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

50100_HC 225 Intelligence Services Commissioner.indd 1 24/06/2015 12:43

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

50100_HC 225 Intelligence Services Commissioner.indd 3 24/06/2015 12:43

OGL

© 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 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: 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

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

50100_HC 225 Intelligence Services Commissioner.indd 5 24/06/2015 12:43

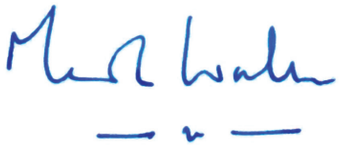
The Rt Hon Sir Mark Waller
Intelligence Services Commissioner
2 Marsham Street
London
SW1P 4DF

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.



The Rt Hon Sir Mark Waller

50100_HC 225 Intelligence Services Commissioner.indd 1 24/06/2015 12:43

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.[1] See Chapters 4.vi and 4.vii of this report for more detail about how I oversee these activities.

1 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

50100_HC 225 Intelligence Services Commissioner.indd 2 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 3 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 4 24/06/2015 12:43

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

50100_HC 225 Intelligence Services Commissioner.indd 5 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 6 24/06/2015 12:43

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

50100_HC 225 Intelligence Services Commissioner.indd 7 24/06/2015 12:43

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 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.

50100_HC 225 Intelligence Services Commissioner.indd 8 24/06/2015 12:43

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

Selection

I select from a list of all warrants and authorisations provided by the agencies which are current or were cancelled during the six months prior to my inspection. The list includes a brief description of what each is about.

Pre-Reading

All selected cases with supporting documentation are available. I scrutinise and review the necessity and proportionality of the operation paying particular attention to whether any intrusion into privacy has been justified. I am supported by my Head of Secretariat who ensures that the proper administrative procedures have been followed.

Formal Inspection Visit

During my inspections, I am briefed on current operations and I follow up on any points arising from my pre read or errors reported to me. I question intelligence officers and senior personnel to ensure they can justify their activity

Under the Bonnet Inspection

In these follow up inspections, which 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 activities specified in any warrant or authorisation.

50100_HC 225 Intelligence Services Commissioner.indd 9 24/06/2015 12:43

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:

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 (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:

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

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

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

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.

50100_HC 225 Intelligence Services Commissioner.indd 10 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 11 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 12 24/06/2015 12:43

- 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;

50100_HC 225 Intelligence Services Commissioner.indd 13 24/06/2015 12:43

- The warrantry 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.

50100_HC 225 Intelligence Services Commissioner.indd 14 24/06/2015 12:43

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

50100_HC 225 Intelligence Services Commissioner.indd 15 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 16 24/06/2015 12:43

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

50100_HC 225 Intelligence Services Commissioner.indd 17 24/06/2015 12:43

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

50100_HC 225 Intelligence Services Commissioner.indd 18 24/06/2015 12:43

- 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 warrantry 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.

50100_HC 225 Intelligence Services Commissioner.indd 19 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 20 24/06/2015 12:43

- 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 re-consider 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

50100_HC 225 Intelligence Services Commissioner.indd 21 24/06/2015 12:43

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.

50100_HC 225 Intelligence Services Commissioner.indd 22 24/06/2015 12:43

v. Intelligence Services Act (ISA) section 7 authorisations

ISA section 7 is intended to ensure that certain activity of SIS and GCHQ overseas, which might otherwise expose their officers or agents to criminal or civil liability in the UK, is exempt from any liability if 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. Under section 7 of ISA the Secretary of State (normally the Foreign Secretary) may authorise activity outside of the United Kingdom necessary for the agencies to properly discharge one of their functions. Authorisations may be for a particular operation or may relate to a broader class of operations. Before granting an authorisation the Secretary of State must be satisfied of the necessity and reasonableness of activity to be authorised. In this context reasonableness includes acting so as not to intrude on privacy any further than justified by the necessity to achieve what is authorised.

Privacy

Section 7 authorisations can be used for highly intrusive activities. Some operations under section 7 class authorisations are conducted under internal authorisations. To obtain an internal authorisation a case has to be made of necessity and proportionality for the intrusion into privacy. These are principles applied and accepted to apply whether or not the Convention on Human Rights or the Human Rights Act strictly applies. In other words anyone seeking authorisation to conduct a particular operation must make a strong case explaining why:

- less intrusive means cannot be used; and
- the necessity of obtaining the information outweighs the invasion of privacy.

Assessment of ISA section 7 authorisations use

There are two aspects of my oversight in this area. Firstly the grant of a section 7 and secondly internal approvals under that authorisation.

Oversight of the granting of a section 7 authorisation

Section 7 authorisations fulfil two functions. First they will relieve the officers acting in accordance with the authorisation from liability under UK law. Second they provide political approval of activities carried out under such an authorisation.

Some Non-Governmental Organisations have expressed concerns about the broad nature of section 7 authorisations and the fear that they may be used to permit SIS or GCHQ to commit serious offences. This is not the case:

- firstly the process for establishing the necessity of the intelligence required by the government and the priority for this is set for the agencies by government. The agencies do not self-task and must justify everything they do in relation to government priorities.

50100_HC 225 Intelligence Services Commissioner.indd 23 24/06/2015 12:43

- secondly it is the Foreign Secretary who decides if the proposed operation is both necessary and reasonable. The Foreign Secretary is accountable to Parliament for the actions of both SIS and GCHQ.

Thirdly as I said in my report for 2013, GCHQ and SIS staff have no desire to operate unlawfully. In both SIS and GCHQ legal compliance is an integral part of the culture, but they do need protection for activities carried out abroad so far as section 7 can give it.

An application to the Foreign Secretary is accompanied by a submission which sets out the planned operation, the potential risks and intended benefits. They usually include a comprehensive legal annex and most importantly from my perspective, includes why any intrusion into privacy is justified by the intelligence sought to be obtained. These applications are submitted through the Foreign Office who provides additional comments for the Foreign Secretary to consider. The Foreign Office are also accountable to me for any decisions they take and I am satisfied that they can and do refer applications back to the relevant agency if they are not satisfied about any aspect of the proposal.

Class Authorisations

Class authorisations cover the essential and routine business of SIS and GCHQ. Again they fulfil two functions. First they give protection for liability under UK law and second they provide political approval for activities authorised by the class authorisation.

I oversee the use of section 7 authorisations by visiting GCHQ and SIS and the warrantry unit of the Foreign Office. But SIS is tasked with operating overseas, dealing with threats and gathering intelligence in order to protect the UK and UK interests, and an important element of my SIS oversight is to visit and scrutinise certain of the overseas stations in which they operate. On these visits I have two main priorities:

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

In all my visits I have been impressed at the dedication of the officers and by their evident desire to act in accordance with high ethical principles. This in fact goes for all those that work for the agencies and the MOD whether home or abroad.

- SIS Internal Approvals

For each operation there is a controlling officer in the UK who is in constant communication with the overseas station.

50100_HC 225 Intelligence Services Commissioner.indd 24 24/06/2015 12:43

Although RIPA does not apply to the majority of SIS activity overseas, in overseeing the internal use of class authorisations I look to see that the principles are applied. I do this by:

- looking at the audit trail setting out the thought process, in large measure recorded in e-mails with the controlling office in Head Office; and
- checking the necessity and proportionality of activity taking place.

I have **recommended** that SIS implement a better audit trail of operations taking place similar to the RIPA procedure used in the UK. This would allow for improved accountability for the work and allow greater oversight by management as well as by me as Commissioner. I am confident that proper consideration is given to the necessity and proportionality from my interviews and the e-mail trail but it is not currently possible to see this set out in one document and can be a time consuming process to find.

I have also **recommended** that when I visit stations overseas I am provided with the stations' operational objectives, priorities and resources to help reassure me that all of the work undertaken is properly authorised and in support of their statutory functions.

- GCHQ Internal Approvals

GCHQ primarily operate under class authorisations and have very few specific section 7s. They provide for my oversight the internal approvals they make under each class authorisation and have implemented my **recommendation** to ensure that the paperwork reflects that these approvals are only valid as long as the class authorisation is in place. They are approved by a GCHQ senior official but if there is any additional sensitivity or political risk it will only be signed after a senior Foreign Office official or the Foreign Secretary has been consulted and agreed the operation is appropriate. I have made it clear that the senior official cannot authorise necessity and proportionality; this decision must be made by the Secretary of State and cannot be delegated.

