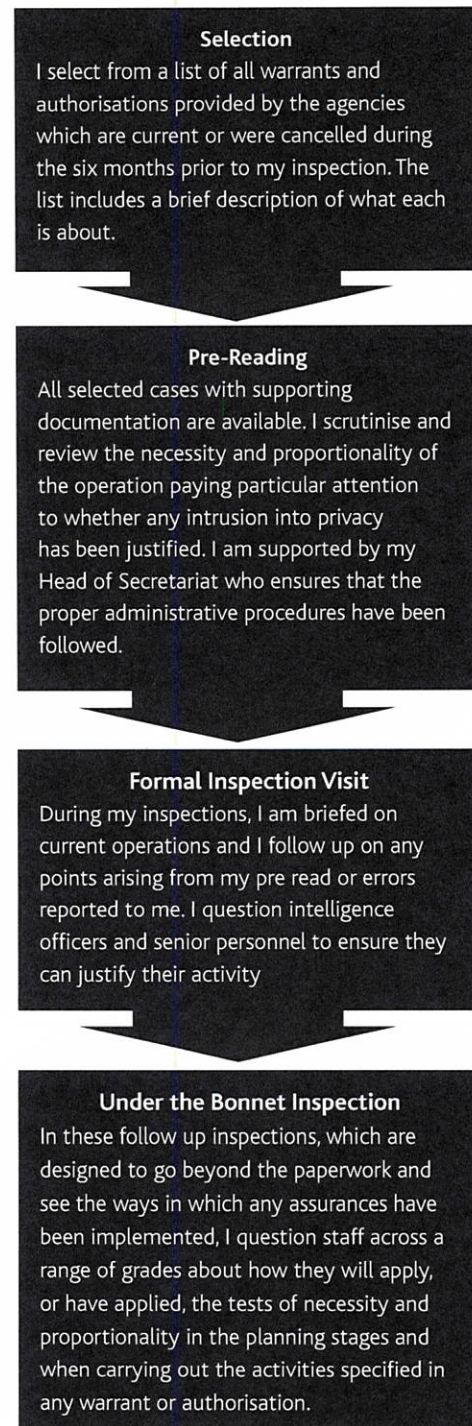
I examine the systems in use to assure myself that the organisations I oversee have robust and rigorous internal checks and assurances in place. I also attend training courses given to both new and existing intelligence officers in order to gain a better understanding of the culture and ethos of the organisation.

During my formal inspections, I examine a statistically significant sample of:

- warrants issued by Secretaries of State authorising intrusive surveillance and interference with property and;
- other authorisations issued by designated officials (such as for covert human intelligence sources and directed surveillance)

In 2014 I was provided with a complete list of all 2032 warrants and authorisations and selected 343 so that I could read and scrutinise the supporting submissions and paperwork behind the same. Because some operations continue for substantial periods of time, I will have seen other warrants and authorisations on the list and the paperwork behind them during previous inspections.

Figure 3: Stages of oversight



## Who I met

During 2014 I undertook formal oversight inspections of each of the authorities that apply for and authorise warrants that I oversee. They are:

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

In addition I inspected the departments processing warrants (warrantry units) for each Secretary of State where I scrutinise the way submissions have been analysed and the advice given to, and the approach of, the Secretaries of State. They are:

<b>The Home Office</b>
<b>The Foreign Office</b>
<b>The Northern Ireland Office (NIO)</b>

I also meet the respective Secretaries of State who sign off warrants at each department. They are:

<b>The Home Secretary</b>
<b>The Foreign Secretary</b>
<b>The Defence Secretary</b>
<b>The Northern Ireland Secretary</b>

Details of the visits made to the agencies, MOD and to the Foreign Office, Home Office and Northern Ireland Office are contained later in my report with a summary of my conclusions on the same.



### 3. STATISTICS

I believe that publishing the total number of RIPA and ISA authorisations 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.

I select warrants for scrutiny from a full list of all 2032 current warrants and authorisations provided by the agencies. This list includes brief descriptions of what each is about so in effect I see all of warrants and authorisations but select some for closer examination including in particular the submissions and other underlying documentation. In 2014 I selected 343 warrants and authorisations with their supporting documentation for closer scrutiny. Others or more accurately their predecessors, particularly those for long running operations, will have been seen during previous inspections.

Warrants and authorisations have a finite duration, expiring after 3, 6 or 12 months. As a result, the 2032 warrants and authorisations approved in 2014 should not be interpreted as adding to a cumulative total of warrants and authorisations over preceding years. I have set out these figures below for comparison.

**Figure 4: Statistics by Year**

Year	2011	2012	2013	2014
Approved	2142	2838	1887	2032
Scrutinised	————	242	318	343
Percentage	————	8.5%	16.8%	16.7%

Although it is vitally important that I scrutinises a representative sample of warrants and their underlying documentation I am of the view that understanding the systems and processes in place in the agencies is also important. Inspection of the warrants and their supporting documentation is not the extent of my oversight in this area. As well as the four stages of my inspection regime I also attend training courses given to both new and existing intelligence officers so that I can gain a better understanding of the culture and ethos of the organisation. On top of this I check the systems in place within the organisation to assure myself that they have in place robust and rigorous internal checks and assurances.