GCHQ's internal approvals are supplemented by what they call an "addition". To help me to gain a better understanding I spent a day in GCHQ:

- looking more closely at the system;
- questioning the staff who undertake the approvals; and
- questioning the staff who undertake the activity.

I wanted to be clear what consideration was being given to protecting privacy at each stage of the process and what was done with any product obtained. I stressed to them the importance I place on filters which help avoid any unnecessary intrusion.

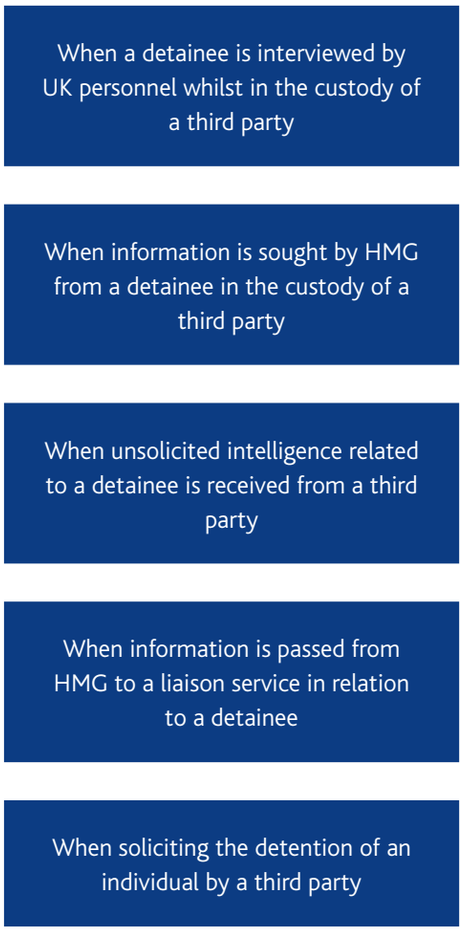
50100_HC 225 Intelligence Services Commissioner.indd 25 24/06/2015 12:43

I was impressed with the formality of the audit trail and the level of consideration; it was clear to me that a great deal of thought was going into assessing the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible. In future I **recommended** that these additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ.

50100_HC 225 Intelligence Services Commissioner.indd 26 24/06/2015 12:43

vi. Consolidated Guidance

Figure 5: Areas subject to my oversight include:



On 27 November 2014, under section 59A of RIPA, the Prime Minister published a direction which put my oversight of 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 (the Consolidated Guidance) onto a statutory footing. The Consolidated Guidance sets out principles that UK intelligence and security agency officers and members of the UK Armed forces and employees of the Ministry of Defence must adhere to when they interview detainees overseas or pass and receive intelligence relating to detainees.

How I oversee the Consolidated Guidance

I oversee the Consolidated Guidance during my formal inspections of the agencies. I follow the same method to review the Consolidated Guidance as I use for other areas within my remit. Further detail on how I fulfil my oversight can be found in my 2013 Annual Report.

My objective is to ensure that intelligence officers and military personnel are aware of and follow the Consolidated Guidance so that when they are faced with situations which involve detainees, they are able to apply the Guidance and take decisions at the correct level. I do this by:

- reviewing the "detainee grid" which sets out the date, details of occasions when the agencies have assessed that there may be a need to apply the Consolidated Guidance or where the Consolidated Guidance has been applied including the operation/overarching submission, risk assessment, reference to senior personnel, legal advisors or Minister and the level at which the decision was taken.
- reviewing the audit trial which demonstrates that operational staff engaged in detainee matters are following the Guidance.
- ensuring that the agencies are providing the appropriate levels of assurance to me and Ministers that the Guidance is being followed.

50100_HC 225 Intelligence Services Commissioner.indd 27 24/06/2015 12:43

Developing the Grid

Cases of the Consolidated Guidance which fall within my remit[2] are set out for me in a grid format for me to select from. The grid has developed over the years but my preference is that it sets out what liaison country and liaison service is involved and then reflects under headings the following questions:

- Are you passing information relating to an existing detainee?
- Is this a detention request or is detention the likely outcome?
- Are you attending the interview of detainee?
- Will information be put to a detainee?
- Is information to be derived from a detainee?
- Is there serious risk of mistreatment?

The grid will also set out for me who was consulted, the level the decision was taken and a narrative of the action taken.

This format directs people through the consolidated guidance process and if all the answers are "no" then the guidance needs no further consideration. I have **recommended** that, rather than sticking to a strict date order, operations should be grouped together so that I can review every occasion it has been considered.

I select a random sample of cases for closer scrutiny although in doing so I try to ensure that I select different foreign liaison services as well as different decision levels.

During my inspection I review the detainee grid in relation to the cases I selected to ensure that the grid has been completed accurately. If it has then I believe I can be assured that the consolidated guidance process is being followed in all cases.

In my report for 2013 I **recommended** to SIS that they ensure they capture all cases in stations overseas where consideration was given as to whether the guidance applied even if a decision was taken ultimately that it did not. They implemented an email system of selection. This ensured that I could also see cases where the guidance was considered and a decision taken either that the guidance was not engaged or that intelligence was not to be shared. However at the start of 2014 I **recommended** to SIS that they consider how this method of selection could be more formalised. SIS responded to this by converting their emails from the group email box into a grid format. This was an improvement with both the benefit of the grid and the flexibility required for a global organisation but I **recommended** that they set out their grid in my preferred method.

2 The areas that fall within my remit are set out in full on my website and in the Prime Minister's direction in the appendix to this report. It does not relate to people in the custody of the UK.

50100_HC 225 Intelligence Services Commissioner.indd 28 24/06/2015 12:43

I also **recommended** to GCHQ and MI5 that they reformat their grid so that it reflected in more detail the level that the decisions were taken.

Form

To support the grid both MOD and MI5 have very useful forms in terms of the way they force consideration of the relevant questions. These forms are also available for my inspection. I have **recommended** that GCHQ and SIS consider having similar forms.

Liaison Relationships

An important part of my oversight of the guidance relates to the risks associated with working with overseas liaison partners and how the agencies mitigate against any risk. In November 2014 the Prime Minister tasked me to examine the concerns the ISC raised on the government's responsibilities in relation to partner counter-terrorism units overseas. As part of this inquiry I am seeking to establish whether the procedures now in place address the concerns of the ISC. I will report on this further when my inquiry is complete.

During station visits I am briefed and discuss with intelligence officers their work with liaison partners. This is a highly sensitive and complex area in which to operate. The obtaining of assurances upon which, for example, decisions around the passing and receipt of intelligence in relation to detainees are often based is vital as is the assessment of the extent they can be relied on.

During my inspections I have asked the agencies to inform me about significant developments in knowledge or belief that mistreatment has occurred. I have asked that these developments are recorded to help build up a record of behaviour with the liaison service. This is already covered by SIS's compliance work within the Consolidated Guidance.

Due Process

On occasion there may be cases where there is a greater than serious risk of a detainee being denied due process. Individuals must be allowed access to a lawyer and be given the opportunity to appear before a judge and ultimately have a fair trial. As part of the country assessment it is important to understand what legal system is in place and a qualitative assessment made of whether the system will be followed. I have **recommended** that as well as recording the specific assurances sought, there should be an assessment of whether it is likely that the liaison service in question will comply with those assurances.

Assurances

I have emphasised the importance of obtaining signed written assurances from the foreign liaison but failing that to provide liaison with a written record of the assurances provided verbally. It is obviously preferable to obtain signed written assurances but if this is not possible I have **recommended** that assurances must

50100_HC 225 Intelligence Services Commissioner.indd 29 24/06/2015 12:43

be recorded in writing and sent to liaison as a preference to relying on verbal assurances.

Sharing intelligence *in extremis*

Paragraph 12 of the Consolidated Guidance allows for time sensitive military operations which involve questioning a detainee held by another liaison partner when time constraints do not allow the opportunity to apply the Guidance in advance. In such circumstances they must apply the Guidance "so far as it is practicable" and report to senior personnel as soon as possible. The Guidance does not have some general provision allowing for example the sharing of intelligence in extremis situations where lives are at risk.

MOD brought a situation to my attention which involved sharing intelligence with foreign liaison during a time sensitive operation when there were lives at risk. There was no opportunity to refer to senior personnel or Ministers for guidance on any concerns over standards of detention or treatment so a decision had to be taken by the most senior person present. I consider there to be an oversight in the Guidance which does not allow for a more general application of such a principle. I **recommend** that the Consolidated Guidance be amended to allow for in extremis sharing of intelligence.

Informing Liaison that no intelligence was held

On occasion the intelligence agencies receive trace requests from liaison partners seeking information about individuals already in their detention or who are judged likely to be detained. The question has arisen as to whether a 'no trace' reply was the passing of intelligence to which the Guidance applied. If the Guidance applied that might lead to a person being continued to be detained while authorisation was sought for making such a reply. In such circumstances I have said a 'no trace' reply was not 'passing of intelligence' to which the Consolidated Guidance applied.

Statistics

In my report for 2013 I published statistics for the first time indicating the number of occasions when the Consolidated Guidance has been applied and the extent of my checking. When I did so I explained that the figure can easily be misrepresented both 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 I would continue to give these figures, but with strong warning against misrepresentation.

The total number of cases where the Consolidated guidance was considered during 2014 was 516. I have full details of all 516 including what decision was taken and by whom. The statistics do not show the number of individuals subject to unacceptable conduct; only that proper consideration was being given to that risk in a number of cases.

50100_HC 225 Intelligence Services Commissioner.indd 30 24/06/2015 12:43

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 should be considered and that decisions are then taken at the correct level. I do this scrutinising by the grid setting out the way in which the Guidance was applied in the 516 cases and taking a random sample to cross check that the information with which I am being supplied is accurate. That sample was 64 ie 12.5% of the 516 cases.

Conclusion

In all the instances I reviewed staff demonstrated they had considered the risk of mistreatment or unacceptable conduct of any detainee as set out in paragraphs 9 – 11 of the Consolidated Guidance. I found that the grids presented to me had been completed properly.

Because SIS staff work with overseas liaison they have a more difficult role to play and are most likely to have to consider Consolidated Guidance issues. They will work with liaison to help mitigate risk of mistreatment and seek signed assurances that detainees will be treated in accordance with those assurances. GCHQ, MI5 and the MOD may rely on SIS in relation to country assessments and assurances. I noted that SIS record keeping for Consolidated Guidance issues has improved. Their new system for selection captures cases where the Guidance has been considered even when it does not apply. Senior managers in SIS are keen to see record keeping improve and have agreed to talk to overseas staff about this.

50100_HC 225 Intelligence Services Commissioner.indd 31 24/06/2015 12:43

vii. Bulk Personal Data

On 12 March this year, under section 59A of RIPA (as inserted by section 5 of the Justice and Security Act 2013), the Prime Minister published a direction which continued and 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. Essentially I oversee how the intelligence services store and use bulk personal data (BPD).

There is no statutory definition of BPD, but in essence BPD refers to data belonging to a range of individuals acquired by or held on one or more analytical systems in the intelligence services. The majority of these individuals are unlikely to be of intelligence interest. I consider the most important aspect of my role is to see that the agencies have systems in place to protect privacy of those individuals.

Acquisition and Retention of Bulk Data

Section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 provide, in effect, that the intelligence services may only obtain information for the proper discharge of their functions.

In addition, section 19 of the Counter-Terrorism Act 2008:

- allows a person to disclose information to any of the intelligence services for one of those functions;
- permits information they obtain in connection with one function to be used by the intelligence services in connection with any of their other functions; and
- provides that disclosing information to the intelligence services overrides any duty of confidentiality or other restriction on disclosure.

The Head of each agency is responsible for ensuring that no information is obtained or disclosed unless it is necessary for the proper discharge of its functions.

So far as BPD is concerned each dataset is separately authorised before it is made available on analytical systems for use by intelligence officers. The authorisation sets out the necessity and proportionality argument for exploiting the data and considers any sensitive data which might be included in that dataset.

The agencies assess each dataset individually including:

- a statement of necessity for retaining the dataset,
- an assessment of intrusion into privacy,
- measures to minimise intrusion into privacy.

50100_HC 225 Intelligence Services Commissioner.indd 32 24/06/2015 12:43

The agencies each have a review panel of senior managers who meet regularly to review:

- the retention of datasets,
- the decision to ingest any new dataset into analytical systems,
- examples of its use during any previous period,
- the decision to delete datasets.

Some datasets have very little private data or even publicly available data in them so the justification for retention is much easier as long as the dataset is still being used and contributing towards the aims of the organisation. Other datasets may contain intrusive data and any containing sensitive confidential data should be flagged.

Data Protection Act

Each agency recognises that the acquisition, retention, exploitation and disclosure of personal data about individuals constitutes "processing" for the purpose of the Data Protection Act (DPA). Any such processing of personal data therefore has to be considered under the DPA. However, the processing involved in the acquisition, disclosure and exploitation of personal data is exempt from specific provisions of the DPA where such exemption is required in order to safeguard national security. In such cases a Minister of the Crown may issue a certificate under section 28(2) of the DPA, confirming that the exemption under 28(1) is required, such a certificate being conclusive evidence of that fact. In accordance with section 28(3), the ministerial certificate may identify the personal data to which it applies by means of a general description and be prospective in its effect. The agencies' certificates effectively provide exemption from the 1st, 2nd, 6th and 8th Data Protection Principles (DPPs). In summary:

50100_HC 225 Intelligence Services Commissioner.indd 33 24/06/2015 12:43

DPP		
1st	Personal data shall be processed fairly and lawfully	EXEMPT
2nd	Personal data shall be obtained and processed only for specified and lawful purpose	EXEMPT
3rd	Personal data shall be adequate, relevant and not excessive in relation to the (statutory) purpose for which they are processed	NOT EXEMPT
4th	Personal data shall not be kept for longer than is necessary for the (statutory) purpose for which they are being processed	NOT EXEMPT
5th	Personal data shall not be kept for longer than is necessary for the (statutory) purpose for which they are being processed	NOT EXEMPT
6th	Personal data shall be processed in accordance with the rights of the data subject	EXEMPT
7th	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data	NOT EXEMPT
8th	Personal data shall not be transferred outside the European Economic Area unless the relevant country ensures an adequate level of protection for the rights of the data subject	EXEMPT

It is also still open to the agencies to argue on a case by case basis that exemption from one or more of the DPPs was required in order to safeguard national security.

How I oversee Bulk Personal Data

In summary I oversee BPD in a number of ways.

- first I require the services to provide me with a full list of all datasets they hold. I see the records of the internal review bodies which consider the retention of datasets. I inspect these documents along with the formal justification for acquiring the dataset and making it available for use on analytical systems. I assess whether the review bodies have properly applied the test of necessity and proportionality in retaining and making the data available.
- I then inspect how members of the intelligence services access the data sets including the training required before gaining access and restrictions in place to limit access as well as reviewing how they apply the necessity and proportionality justifications of intrusion into private information.
- finally I review the possible misuse of BPD and how this is prevented. This is a key part of my oversight. Access to BPD must be tightly controlled and

50100_HC 225 Intelligence Services Commissioner.indd 34 24/06/2015 12:43

what must be guarded against is the risk that some individuals will misuse the powers of access to private data.

As part of my oversight I ask for an explanation of how the datasets I select for closer examination are used. In general I have no difficulty with the justification for retaining the datasets. In essence the justification will be that although the particular dataset has information on individuals of no intelligence interest it will also have important information on persons who will be or are of intelligence interest and which will provide important links assisting in the identification or movements of those individuals.

It is important I stress that the acquisition of datasets can be justified on the basis that it is necessary and proportionate to have them. Thus for example, in SIS with two linked older datasets I had concerns that they had acquired them for one reason and now wished to use them for another. I have required SIS to:

- provide me with justification for the necessity and proportionality for continued retention; and
- keep the datasets locked up until/unless their data review panel approve their continued use and I have had a chance to review that decision.

Training

Before officers are allowed access to BPD they must undergo formal training and in MI5 agree to and sign a code of conduct. The training explains that users have personal responsibility for any use of the system and managers are responsible for their staff. The code of conduct 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 of the agency and where it is proportionate to those aims.

This standard is reflected at the other two agencies without a formal code of conduct.