It is all of this taken together which allows me to undertake my oversight of the warrantry and authorisations.

## 4. ASSESSMENT OF MY INSPECTION VISITS

### i. Intrusive Surveillance

Intrusive surveillance is covert surveillance related to anything taking place on residential premises or in a private vehicle, and involving an individual being present on the premises or in the vehicle, or deploying of a surveillance device. The definition of surveillance as intrusive relates to the location of the surveillance, since the surveillance in residential premises or vehicles is likely to involve a greater intrusion into privacy. Part II of RIPA and the associated code of practice provide the legal framework for authorising surveillance activity which is compatible with Article 8 of the European Convention on Human Rights (ECHR) (see appendix).

#### Privacy

Intrusive surveillance involves the greatest invasion of privacy and as such consideration must be given as to how to avoid unnecessary intrusion into privacy and specifically the privacy of any family members or friends of the individual under surveillance. The agencies must make a strong case to explain why the information to be obtained cannot be gathered by less intrusive means and that the necessity of obtaining the information outweighs the intrusion into privacy.

#### My overall assessment

In the submissions I have examined proper cases for necessity have been made and proper consideration has been given to limiting unnecessary intrusion into privacy and minimising collateral intrusion. The invasion authorised has also been justified by the necessity. **There are however some points to be made.**

- Timing of applications for warrants

According to the relevant codes of practice, application for DSA and CHIS renewals must be made **shortly** before the authority in force is due to end. However, warrants signed by a Secretary of State only require that the renewal is made **before** the warrant expires. This does not prevent the agency from applying for a renewal some months before the expiry date so that when the Secretary of State gives consideration to the renewal, the case for necessity and proportionality is in danger of being out of date. The possibility of a busy period coming up (such as the Olympic Games) or difficulties of availability (such as can be caused by a General Election) understandably lead agencies to put applications in train early but I have **recommended** that applications for renewal should be made only shortly before the warrant expires.

- Breadth of language

Intrusive surveillance can only take place in support of one of the functions of the intelligence services in relation to the activity specified in the warrant signed by the Secretary of State. In Northern Ireland I was concerned with the breadth of language used to define the subjects on two urgent warrants, one of which included an intrusive surveillance authorisation. However after challenging the Northern Ireland Office (NIO) I was reassured that they were keeping a very close eye on the use of the warrants and that the Secretary of State expected to be notified of any use. I was satisfied that the urgency of the warrants was necessary and that the correct procedures had been applied but **recommended** that the renewal submission, which had to take place within two working days, should reflect the limitations being applied by NIO to the use of the warrant.

I also noticed this in a few warrants seen at MI5 and stated that **care should be taken** with the language to identify who the subject of the warrant could be.

- Confidential Information and Collateral Intrusion

In the cases I reviewed I noted that careful consideration was given to the possibility that any confidential information might be obtained and consideration was given to any collateral intrusion and how to limit this. I **recommended** that the submission should spell out what is in place to limit collateral intrusion and that the submission should make clear that anything that is not of intelligence interest should be deleted as soon as practicable.

- Gardens

Paragraph 2.16 of the surveillance code of practice states that a front garden or driveway readily visible to the public would not be regarded as residential property for the purpose of RIPA. I **recommended** that this should be interpreted with caution and read in conjunction with RIPA s26(5) which states that devices which constantly provide information as if the device were actually present on the premise would be intrusive surveillance.

## Conclusion

Intrusive surveillance is the most intrusive technique because it takes place inside family homes and cars. I keep this in mind when I am reviewing applications and when they come up for renewal I expect to see evidence of intelligence obtained to help justify the continued operation. I am satisfied that:

- The agencies take great care to seek other less intrusive means before undertaking this level of intrusion and often consult their lawyers to ensure the legality of their submission;



- The warranting units at the Foreign Office, Home Office and Northern Ireland Office can and will question the agencies concerning the use and applicability of the suggested activity and they will not forward anything to the Secretary of State until they are satisfied. These units are an effective additional safeguard.

Finally I am satisfied that a Secretary of State will refuse any warrant if they are not convinced of the necessity and proportionality; they are aware that they are ultimately accountable for the operation.

## ii. Directed Surveillance Authorisation (DSA)

Directed Surveillance is surveillance which obtains private information in a covert but not intrusive manner. Part II of RIPA and the associated code of practice provide the legal framework for authorising surveillance activity which is compatible with Article 8 of the ECHR (please see the appendix to this report).

### Privacy

Directed surveillance is less intrusive but proper consideration must still be given to the necessity and proportionality of the activity. Specific consideration must be given to ensuring that the necessity of obtaining the information outweighs the intrusion of privacy.

### My overall assessment

From the submissions I have examined the applications to undertake directed surveillance have made out a proper case of necessity and considered properly whether any intrusion into privacy is justified and the extent justified. **There are however certain points to be made.**

- Duration and Combination

During 2014 I became concerned that there is more room for error when directed surveillance is required in combination with a property warrant. Legislation allows the Secretary of State to sign a combined property and intrusive surveillance warrant but when a DSA is required in combination with a property warrant the property warrant is signed by the Secretary of State but the DSA must be authorised separately by the agency. Additionally property warrants and DSAs have different duration periods which means that the warrants and authorisations have different renewal/cancellation deadlines.

It is easy to see how errors can be made and indeed were made when for example through an oversight a DSA authorisation was not obtained. I have **recommended** that if the legislation were to be amended there should be room for flexibility in issuing combined warrants and around the duration of warrants so that they can be combined and synchronised.

- Modification to DSAs

Directed Surveillance may be authorised against a particular terrorist operation because RIPA requires that it is "for the purpose of a specific investigation or a specific operation". The authorisations should thus make it clear what the expected outcome is for these thematic style surveillance operations and identify the targets, preferably by name.

MI5 appear to be diligent in modifying the authorisation to add or delete named individuals taking into account necessity and proportionality as and when they become involved in the investigation. However, from the paperwork provided to

me it is sometimes difficult to keep track of amendments in more complex and long running authorisations. MI5 has committed to looking at ways to improve the provision of inspection material such as moving to online systems rather than paperwork which will assist in the scrutiny process.

- Open Source Information

The increased use of the internet and social media among target groups has led to greater interest in open source internet data by the agencies. The law, including Article 8 of the ECHR, applies equally to online activity as to activity in the physical world and the agencies are obliged to comply with the law in relation to the collection of open source internet data just as much as to the collection of any other type of intelligence. The agencies recognise that the collection of open source internet data may be capable of amounting to directed surveillance if the statutory criteria are met and they are working to formulate clearer guidance on when the collection of open source internet data might amount to directed surveillance. I have asked to be provided with any such guidance.

### iii. Intelligence Services Act (ISA) – Property Interference Warrants

The Secretary of State under section 5 of ISA may issue warrants authorising MI5, SIS or GCHQ to enter into, go onto, or interfere with, property, or to interfere with wireless telegraphy. Property includes physical property and intellectual property. They are often referred to as property warrants. A property warrant may be used for remote interference with a computer in order to obtain information from that computer. It could also be used to authorise entry into or interference with a domestic residence for the purpose of concealing a listening device. In such cases they are used in conjunction with an intrusive surveillance warrant.

#### Privacy

These can be highly intrusive techniques and as such separate consideration must be given to limit any unnecessary intrusion into privacy and specifically the privacy of any family members or friends. A strong case must be made to explain why the information cannot be obtained through less intrusive means and that the necessity of obtaining the information outweighs the invasion of privacy.

#### My overall assessment

In the submissions for section 5 warrants which I have examined proper cases of necessity have been made and proper consideration has been given to avoiding unnecessary intrusion into privacy and limiting collateral intrusion. Such intrusion has also been justified by the necessity. **Once again however, there are points to be made.**

- Duration of Warrants

The legislation is ambiguous when it comes to dates from which warrant renewals run: it is possible to read ISA so that renewal of a property warrant begins on the day that the Secretary of State signs the renewal. For example if a warrant is issued on 16 March, its first day is 16 March and six months later it expires on 15 September i.e. 6 months less a day. If it is renewed at signing, on 7 September, its next period begins on the day of renewal [7 September] and runs for six months expiring on 6 March.

However, the code of practice for surveillance and property interference paragraph 7.40 states that renewal begins with the day it would have ceased to have effect but for the renewal. On this interpretation a warrant issued on 16 March and renewed on 7 September runs for 6 months from the date of the expiry 15 September to expire on 15 March.

According to the RIPA explanatory notes, RIPA s43(9) "clarifies the time from which a grant or renewal of an intrusive surveillance authorisation takes effect. It synchronises the duration of intrusive authorisations with those given for property



interference." This seems to support the code of practice understanding [see s43(9)(b)] but it remains unclear.

No harm is done if the first interpretation is being followed because renewal if anything is taking place early. But this lack of clarity is unhelpful so I have **recommended** that if the legislation were to be amended there should be greater clarity in the date from which warrants or authorisations run particularly following renewals.

- Thematic Property Warrants

I have expressed concerns about the use of what might be termed "thematic" property warrants issued under section 5 of ISA. ISA section 7 makes specific reference to thematic authorisations (what are called class authorisation) because it refers "to a particular act" or to "acts" undertaken in the course of an operation. However, section 5 is narrower referring to "property so specified".

During 2014 I have discussed with all the agencies and the warrantry units the use of section 5 in a way which seemed to me arguably too broad or "thematic". I have expressed my view that:

- section 5 does not expressly allow for a class of authorisation; and
- the words "property so specified" might be narrowly construed requiring the Secretary of State to consider a particular operation against a particular piece of property as opposed to property more generally described by reference for example to a described set of individuals.