Use

The agencies have systems in place to ensure that BPD cannot be trawled indiscriminately by analysts. Access to BPD is restricted by individual user login. If an officer gives their personal login to someone else or leaves their system unattended this is considered a security breach and subject to disciplinary procedures. The login is post specific.

Before an individual analyst is allowed access to BPD GCHQ have a system in place which requires them to justify the necessity and proportionality of their proposed search. This justification box is audited regularly and available to me for inspection.

50100_HC 225 Intelligence Services Commissioner.indd 35 24/06/2015 12:43

SIS have also introduced a system where officers have to complete mandatory fields setting out the purpose of the search and justification for the search (business need) in the free text box.

I was pleased to see that SIS implemented a system but was not satisfied that it prompted the user to consider if the anticipated invasion into privacy would be justified by the desired outcome. I have **recommended** that they amend the fields to reflect how a decision is made, that access to the BPD and possible intrusion into privacy is justified.

MI5 does not use a "justification box" but require their analysts to adhere to their internal policies and guidance which require that searches must be necessary and proportionate for the business they are conducting. Adherence to policy is in part achieved by user training, signing a code of conduct and their protective monitoring regime. BPD access is also restricted to staff who have a valid business reason to use BPD.

During my selection of SIS's bulk data I had particular concern about datasets which had been obtained but not yet put onto analytical systems. I required SIS to provide me with a list of all datasets they had acquired but were not currently exploiting including the date they acquired each dataset. SIS provided the list on the inspection day along with an explanation of each dataset. I made clear that SIS cannot justify the necessity for retaining datasets if they have not been exploited within a reasonable period and **recommended** that they should be deleted unless an exceptional case for necessity can be made. This is a point which I have also taken up with GCHQ and MI5.

Each agency has a limited number of specialist analysts who can perform more detailed searches by reference to particular datasets, but again they are subject to the same policy, guidance and safeguards such as through protective monitoring of their enquiries. I take into account this advanced ability to search datasets when I scrutinise their use of BPD.

Protective Monitoring of BPD

In my oversight of BPD I monitor extremely carefully the steps taken to see how the misuse of BPD is prevented.

Access to BPD is audited through a system of protective monitoring by all agencies. To provide me with confidence in the system as a whole I do not limit my oversight of protective monitoring to BPD so I scrutinise details of general misuse of information and security breaches.

In all three services there is an automatic monitoring system which uses predefined search terms as well as random audits of individual users. I scrutinise these search terms and the results of the audit as part of my oversight. Obviously it would be

50100_HC 225 Intelligence Services Commissioner.indd 36 24/06/2015 12:43

inappropriate to give details of the way the monitoring works in a public document. Queries arising from these audits were primarily "false positives"; that is although they initially met a search term designed to catch misuse there is, on investigation, a fully justified explanation for their use in each case.

Misuse of Bulk Data

The agencies take any deliberate misuse of the system seriously and sanctions include dismissal, revocation of security clearance and possible criminal prosecution. Any breach of the system may result in a breach notice being issued. When a breach notice is served it remains on a person's personnel file (HR record) and is taken into account in the event of any subsequent breach.

When I first began monitoring misuse of data there were two serious breaches where officers had undertaken unnecessary queries of bulk data with no proper business justification. Both were contractors and in both cases, following investigation they were escorted from the premises and their contract revoked. Fortunately such action is rare but I am very clear that the agencies accept that any inappropriate use is unacceptable and will be treated very seriously.

Unacceptable uses are in fact few in number and not as serious as the cases referred to. For example well intentioned work-related instances such as failure to properly limit the parameters of a search are treated as serious breaches and I have made it clear that this it is absolutely right that that should be so.

In MI5 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 BPD since that note was circulated.

In one recent instance of misuse in SIS an officer accessed the BPD system despite having moved to another role which did not require access. The access was for a legitimate work purpose but still unacceptable and a breach notice was issued. However, I informed SIS that the corporate failure which allowed the officer to retain access to the system was a more serious breach.

BPD systems hold highly personal data and it is vital that staff only have access if they have a business need. The officer should not have been able to retain access to the system after moving post so I have asked SIS:

- to investigate if any more staff have access bulk data when they do not have a business need and to update me on this investigation;
- to inform me what has been done to ensure people are removed from the bulk data register when they move post.

50100_HC 225 Intelligence Services Commissioner.indd 37 24/06/2015 12:43

I have **recommended** to all three intelligence services that they work together to treat all misuse of data in the same way to ensure fairness to all staff.

Conclusion

The case for holding BPD has been established in each service. The data review panels consider and regularly review the necessity and proportionality of retaining data. They also recommend deleting any datasets which cannot be justified for retention. When datasets are acquired there is a good system in place to consider if the dataset should be incorporated into analytical systems and made available to users.

The agencies all have strict procedures in relation to handling, retention and deletion.

Misuse of data is fortunately rare. My experience is that officers work with a high degree of integrity and an awareness that the systems they have access to contain highly sensitive information which must be protected.

Access to information held on BDP must be justified so the vast majority of data the agencies acquire is not used because no case can be made justifying access to it.

I have made a number of recommendations relating to the agencies use, retention and protective monitoring of BPD. Most of these recommendations have related to improving privacy considerations or protecting individual privacy.

50100_HC 225 Intelligence Services Commissioner.indd 38 24/06/2015 12:43

5. PRODUCT OBTAINED AND HANDLING ARRANGEMENTS

This chapter is concerned with product obtained through warrants or internal authorisations.

I have noted that submissions often state that "normal procedures" would be adopted for handling any product obtained. However, unlike the Interception of Communications Commissioner I do not have express oversight of these arrangements. With this in mind in the confidential annex to my report for 2013, using the power given to me under RIPA s59A(3) I asked the Prime Minister to extend my oversight to the use by the agencies of operational data obtained under Part II of RIPA or ISA sections 5 and 7. I have repeated this request this year but in the mean time I consider that on a broad reading of my remit I can and should oversee at least the retention storage and deletion of product obtained from those warrants and authorisations which fall within his remit.

I am considering how I can oversee the agencies compliance. Taking into account the existing statutory oversight undertaken by the Interception of Communications Commissioner I will particularly focus on:

- the retention policy for information which is not of intelligence interest (which should by preference be immediately destroyed);
- the procedure used to handle information retained for evidential purposes which could include information which is not of intelligence interest;
- the procedure to handle unwanted information so that submissions would not need to set this out each time; they could simply refer to the policy;
- the policy for deletion of all product; and
- procedures enforcing compliance with handling arrangements.

50100_HC 225 Intelligence Services Commissioner.indd 39 24/06/2015 12:43

6. ERRORS

Figure 6: Categories of errors

Category A

An administrative error such as where a typing error has occurred and the correction is obvious

Category B

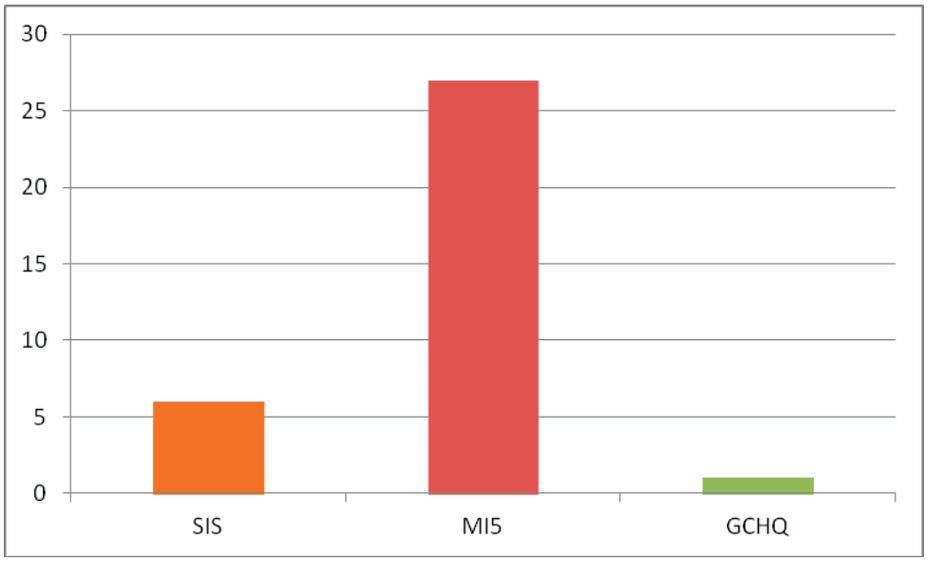
A situation where there has been, for example, an inadvertent failure to renew a warrant or obtain authorisation in time and where, if done properly, the application would have been granted

Category C

A deliberate decision to obtain information without proper authority and with no intention to obtain proper authority.

In addition to my bi-annual inspections, I require the agencies to report to me any errors that might have occurred during a warrant application, authorisation or when the warrant was put into operation. Examining these reports is an important element of my oversight of how the agencies use their intrusive powers. I expect the reports to explain: (1) when an error occurred, (2) when it was discovered, (3) the nature of the error, (4) how it happened and (5) what, if any, unauthorised invasion of privacy resulted. The reports also include details of the steps taken to avoid errors happening again. In 2014 there were **43 errors**. The agencies reported **34 errors** to me and I discovered nine during my inspections.

Figure 7: Number of errors reported in 2014

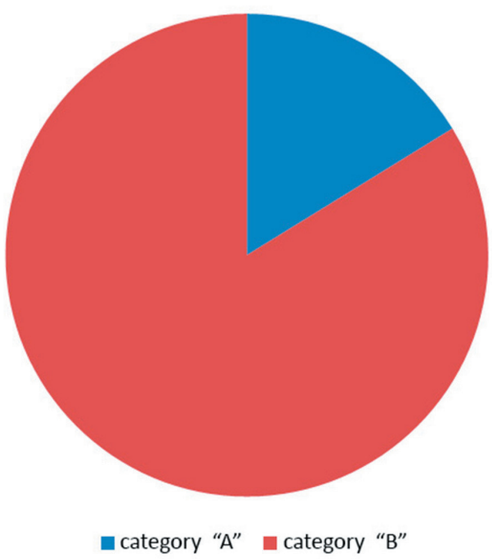


50100_HC 225 Intelligence Services Commissioner.indd 40 24/06/2015 12:43

Please note that MI5 obtain a larger number of warrants and authorisations than the other agencies, so their error rate is low as a proportion of authorisations.

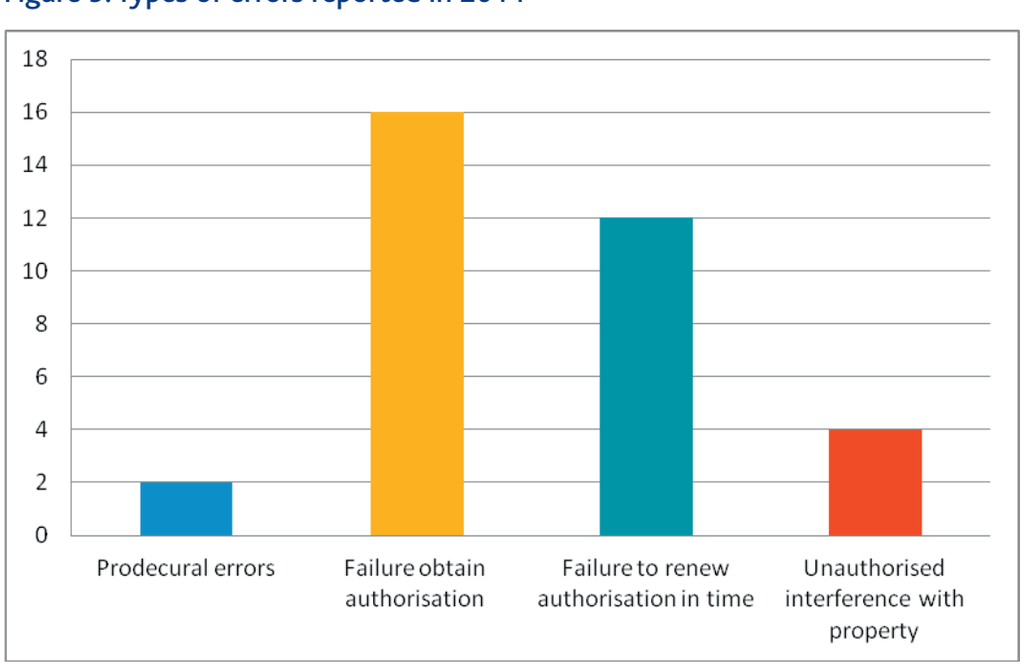
All of the errors reported to me were caused by human error and all resulted in intrusions into privacy to some degree. None were deliberately caused by those involved. Of these, 31 were Category "B" errors or inadvertent errors and 6 were category "A" or administrative errors:

Figure 8: Errors reported in 2014 by category



Of all the errors, the most common error was because of a failure to obtain authorisation in time. The least common error was due to unauthorised interference with property.

Figure 9: Types of errors reported in 2014



50100_HC 225 Intelligence Services Commissioner.indd 41 24/06/2015 12:43

Breakdown of errors by organisation

Security Service (MI5)

In 2014, MI5 reported 27 errors to me. I discovered an additional four Category "A" administrative errors during my inspections.

Of the 31 errors:

- almost all were caused by human error and all resulted in intrusion into privacy to some degree;
- none were caused with the intent to obtain information without the proper authority;
- 10 were the result of a failure to renew an authorisation in time;
- 12 were the result of a failure to obtain authorisation;
- 4 were the result of unauthorised interference with property;
- 5 were the result of procedural errors.

MI5 reported an error which occurred when a Directed Surveillance Authorisation (DSA) lapsed because of an administrative oversight. The original authorisation was obtained to assist in identifying and disrupting new terrorist activity.

The investigation team discovered the error seven days after the authorisation had expired while they were reviewing the DSA. During the period when there was no authorisation in place surveillance had continued but they did not review the surveillance product and deleted it from MI5's systems because they assessed it not to be of intelligence interest. The investigation team responsible for the error were reminded of the importance of renewing authorisations in a timely way.

I have had some concerns which I have raised during my inspections as to the circumstances in which it was permissible to retain product obtained when through an "unintentional error" there was no authorisation in place. I was first inclined to the view that it should take exceptional circumstances to allow retention, but I have been persuaded that if the circumstances are ones in which 1) authorisations would have been granted if sought and 2) retaining the product is necessary and proportionate in the interests of national security, it is not in the public interest to prevent such product being retained.

Administrative errors

During my inspection I discovered four typological errors including one where the date was shown to be 2010 instead of 2012 on a warrant. These were errors at the Home Office but I reminded MI5 that when they review warrants they should check it since it is they who need the authority to act lawfully.

50100_HC 225 Intelligence Services Commissioner.indd 42 24/06/2015 12:43

SIS

In 2014, SIS reported six errors to me. During my inspections all the submissions and authorisations I scrutinised were in good order and I did not identify any "slips" or Category "A" errors.

Of the six errors:

- almost all were caused by human error and resulted in intrusion into privacy to some degree;
- none were caused with the intention to obtain information without the proper authority;
- two were the result of a failure to renew an authorisation in time;
- four were the result of a failure to obtain an authorisation.

SIS reported an error which occurred when an officer failed to obtain an authorisation.

Although the operational team initiated an electronic RIPA authorisation 10 days before the operation was due to take place, it was not approved until after the operation had been carried out. The initiating officer did not carry out a final check that the authorisation was in place before the operation went ahead. The team's RIPA co-ordinator discovered the error during a review of the RIPA authorisation requests.

The team destroyed all the information gathered during the operation and they implemented a new monitoring system for RIPA requests to ensure that breaches did not occur again. The SIS Compliance Team gave the operational team involved a reminder briefing on RIPA requirements.

GCHQ

In 2014, GCHQ reported one error to me which happened when an internal monitoring system of some staff communications was found to be capturing more information than it was authorised to. I followed up on this error during my May inspection and the team explained that because of a lack of understanding of the systems' full capability more data than had been authorised had been collected. It was clear to me that this was a technical error and not deliberate. Following the discovery of the error GCHQ deleted the captured data and reconfigured the system to ensure that it only collected the information that it was authorised to collect. I continue to monitor this project to ensure that this error does not happen again.

Administrative errors

During my inspections all the submissions and authorisations I scrutinised were in good order and I did not identify any "slips" or Category "A" errors.