The agencies and the warrantry units argue that ISA refers to action and properties which "are specified" which they interpret to mean "described by specification". Under this interpretation they consider that the property does not necessarily need to be specifically identified in advance as long as what is stated in the warrant can properly be said to include the property that is the subject of the subsequent interference. They argue that sometimes time constraints are such that if they are to act to protect national security they need a warrant which "specifies" property by reference to a described set of persons, only being able to identify with precision an individual at a later moment.

I accept the agencies' interpretation is very arguable. I also see in practical terms the national security requirement.

The critical thing however is that the submission and the warrant must be set out in a way which allows the Secretary of State to make the decision on necessity and proportionality. Thus I have made it clear:

- a Secretary of State can only sign the warrant if they are able properly to assess whether it is necessary and proportionate to authorise the activity
- the necessity and proportionality consideration must not be delegated

- property warrants under the present legislation should be as narrow as possible; and
- exceptional circumstances where time constraints would put national security at risk will be more likely to justify “thematic” warrants.

This has led to one of the agencies withdrawing a thematic property warrant in order to better define the specified property. We remain in discussion to find a way to do so but I am anxious to ensure that they are not missing intelligence opportunities which might endanger national security.

I made **five recommendations** at each of the intelligence agencies and warranting units in relation to what might be termed thematic property warrants:

1. For any warrants which might be considered to be thematic to be highlighted in the list provided for my selection;
2. The terms of a warrant and the submission must always be such as to enable the Secretary of State to assess the necessity and proportionality;
3. The assessment of proportionality and necessity should not be delegated;
4. Property warrants should be as narrow as possible but circumstances where time constraints and national security dictate may allow a more broadly drawn “thematic” warrant; and
5. As the agencies and the Secretaries of State have made clear to me is the case, thematic or broadly drawn warrants should not be asked for simply for administrative convenience.

I have **recommended** in general, and not just for thematic warrants, that the submission attached to the warrant should set out all the limitations applied to the use of the warrant and particularly should identify what action is being taken to minimise intrusion into privacy.

- Renewing Property Warrants

Although the legislation does not require it, when renewing a property warrant I have in the past said that the warrant renewal instrument should state that the Secretary of State still considers the activity to be necessary and proportionate. It is important that it is clear that the Secretary of State has applied their mind to necessity and proportionality when a warrant is renewed. Unfortunately however on occasion a shortened format renewal wording is still being used. This is something that I have said should be addressed.



## iv. Covert Human Intelligence Source (CHIS)

A CHIS is essentially a person who is a member of, or acting on behalf of, one of the intelligence services or MoD and who is authorised to obtain information from people who do not know that this information will reach the intelligence agencies or armed services. A CHIS may be a member of the public or an undercover officer. Part II of RIPA and the associated code of practice provide the legal framework for authorising the use and conduct of a CHIS which is compatible with Article 8 of the ECHR (please see the appendix to this report).

The agencies maintain an unshakeable commitment of confidentiality regarding the identity of CHIS which remains indefinitely. Revealing the role a CHIS has played could result in reprisals by a state or an organisation which could threaten the life of the CHIS or their family. In conducting my oversight and in scrutinising the authorisations this is an important consideration.

### My overall assessment of CHIS use and conduct

From the cases I have examined the applications for the use and conduct of CHIS have properly considered the necessity and proportionality and in particular considered possible invasion of privacy and the justification for this. **There are however, points to be made.**

- Duration of authorisations

During 2014 I noticed that some CHIS applications had been made for three months and some for twelve months. The code of practice suggests that an application for the use and conduct of a CHIS must be made for a twelve month period even if it is known at the outset that activity will only take place for a matter of days. I have suggested that under these circumstances, where it is arguable that it is neither necessary nor proportionate to issue for the full twelve month period, the agencies might consider issuing for a shorter period. However the convention at present is, and the code of practice would seem to support this, that warrants or authorisations be issued for the full period allowed and cancelled when no longer needed. It is argued that this allows a greater degree of certainty and simplicity in "policing" warrants and authorisations of a particular kind if they have the same lifespan. With this in mind I have **recommended** that authorisations should be for the full period but applications must be cancelled in good time as soon as it is known that they are no longer required.

- Undercover Operatives

The authorisation process for police undercover CHIS was amended on 1 January 2014 so that:

- authorised undercover operations must be notified to the Surveillance Commissioners as must their subsequent cancellation.

- a prior approval process by a Surveillance Commissioner is required for undercover operations employed by law enforcement agencies for longer than 12 months.

This did not extend to the intelligence services' or armed forces undercover officers' who have not had the same criticisms as the police (so have not been included in the various reviews or amended legislation). However, I have kept an eye on emerging recommendations. MI5 in particular has reviewed their policy and guidance and have improved their record keeping.

- MOD

It is not accepted by HMG that RIPA Part II applies to all relevant activity outside the UK but the MOD applies the principles and it is that application which I oversee. In the MOD CHIS authorisations are obtained and RIPA safeguards applied as if it did. In some applications for CHIS the paperwork focused on the privacy of the CHIS. I **recommended** that consideration must also be given to the privacy of the subject of investigation and any subsequent collateral intrusion. Having carefully questioned the MOD about this I am satisfied that full and proper consideration is being given to privacy so it just needs to be reflected in the paperwork.

- SIS

SIS is primarily a humint (human intelligence) organisation. They operate overseas under a section 7 class authorisation for agent running (CHIS). I have **recommended** that this is an area where SIS could improve their paperwork recording in one document all the relevant considerations relating to authorising a CHIS. I am satisfied that although RIPA does not apply, SIS seek to apply the same principles and that the relevant points are being considered in relation to authorising a CHIS. It would be better for operational reasons as well as from an oversight/compliance perspective if all relevant considerations were recorded in one document. When they have long term CHIS I have encouraged them to reconsider regularly whether the necessity and indeed proportionality case is still made out making it appropriate to continue tasking the CHIS.

- GCHQ

GCHQ is primarily a sigint (signals intelligence) organisation but they are able to undertake CHIS activity if it is in support of one of their statutory functions. I was content that GCHQ has systems in place to properly authorise and regularly review CHIS operations to ensure they remain necessary and proportionate and the authorisation remains justified.

- CHIS Reviews

In accordance with the code of practice CHIS activity must be kept under review to ensure that the use or conduct of the CHIS remains within the parameter of the extant authorisation because circumstances can change during the 12 month duration of the authority. The authorising officer should set the frequency of these

reviews. I have been concerned that these reviews are not always recorded as formally as they should be. In MI5 I have seen instances which imply that reviews have been ongoing even after tasking ceased so the "date reviewed" was clearly being automatically generated without a review taking place. This must not happen. In the new MI5 system, the authorising officer selects the review period and can comment on what they expect to see reviewed so the reviewing officer is required to manually populate the field to confirm that a review has taken place.

## **Conclusion**

The level of intrusion into privacy in CHIS operations is relatively low level. Consideration must be given to the privacy of the CHIS and also to the subject of the investigation. The safety and welfare of the CHIS is essential and I take this into account when conducting my oversight. In the cases I reviewed I have been satisfied that proper consideration has been given to necessity and proportionality. My primary concern has been the duration of authorisations which must be authorised for 12 months so I have made it clear that they must be properly reviewed and cancelled when no longer required.



(d)



# Report of the Intelligence Services Commissioner for 2013

---

CONFIDENTIAL ANNEX

The Rt Hon Sir Mark Waller

26<sup>th</sup> June 2014

Excluded from publication under section 60(5) of the Regulation of Investigatory Powers Act 2000



1

20



[REDACTED]

## 10. SECTION 94

There continues to be [REDACTED] s94 directions [REDACTED] of which have been reviewed previously. One was selected for Inspection which had not previously been reviewed.

The list set out

- the name of the communications provider
- when the direction was first served
- the date of previous inspection
- a brief description of the data provided under the direction

Although there is no formal mechanism in existence to cancel a Section 94 direction once it is in place, GCHQ inform both the CSP and the Minister when they cease to rely on it.

The directions are reviewed every six months and the relevant CSP is informed of the review (this is done in writing where possible but some CSPs cannot handle classified material).

S94 product can be stored for [REDACTED] but most is overwritten after a few [REDACTED]. Following a recommendation from the Interception of Communications Commissioner this is being reduced to a [REDACTED] storage period.



[REDACTED]

[REDACTED]

[REDACTED]

Not making a good case in the HRA justification may not mean that the action was not necessary and proportionate - It may just mean that the analyst has not set this out adequately.

There is an Information and Security Board which meets regularly to consider topics relating to Security.

Bulk Personal data is only a proportion of all operational data. Three minor breaches shown to the Commissioner did not relate to Bulk Personal Data but it was important for me to have the complete picture so as to be able to assess the effectiveness of the monitoring system.

• **HRA Audit**

Each use of GCHQ's IT system results in an invasion of privacy so the HRA justification must be completed. These justifications are audited and, if necessary investigated further by the compliance team. Saying something like "counter intelligence" is not acceptable; the analysts must set out in full why there is a requirement such as "believed to be a member of x involved in x".

I commented that this monitoring system seemed a good system. It is not an absolute guarantee but nothing could be absolute. MI5 and SIS treat any inappropriate access of personal data as a major breach and I recommended that GCHQ discuss with colleagues across the SIA to ensure consistency in approach.

[REDACTED]

individual(s) concerned. During the November 2014 inspection I was shown the results of an audit of these 'HRA justifications', which looked at a sample of several hundred queries. While some improvements needed to be made to a proportion of the justifications, **the audit did not find any evidence that any of the queries represented an inappropriate use of the data.**

Only a handful of GCHQ's bulk personal datasets are likely to contain data relating to UK persons or persons known by GCHQ staff, thus the motivation to misuse access is likely to be minimal. There is also the deterrent presented by GCHQ's protective monitoring of access to operational systems - knowledge of the existence of this monitoring is widespread, though details of specific monitoring capabilities are tightly controlled for security reasons. Automated monitoring of the tool in which most of GCHQ's bulk personal datasets are stored has been in place since late 2011.