50100_HC 225 Intelligence Services Commissioner.indd 43 24/06/2015 12:43

Home Office

During my inspection of the Home Office Warrantry Unit, I discovered three administrative errors or Category "A" errors which I asked the Home Office to write formally to me about.

- The first error happened when a warrant incorrectly referred to an operation as a counter-espionage investigation when it was in fact an investigation into Islamist terrorism.
- The second error was a typographical error. The Home Office, on behalf of MI5, sought urgent authorisation from the Home Secretary to conduct activity in response to an urgent operational requirement. However, the application for the warrant which was signed by a Senior Official under the authority of the Home Secretary contained a typographical error which erroneously stated that the authorisation was specified in 1(ii) of the warrant, when it was in fact specified in 1(iii). The error was identified promptly, the warrant cancelled and replaced with a new warrant before any unauthorised action was taken.
- The third error was also a typographical error which included incorrect wording which only authorised one specified property belonging to the subject rather than several properties.

Ministry of Defence

In 2014, the Ministry of Defence did not report any errors to me. However I discovered two slips or Category "A" errors during my inspections.

The first error happened when an authorising officer failed to cross out "disagreed" in a warrant. To do so was required as part of the form to be completed at the time. However, I was informed during the inspection that the form had been updated and the new form did not have the requirement to strike out "disagree".

The second error happened when a directed surveillance authority (DSA) was only renewed two days after the original authority had expired. Although there was no unauthorised invasion of privacy, I advised the MOD that they should have made another application for a new authorisation rather than a renewal, once they had realised the original authorisation had expired.

Category C errors

Once again this year, I have not found any Category "C" errors. A Category "C" error or act is essentially when someone takes a deliberate decision to obtain information without proper authorisation and with no intention to obtain authorisation. In my 2013 Annual Report, I said that it would require dishonesty on the part of more than one person including a person of some seniority for such a situation to take place without discovery. However, in his latest report, the Interception of Communications Commissioner disclosed that a GCHQ employee

50100_HC 225 Intelligence Services Commissioner.indd 44 24/06/2015 12:43

deliberately undertook a number of unauthorised searches. This error did not occur within the boundaries of my oversight, but it demonstrates the need to remain vigilant.

Despite this, I would emphasise that the likelihood of a Category "C" error occurring is low for the reasons I articulated in my Annual Report for 2013. Were I to discover such a deliberate decision, I would report it to the Prime Minister immediately and notify the Crown Prosecution Service.

Area of concern – delays in reporting errors

During 2014 I expressed concern that the agencies did not report errors in a timely way. I raised this issue both during inspections and in writing and asked for an explanation for the delays in reporting. The agencies responded that the length of time it took to complete internal reviews and investigations into errors caused the delay.

As a result I now require the agencies to notify me as soon as they anticipate that an error investigation will take longer than the three month limit for reporting.

50100_HC 225 Intelligence Services Commissioner.indd 45 24/06/2015 12:43

7. BRIEF SUMMARY OF ASSESSMENTS

SIS

	Round 1	Round 2
Selection	20 March	30 October
Pre-Reading days	16 April	17 November
Inspection days	1-2 May	24 – 25 November
Station Visits	1-9 April (South America)	31 July – 1 August 2014 (North America)
Under the bonnet	14 January and 19 November 2014	

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading at SIS made out the case for necessity in all the individual cases.
Proportionality **Was the case for proportionality made In each case inspected?**	The paperwork I selected made the case for proportionality apart from one case where the authorisation had not set out if intelligence could be gained by other less intrusive means. However, after challenging the case officer I was content that the case could be made.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Most of the paperwork I selected for reading made the case for privacy. In one case where internal authorisations were being made under a thematic property warrant, proportionality and privacy were not set out in enough detail to reassure me that proper consideration had been given. The warrant set out the details in full but I would like to see separate consideration in the individual internal authorisation. Consideration must always be given to collateral intrusion and what will happen to any information acquired or where none was expected.

50100_HC 225 Intelligence Services Commissioner.indd 46 24/06/2015 12:43

Warrantry and authorisations

SIS take compliance seriously. It would however be better if instead of following an e-mail trail they recorded their considerations including necessity and proportionality in one document preferably a form which pointed to the questions to be considered.

I will continue to monitor closely:

- error reporting;
- record keeping

During my first under the bonnet visit I saw an example of the processes in place in SIS to help ensure their actions are legally compliant. In my second visit to a planning meeting I saw how teams consider where resources should be focused and look at legal and compliance issues.

I made a number of recommendations mostly in relation to ensuring SIS made a written record in one place. When I challenged the officers they demonstrated they had properly considered the necessity and proportionality but I would like to see it recorded. I continue to monitor thematic property warrants.

Bulk Personal Data

SIS have a proper system in place for considering whether BPD sets should be held and retained; they have good systems in place to ensure analysts have to justify access on a necessity and proportionality test which means that searches are aimed at subjects of intelligence interest; and they have a strong monitoring system to prevent individuals misusing BPD.

Consolidated Guidance

Whenever consideration is given to a situation in which a detainee of a foreign liaison is involved SIS take seriously compliance with the guidance and in particular consideration of whether there is a risk of mistreatment or unacceptable conduct and they do comply with the guidance but this is an area where putting all the considerations on one form would be an improvement.

MI5

	Round 1	Round 2
Selection	20 May	15 November
Pre-Reading days	11 & 12 June 2014	27 – 29 November
Inspection days	20 June 2014	11 December 2014
Under the bonnet	15 April 2014 and 13 January 2015	

50100_HC 225 Intelligence Services Commissioner.indd 47 24/06/2015 12:43

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made the case for necessity in all individual cases.
Proportionality **Was the case for proportionality made in each case inspected?**	The paperwork I selected for reading made the case for proportionality.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was mostly set out in the paperwork selected for reading. However, I noted that the paperwork for some urgent warrants did not have a separate box for considering privacy. At my request MI5 provided a copy of their "handling arrangements" concerning how operational data obtained from warrants and authorisations is managed and shared.

Warrantry and authorisations

MI5 also take compliance extremely seriously. I made a number of **recommendations** about selecting and presenting warrants in order to develop a broader picture of operations and handling arrangements where I was concerned in one case about the retention, storage and deletion of product obtained from a warrant.

My under the bonnet inspections supported my view that there is a high level of professionalism and a great deal of rigour given to the authorisation process. I will continue to monitor closely thematic warrants and the protections in place concerning product obtained without proper authority due to administrative errors.

Bulk Personal Data

MI5 have good systems in place to make sure the retention of and access to BPD is justified. They also have good systems in place to ensure that analysts only have access to BPD if they can justify the necessity and proportionality of their access with the result that intrusion into privacy is as far as it can be limited to that of subjects of intelligence interest. MI5 also have a good monitoring system in place to prevent individuals misusing BPD.

Consolidated Guidance

Whenever consideration is given to a situation in which a detainee of a foreign liaison is involved MI5 take seriously compliance with the guidance and in particular consideration of whether there is a risk of mistreatment or unacceptable conduct and they have a good form which has to be filled out demonstrating in one place all the relevant considerations and compliance with the guidance.

50100_HC 225 Intelligence Services Commissioner.indd 48 24/06/2015 12:43

GCHQ

	Round 1	Round 2
Selection	6 May 2014	2 October 2014
Inspection days	27 and 28 May 2014	11-12 November 2014
Under the bonnet	11 September 14 and 9 December 14	

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made out the case for necessity.
Proportionality **Was the case for proportionality made in each case inspected?**	In the paperwork I selected for reading the case for proportionality was set out
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was mostly set out for the operations I selected for inspection. GCHQ have recently updated their RIPA template and renewals now have separate headings forcing applicants to outline separately proportionality and the anticipated degree of intrusion into privacy.

Warrantry and authorisations

GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips. Following a recommendation I made during my May inspection, GCHQ agreed to propose a new form of words for warrants which make it clear that the Secretary of State is authorising on the basis that GCHQ will act in accordance with the accompanying submission. I made a number of recommendations primarily concerning the conditions set out in the submissions and instruments. I will continue to monitor thematic property warrants closely.