- Safeguards

GCHQ apply RIPA Part I safeguards to all data which includes protection of Information of no intelligence Interest, when data can be deleted and protection of confidential information.

- Incident Management

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

not be possible to carry this across to another designation (post). I asked SIS to explain what they are doing to ensure this has not happened elsewhere.

SIS explained that in this case IT Admin re-set the officer's password, without going through the normal process which is in place to ensure that the requester is entitled to access. They do not believe that this officer was knowingly misusing the system. They hope this is an anomaly but are checking to see if it has happened elsewhere.

I tasked SIS to update me on this. I also want to see what they have done to ensure people are removed from the [REDACTED] register when they move post and what they are doing to ensure that IT Admin follow the correct procedure.

I was very firm in saying that unauthorised access to [REDACTED] must be stopped. The corporate failure in this case was a more serious breach than the misuse. [REDACTED] carries highly personal data and it is vital that staff only have access if they have a business need.

## Government Communications Headquarters

Use of bulk personal datasets is a relatively niche and small-scale activity for GCHQ, particularly compared to its use of material obtained via interception, but also when compared to its use of material obtained via CNE. Only a subset of GCHQ analysts have access to bulk personal datasets, and each of these staff will only have access to a subset of the datasets held by GCHQ, when those datasets are determined to be relevant to that analyst's operational targets.

All GCHQ analysts, including those with access to this data, have to complete mandatory legalities training, including a test, which reminds them of their legal obligations when examining any operational data – examination must be justified, necessary and proportionate.

For each query against a bulk personal dataset an analyst is required to briefly describe why they feel it is justified to intrude into the privacy of the

[REDACTED]

[REDACTED]

[REDACTED]

### DISCIPLINARY CASES

1	A query on a telephone number which was displayed on the user's desktop phone. The phone number turned out to be that of a colleague. The record was not entered.	Serious breach issued
2	A self search by a non-operational officer while on the [REDACTED] training course and the following day when they had returned to their desk.	The searches were to familiarise themselves with the system before going out to train [REDACTED] Serious breach issued.
3	A self search by a non-operational officer to retrospectively fill in a Personal Security Log with travel details following a vetting interview. Associates were also clicked on but were not entered into in any depth for system familiarisation.	Pending

The two serious breaches were a breach of the [REDACTED] code of practise and classed as serious security breaches on the individual's HR record. I agreed that, although the sanction appears tough because there was no invasion into privacy, the penalty was absolutely right because both officers had undertaken an inappropriate use of the [REDACTED] system. SIS assured me that they had undertaken an investigation of all other searches undertaken by both users and assured themselves that these were the only incidents.

SIS confirmed that they are following my recommendation to categorise [REDACTED] misuse as breaches. When a query is not necessary to the role and proportionate it is a case of serious misconduct.

I was concerned that the officer searching for the contact details of a relative had retained access to [REDACTED] despite changing designation. [REDACTED] access is determined by designation which places limitations on access to data. It should

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The majority of the current systems containing bulk personal data are subject to protective monitoring. Furthermore, all new systems containing bulk personal data are required to have protective monitoring included in them. Whilst some legacy systems do not have an automated protective monitoring capability, spot checks are undertaken

**Secret Intelligence Service**

I reviewed SIS's protective monitoring procedures. Access to [REDACTED] was restricted by individual user login. Giving personal login to someone else or leaving a system unattended are considered security breaches and subject to SIS's usual HR disciplinary procedures. The login is post specific so that (for example) an SIS officer working in the China team would not have access to the same information as the Russia team or staff in the security vetting team.

[REDACTED]

[REDACTED]

[REDACTED]

SIS also conduct manual random searches to query the justification for that search. They believe this is a strong audit which mostly focuses on breach of "need to know"

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The MI5 [REDACTED] team was created in 2009 and since that time have seen a change in culture which has resulted in a significant improvement in compliance. Over these years most cases were work related and had the best of intention but were still unacceptable. I have encouraged them to quote me if it helps make clear to people that there is no leeway. In 2014 there were no recorded instances of misuse of bulk personal data.

Protective [REDACTED] of other MI5 systems uncovered a number of other instances of misuse.

	Detail	Assessment
1	5 cases of staff forgetting to put parameters on their search [REDACTED]	All were issued with breach notices. [REDACTED]
2	1 officer searched for information which was outside of their area out of curiosity [REDACTED]	This was determined to be misconduct and will be on the officer's permanent record. [REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

MI5 ran through the outcome of these investigations in order to provide context and reassurance around the system of protective monitoring in place. While I have oversight of data relating to my statutory remit (Bulk Data, CHIS, DSA, and Property Warrants) I explained that seeing wider areas of protective monitoring helps me to have confidence in the system as a whole.