My under the bonnet inspection in December provided me with a greater understanding of how GCHQ's internal approvals apply to section 7 class authorisations. I was satisfied with the formality of the audit trail and the level of consideration given to each operation; it was clear to me that a great deal of thought was going into the process.

50100_HC 225 Intelligence Services Commissioner.indd 49 24/06/2015 12:43

Bulk Personal Data

GCHQ have a strong system in place which considers on a regular basis whether the retention is and continues to be justified. They also ensure that analysts must justify their access and demonstrate both necessity and proportionality with the result that intrusion into privacy is so far as possible aimed at subjects of intelligence interest. They also have a strong monitoring system to prevent improper access to the BPD.

Consolidated Guidance

Whenever consideration is given to a situation in which a detainee of a foreign liaison is involved GCHQ take seriously compliance with the guidance and in particular consideration of whether there is a risk of mistreatment or unacceptable conduct and they do comply with the guidance.

MOD

	Round 1	Round 2
Selection	8 May 2014	4 November 2014
Inspection days	16 & 21 May 2014	26 November 2014

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made the case for necessity.
Proportionality **Was the case for proportionality made In each case inspected?**	The paperwork I selected made the case for proportionality.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The privacy argument was set out in the paperwork I selected for reading. In some applications for CHIS the paperwork focused on the privacy of the CHIS. I advised that consideration must also be given in the paperwork to the privacy of the target of the tasking and any subsequent collateral intrusion.

Authorisations

MOD voluntarily apply a high compliance standard to RIPA principles. Generally the paperwork provided by the MOD was in good order although there was a minor slip because the wrong form had been used to apply for a DSA. In particular the Special Forces were doing well and I had little to comment on except to say that the paperwork was extremely good.

50100_HC 225 Intelligence Services Commissioner.indd 50 24/06/2015 12:43

I commended the MOD RIPA forms which set out in simple terms the areas which must be considered. I requested a copy of the template in order to share best practice; in particular their practice at the point of renewal of assessing the benefits already obtained and re-assessing privacy and intrusion.

Consolidated guidance

Compliance is taken seriously and the MOD have a good form which is filled in whenever consideration is given to circumstances involving a detainee and in particular whether there is a risk of mistreatment, and the MOD do comply with the guidance.

Home Office

	Round 1	Round 2
Selection	2 May 2014	11/12/14
Inspection days	13 May 2014	16/12/14

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The cases I selected for reading made the case for necessity.
Proportionality **Was the case for proportionality made in each case inspected?**	The paperwork selected for reading made the case for proportionality. Many of the submissions contained assurances that collateral intrusion of non intelligence value would be deleted. However a number did not. Whilst these assurances would have applied, I said that it was vital to make it explicit and the Home Office should see that it was included in submissions.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork I selected for reading. The proposed new wording for renewing warrants does not set out how the intelligence to be gained outweighs the invasion of privacy. Although this does not make the warrant unlawful I would prefer that this wording is reflected.

The Home Office warrantry unit provided a useful paper setting out the significant progress and developments since the last inspection and they are well on the way towards achieving the recommendations I made last year. They are generally doing

50100_HC 225 Intelligence Services Commissioner.indd 51 24/06/2015 12:43

well with a few recommendations which I will continue to monitor. I saw evidence that the warrantry unit questioned the submissions made by MI5. I saw evidence that the warrantry unit questioned as and when appropriate the submissions made by MI5.

The inspections focused on the use of thematic warrants where I sought more information about their use and restrictions.

The Home Secretary takes her responsibility to consider the necessity and proportionality of what she will be authorising very seriously.

NIO

	Round 1	Round 2
Selection	24 March 2014	21 September 2014
Inspection days	14 – 15 April	6 – 7 November 2014
Senior Official follow up	30 June 2014	

Detail	
Necessity **Was the case for necessity made in each case inspected?**	The submissions I scrutinised made out a case of necessity. In one case I questioned the necessity of continuing surveillance and subsequently spoke to MI5 about this. Both NIO and MI5 were able to reassure me that the correct authority was in place and the operation ceased as soon as it was no longer required. However, they accepted they were slow to cancel the warrant.
Proportionality **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I reviewed. The language of submissions should reflect any limitations applied to the use of the warrant. When authorising a warrant the Northern Ireland Secretary may put limitations on that warrant for example by setting a time for her to review it. I regard such limitations as good practice.

50100_HC 225 Intelligence Services Commissioner.indd 52 24/06/2015 12:43

Detail	
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork selected for reading although some submissions could contain more precise wording in order to set out how privacy will be protected. Submissions now set out: • What interference there is likely to be with the target of the operation's privacy and any other individual's privacy • How this will be limited • Why the expected intelligence cannot be gained by other less intrusive means The wording of the warrants reflects this. Renewal submissions at present do not always set out what interference with privacy there has been including collateral.

The paperwork provided by NIO was in good order. I made a number of **recommendations** mostly around the area of thematic property warrants which I will monitor. Generally NIO take a great deal of care looking at the submissions from MI5 and asking questions to clarify what is required by the Service before submitting to the Secretary of State. I have asked NIO to inform me of any cases where either NIO or the Secretary of State has had doubts. I am not looking to second guess the decisions but would like to see the consideration given to each case and discuss this.

The Secretary of State for Northern Ireland shows a keen interest in the case for necessity and proportionality. She can and does refuse warrants.

Foreign Office SIS

	Round 1	Round 2
Selection	20 March 2014	30th October 2014
Inspection days	12 May 2014	18 December 2014

50100_HC 225 Intelligence Services Commissioner.indd 53 24/06/2015 12:43

Detail SIS	
Necessity **Was the case for necessity made in each case inspected?**	The submissions I reviewed on the pre-read make out a case for necessity.
Proportionality **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I reviewed during the pre-read.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	No questions of privacy arose during the inspection but I asked that privacy is set out in a separate heading and not incorporated into a general heading in the submission.

Foreign Office GCHQ

GCHQ	Round 1	Round 2
Selection	6 May 2014	4 December 2014
Inspection days	21 May 2014	15 December 2014

Detail GCHQ	
Necessity **Was the case for necessity made in each case inspected?**	The submissions I reviewed on the pre-read make out a case for necessity. I have been looking closely at the case for necessity in relation to internal approvals and accept that the agencies do not self task. Their intelligence priorities are set out for them by government.
Proportionality **Was the case for proportionality made in each case inspected?**	The proportionality argument was clearly set out in the operations I selected for review.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	The case for privacy was set out in the paperwork I selected for reading. Internal approvals supplied for FCO or Ministerial consideration had set out that the level of intrusion is justified by the expected intelligence gain.

50100_HC 225 Intelligence Services Commissioner.indd 54 24/06/2015 12:43

FCO warrantry unit carefully consider submissions and seek clarification from SIS or GCHQ when necessary. Detailed consideration appears from the documents I inspect and from my meetings with officials. Necessity and proportionality is carefully addressed. I saw good examples in the GCHQ and SIS papers of good and proper administration.

The Foreign Secretary is supported by notes on the documents and considers points very carefully.

I will continue to review the use of thematic property warrants.

50100_HC 225 Intelligence Services Commissioner.indd 55 24/06/2015 12:43

8. CONCLUSIONS

As appears from the body of my report human errors have occurred as they will in any large organisation. I have also made a number of recommendations. But my overall conclusion is that the agencies and the MOD take compliance extremely seriously and seek to obtain their authorisations on a correct legal basis, establishing necessity to do what they seek to do, and properly considering proportionality and the justification for any intrusion into privacy. Equally where a warrant or authorisation has to be obtained from a Secretary of State, the warrantry units consider with care whether the case for necessity and the justification for any intrusion into privacy has been made out and the ministers themselves only sign the warrants or authorisation if they are satisfied of the necessity and proportionality of the activity they are authorising.

In light of the fact that new legislation in this area is likely to be considered I would draw attention to my recommendations in relation to the ability to combine warrants and to my concern for clarification as to the duration of warrants.

As regards Bulk Personal Data I am satisfied that the agencies properly consider and keep under review whether it is necessary and proportionate to hold or continue to hold Bulk Personal Data. I am also satisfied that access to that data is only permissible if a case of necessity justifies access and that any intrusion into privacy is kept so far as it can be to intrusion into the privacy of subjects of intelligence interest. I am also satisfied that the agencies have monitoring systems which are as effective as possible in preventing any individual having access to Bulk Personal Data other than that which they can properly justify for a business purpose.