[REDACTED]

[REDACTED]





## 9. MISUSE OF DATA AND PROTECTIVE MONITORING

My oversight is limited to bulk personal data but I believe it would be helpful if I had oversight of all data obtained under the warrants/authorisations subject to my remit, including potential misuse of such data. Agencies do monitor the use of all data whether open source, targeted or bulk data holding and review the collection, retention and deletion of this data. Looking at misuse they have a mass of private information, a lot of it unused, so stringent rules need to be in place to check for and prevent misuse with strong disciplinary procedures for misuse. The chance that targeted data (from people of intelligence interest) would be misused is less but it is still personal data and it should not be accessed unless necessity can be demonstrated - there is no entitlement to misuse this data.

### Security Service

The use of bulk data within the Security Service is protectively monitored to both deter and identify inappropriate behaviour. In the event of inappropriate behaviour being identified, there are a range of disciplinary actions varying in severity that can be implemented. Furthermore, the Bulk Personal Data Review Panel (BPDRP) regularly reviews thematic issues arising from the use of bulk personal data; including consideration of usage where the necessity and proportionality might be judged marginal.

MI5's protective monitoring team explained that the message regarding misuse of data is getting through and the number of offences is on the decline. A note has been circulated to all users informing them of my recommendation endorsing MI5's policy to tighten up its procedures so that data on staff remains properly protected. The note introduced an automatic security breach if the procedures were not followed. There has not been a single breach in MI5 for access to Bulk Personal Datasets since that note was circulated.

[REDACTED]

## Government Communications Headquarters

Datasets held at the start year: [REDACTED]  
Datasets acquired in year: [REDACTED]  
Datasets deleted in year: [REDACTED]  
Datasets held at the end of year: [REDACTED]

GCHQ supply me with a complete list of the bulk personal data sets they hold. For those datasets I select for inspection they also supply me with copies of the minutes recording the justification for acquisition and the associated retention reviews which they carry out on a regular basis. I am satisfied GCHQ can justify retention of the data sets held by them.

GCHQ authorises the acquisition of each dataset before it is loaded into operational systems and retention of each dataset is reviewed by a panel of senior staff (including a lawyer) at least once a year (more frequently for more sensitive datasets). The business case for extended retention and the decision of the review panel are recorded in the paperwork relating to the specific dataset and this paperwork is presented to me for inspection. The majority of bulk data has historically been held on [REDACTED]

The case for renewal or cancellation includes:

- an assessment of the necessity and proportionality for retention
- how the data has been used
- an assessment of the benefits of the data and if these could have been achieved through other means
- the intelligence outcomes during this review period

The documentation was made available to me as were the minutes of GCHQ senior managers' regular reviews of BPD.

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

SIS agreed to revert to the relevant teams to make their case for retaining the datasets. If they want to retain the older dataset then they will have to prioritise this over newly acquired datasets. In future the relevant business area will take ownership of the datasets and provide the justifications.

SIS consider there to be three main causes for the delay in exploiting or deleting datasets:

1. Difficulties in accessing the data or difficulties in assessing the content of the data. [REDACTED]
2. The technical complexities for some datasets can cause delays in transforming them into a format that permits exploitation.
3. Delays in the authorisation process which requires six people to approve it. Of the [REDACTED] datasets, [REDACTED] fall within this category which may also have been caused by problems in the corporate IT system.

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

Since this muster SIS have put into place a tracking system with one officer as single point of contact [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- **Unexploited Datasets**

I asked SIS to chart any datasets acquired but not currently available for exploitation and was provided with two lists which showed that there were:

- [REDACTED] existing datasets which were also in this category six months ago
- [REDACTED] datasets which were not in this category at the previous inspection (new acquisitions)

The [REDACTED] older datasets should all have written justification from a senior officer or legal adviser while they are waiting to be authorised for exploitation into [REDACTED]. However, SIS could not find authorisations in the permanent record for [REDACTED] of these datasets and were taking immediate action to rectify this.

I expressed concern that there were [REDACTED] old and unexploited datasets; some dating back to 2005 and advised that SIS could not justify the necessity for retaining datasets if they have not been exploited within three years. SIS explained that one dataset was retained [REDACTED] which I accepted as a valid reason.

SIS have set up a project to deal with the old datasets and are aiming

- To authorise any dataset over 12 months for exploitation by May 2015
- To authorise any dataset over 6 months for exploitation by Nov 2015

All unauthorised datasets after this period will be deleted by the Data Review Panel unless an exceptional case for necessity is made. I instructed them to be ruthless in deleting old datasets

[REDACTED]

[REDACTED]

At the inspection SIS said that they strongly believe that this missing data is not down to malicious theft - there has been no leak to the media for example. A full search of media is underway with amnesty for any found and registered now.<sup>1</sup>

[REDACTED]

<sup>1</sup> SIS wish to make it clear that since this report, enquiries were conducted in respect of the 367 items referred to. The conclusion of those enquiries was that it was likely that the 367 items had been deleted. Furthermore, it became clear that not all the items were BPD. Some items were not BPD but other items of media held by the BPD team.



[REDACTED]

I asked if the justification box required consideration of proportionality. SIS explained that the box has a limited word count (300 characters) but staff are expected to give the operational context and the [REDACTED] team review what is written. Users also have to comply with the code of practice which explains that users have a responsibility to ensure enquiries are necessary and proportionate.