As regards the Consolidated Guidance I am satisfied that the agencies and the MOD and those employed by them take compliance with the Consolidated Guidance extremely seriously and that the Guidance is properly followed.

50100_HC 225 Intelligence Services Commissioner.indd 56 24/06/2015 12:43

APPENDIXES

Useful Background Information

By way of background to my oversight role, I believe it is useful to be aware of the directions from the Prime Minister placing my oversight on a statutory footing as well as the functions imposed upon each of the intelligence services and certain constraints to which they are all subject.

In this appendix I have set out

Appendix 1 The statutory functions of the Intelligence Services

Appendix 2 A summary of the Regulation of Investigatory Powers Act 2000 (RIPA)

Appendix 3 A summary of warrants and authorisations under RIPA

- Directed Surveillance
- Covert Human Intelligence Source
- Intrusive Surveillance

Appendix 4 A summary of warrants and authorisations under the Intelligence services Act 1994 (ISA)

- Section 5
- Section 7

Appendix 5 Article 8 of the European Convention on Human Rights

Appendix 6 Definition of Necessity and Proportionality

Appendix 7 Bulk Personal Data Direction

Appendix 8 Consolidated Guidance Direction

50100_HC 225 Intelligence Services Commissioner.indd 57 24/06/2015 12:43

Appendix 1

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.

50100_HC 225 Intelligence Services Commissioner.indd 58 24/06/2015 12:43

Appendix 2

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:	is concerned with the interception of communications (the content), and the acquisition and disclosure of communications data (the who, when and where). Oversight of Part I activities is provided by the Interception of Communications Commissioner who produces his own report on Part I activities.
Part II:	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:	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 IV:	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 RIPA and ISA.
Part V:	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.

50100_HC 225 Intelligence Services Commissioner.indd 59 24/06/2015 12:43

Appendix 3

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.

50100_HC 225 Intelligence Services Commissioner.indd 60 24/06/2015 12:43

Duration	Urgent	Renewal
Ceases to have effect [unless renewed or cancelled] at the end of a period of three or six months beginning with the time at which it took effect.	Unless renewed ceases to have effect after 72 hours beginning with the time when the authorisation was granted	May be renewed for a further period of six months (three months for the MOD) beginning with the date on which it would have ceased to have effect but for the renewal. Application to be made shortly before the authorisation period is drawing to an end.

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:

50100_HC 225 Intelligence Services Commissioner.indd 61 24/06/2015 12:43

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 close management of a CHIS, 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.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of 12 months beginning with the day on which it took effect [except juveniles].	Unless renewed ceases to have effect after 72 hours beginning with the time when the authorisation was granted	Renewal for a further 12 months. Renewal takes effect at the time at which the authorisation would have ceased to have effect but for this renewal. Application to be made shortly before the authorisation period is drawing to an end.

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.

50100_HC 225 Intelligence Services Commissioner.indd 62 24/06/2015 12:43

How is intrusive surveillance authorised?

Under section 32 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.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of six months beginning with the day on which it was issued. They expire at 23.59 on the last day so an authorisation given at 09:00 on 12 Feb will cease to have effect at 23:59 on 11 Aug,	Oral authorisation may be given by the Secretary of State will cease to have effect [unless renewed] at the end of the second working day following the day of issue.	Where renewed it ceases to have effect at the end of six months beginning with the day it would have ceased to have effect if not renewed again Application to be made before the warrant expires.

50100_HC 225 Intelligence Services Commissioner.indd 63 24/06/2015 12:43

Appendix 4

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 SIS, the Security Service and GCHQ to carry out certain actions in connection with their functions. 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 the Security Service, 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.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of six months beginning with the day on which it was issued.	Oral authorisation may be given by the Secretary of State which will cease to have effect [unless renewed] at the end of the period ending with the fifth working day following the day on which it was issued.	The warrant may be renewed in writing for a further period of six months beginning with the day on which it would otherwise cease to have effect.

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.

50100_HC 225 Intelligence Services Commissioner.indd 64 24/06/2015 12:43

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.

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.

Duration	Urgent	Renewal
Ceases to have effect at the end of a period of six months beginning with the day on which it was issued.	Oral authorisation may be given by the Secretary of State which will cease to have effect [unless renewed] at the end of the period ending with the fifth working day following the day on which it was issued.	ISA states: "If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of six months beginning with that day."

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.

50100_HC 225 Intelligence Services Commissioner.indd 65 24/06/2015 12:43

Appendix 5

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.

50100_HC 225 Intelligence Services Commissioner.indd 66 24/06/2015 12:43

Appendix 6

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 utilised, the intelligence services much 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 take care to apply for warrants only where they believe the threshold is clearly met.

50100_HC 225 Intelligence Services Commissioner.indd 67 24/06/2015 12:43

Appendix 7

Bulk Personal Datasets Direction

Regulation of Investigatory Powers Act 2000

Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015

The Prime Minister, in exercise of the power conferred by section 59A of the Regulation of Investigatory Powers Act 2000 ("the Act"), directs the Intelligence Services Commissioner appointed under section 59 of the Act as follows:

Citation and Commencement

1. This Direction may be cited as the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015.

2. This Direction comes into force on 13 March 2015.

Additional Review Functions

3. The Intelligence Services Commissioner must continue to keep under review the acquisition, use, retention and disclosure by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters ("the Security and Intelligence Agencies") of bulk personal datasets, as well as the adequacy of safeguards against misuse.

4. The Intelligence Services Commissioner must seek to assure himself that the acquisition, use, retention and disclosure of bulk personal datasets does not occur except in accordance with section 2(2)(a) of the Security Service Act 1989, sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994. As part of this, the Intelligence Services Commissioner must seek to assure himself of the adequacy of the Security and Intelligence Agencies' handling arrangements and their compliance therewith.

5. For the purposes of this Direction, a bulk personal dataset means any collection of information which:

    a. Comprises personal data as defined by section 1(1) of the Data Protection Act 1998;

    b. Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;

    c. Is held, or acquired for the purpose of holding, on one or more analytical systems within the Security and Intelligence Agencies.

Signed: David Cam

Date: 11.3.15

50100_HC 225 Intelligence Services Commissioner.indd 68 24/06/2015 12:43

Appendix 8

Consolidated Guidance Direction

Regulation of Investigatory Powers Act 2000

Intelligence Services Commissioner (Additional Review Functions) (Consolidated Guidance) Direction 2014

The Prime Minister, in exercise of the power conferred by section 59A of the Regulation of Investigatory Powers Act 2000 ("the Act"), directs the Intelligence Services Commissioner appointed under section 59 of the Act as follows:

Citation and Commencement

1. This Direction may be cited as the Intelligence Services Commissioner (Additional Review Functions) (Consolidated Guidance) Direction 2014.

2. This Direction comes into force on 28 November 2014.

Additional review functions

3. The Intelligence Services Commissioner must keep under review the compliance of persons falling within paragraph 4 with the guidance referred to in paragraph 5 in relation to the circumstances set out in paragraph 6

4. The persons are:

    a. officers of the Security Service, the Secret Intelligence Service and the Government Communications Headquarters;
    b. members of the Armed Forces of the United Kingdom and employees of the Ministry of Defence, so far as any of them engage in intelligence activities within the meaning of section 59A of the Act.

5. The guidance is 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 which was published on 6 July 2010, as amended from time to time.

6. The circumstances are those in which one or more persons falling within paragraph 4:

    a. interview a detainee who is in the custody of a third party;
    b. request a third party to seek information from a detainee in the custody of that party;
    c. pass information to a security or intelligence service of a third party in relation to a detainee held by that party;
    d. receive unsolicited information from a third party which relates to a detainee;
    e. solicit the detention of an individual by a third party.

Signed: David Cameron

Date: 27th November, 2014

50100_HC 225 Intelligence Services Commissioner.indd 69 24/06/2015 12:43

50100_HC 225 Intelligence Services Commissioner.indd 70 24/06/2015 12:43

50100_HC 225 Intelligence Services Commissioner.indd 71 24/06/2015 12:43

ISBN 978-1-4741-2111-8

50100_HC 225 Intelligence Services Commissioner.indd 74 24/06/2015 12:43