I enquired if the justification box could be changed - to include a human rights justification setting out if the invasion of privacy is justified. In my view the "justification" box did not accurately reflect the way in which SIS often ensure that intrusion into privacy is justified. That assessment is often done prior to an analyst actually conducting a search. Thus this box needs to reflect either that the analyst is satisfied the assessment has been made or that he or she has done the assessment themselves.

[REDACTED]

This muster has highlighted a weakness in the system by which they tracked media around the office and then destroyed it. Also the culture around the handling of classified media was not as strong as it should have been. As a consequence SIS were not able to account for all media in the service. Of the 2730 recorded items in their bulk data registrar, 367 are unaccounted for.<sup>1</sup> [REDACTED]

[REDACTED]

<sup>1</sup> SIS wish to make it clear that since this report, enquiries were conducted in respect of the 367 items referred to. The conclusion of those enquiries was that it was likely that the 367 items had been deleted. Furthermore, it became clear that not all the items were BPD. Some items were not BPD but other items of media held by the BPD team.

[REDACTED]

SIS staff have access to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The training explains that users have personal responsibility for any search undertaken. Managers are responsible for ensuring that staff read and sign the code of conduct. This explains that BPD needs to be managed to ensure that the privacy of those whose data is held is respected and that data is held, accessed and disclosed only to the extent necessary for the purpose of the statutory functions and proportionate to those aims.

When undertaking a search SIS must now complete mandatory fields setting out:

- Purpose of the search
- Justification (business need relating back to an intelligence report, sigint etc)
- Free text box

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

The Security Service have access to data sets through:

[REDACTED]  
[REDACTED]

Access is also limited by post so when an officer changes role their access to datasets is likely to change as well.

[REDACTED]

indicate which system(s) they wish to search. RIPA product is also on this system. [REDACTED] does not supply all information at once so the analyst has to consider if further information is needed. They do not have a justification box or field to complete before they undertake a search of [REDACTED] but prior to being granted access to the system they must undergo training and they are expected adhere to the code of practice. Individual analysts will record the necessity and proportionality given to them by the investigator. The Security Service relies on the integrity of their staff. MI5 has also a strong monitoring system.

[REDACTED]  
[REDACTED]

### Secret Intelligence Service

For the calendar year 2014:

Datasets held at start of year	[REDACTED]
Datasets acquired in year	[REDACTED]
Datasets deleted in year	[REDACTED]
Datasets held at end of year	[REDACTED]

Within SIS most bulk personal data sets are available to users through a system called [REDACTED]. A few datasets are stored on standalone systems and not available to [REDACTED] users but can be searched separately. Each data set is authorised separately before input onto [REDACTED]

[REDACTED]



### 3. BULK PERSONAL DATA

On 12 March 2014 the Prime Minister published a direction which put my continued oversight of bulk personal data on a statutory footing.

On 14 October 2010, the Prime Minister wrote to my predecessor, Sir Peter Gibson, setting out a proposed framework for ongoing oversight by the Commissioner on an extra-statutory basis, in respect of the acquisition, retention and deletion of bulk personal data holdings and in respect of the access to and use of such data.

I have set out my oversight of bulk personal data in as much detail as I can in my open report this year.

#### Statistics

Bulk Personal Datasets	SIS	MI5	GCHQ	Total
Held at the start of 2014	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Acquired in year:	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Deleted in year	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Held at the end of year	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

#### Details of my Oversight of Bulk Personal Data

##### Security Service

Datasets held at the start of year: [REDACTED]  
 Datasets acquired in year: [REDACTED]  
 Datasets deleted in year: [REDACTED]  
 Datasets held at the end of year: [REDACTED]

MI5 provided me with a summary of how each of the datasets are used. I had no difficulty with the justification for retention of datasets so I have concentrated on the use of the data.





[REDACTED]

## 2. ADDITIONAL FUNCTIONS

Under paragraph 59A of RIPA, inserted by the Justice and Security Act, the Prime Minister may direct me to keep under review the carrying out of any aspect of the functions of the intelligence services.

The Prime Minister has now issued three such directions placing all of my oversight on a statutory footing. Two of the directions are set out in my open report:


- the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets including the misuse of data and how this is prevented
- compliance with the Consolidated Guidance.

[REDACTED]

### Section 94

GCHQ asked my predecessor to oversee the activity of GCHQ in relation to data acquired by means of directions given by the Secretary of State under section 94 of the Telecommunications Act 1984. During 2014 I continued to oversee GCHQ's use of section 94 directions in a similar way to my oversight of bulk personal data. However, in January 2015 the Interception of Communications Commissioner was asked and has agreed to formally oversee directions under section 94.

[REDACTED]



**Report of the  
Intelligence Services  
Commissioner for 2014**

---

**CONFIDENTIAL ANNEX**

**The Rt Hon Sir Mark Waller**

**June 2015**

Excluded from publication under section 60(5) of the Regulation of Investigatory Powers Act 2000