Intelligence Services Commissioner

Report of the Intelligence Services Commissioner for 2015

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 8 September 2016

Laid before the Scottish Parliament by
the Scottish Ministers 8 September 2016

HC 459
SG/2016/96

Intelligence Services Commissioner

Report of the Intelligence Services Commissioner for 2015

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 8 September 2016

Laid before the Scottish Parliament by
the Scottish Ministers 8 September 2016

HC 459
SG/2016/96

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

Any enquiries regarding this publication should be sent to info@iscom.gsi.gov.uk

Print ISBN 9781474135535
Web ISBN 9781474135542

ID 30061601 09/16

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

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

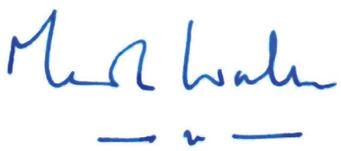
The Rt Hon Theresa May MP
The Prime Minister
10 Downing Street
London
SW1A 2AA

21 July 2016

I enclose my fifth Annual Report covering the discharge of my functions as Intelligence Services Commissioner between 1 January 2015 and 31 December 2015.

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the Confidential Annex containing further details including techniques and operational matters which in my view should not be published.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

1. INTRODUCTION

This is my 5th annual report since first taking up office as the Intelligence Services Commissioner on 1 January 2011. Even since my last, covering 2014, there have been a number of significant developments affecting the areas I oversee which I cover in more detail later in this introduction. I will also address my oversight in general, changes I have made to this report compared with previous reports and recent important developments.

My Oversight

The areas I oversee cover some of the most intrusive powers available to the intelligence agencies, including intrusive surveillance, property and equipment interference and obtaining and accessing bulk personal datasets. I oversee the surveillance activities of the Ministry of Defence. I also oversee compliance by the agencies and the Ministry of Defence 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', known as the Consolidated Guidance, a complex area involving difficult decisions relating to intelligence sharing.

In essence my oversight role requires me to check:

- that warrants and authorisations which enable the intelligence services to carry out their functions are being granted by the Secretaries of State and/or being internally authorised only after a proper case of necessity has been demonstrated and a proper case that what is to be authorised is proportionate has been made;
- that bulk personal datasets are being obtained, retained and used only where it is shown to be both necessary and proportionate to do so;
- that the Consolidated Guidance is being complied with so that proper consideration is given as to whether a detainee of a third party state is being and/or will be properly treated before intelligence is shared with that country.

To do this I scrutinise how the agencies and MOD carry out their activities. I do so in a number of different ways:

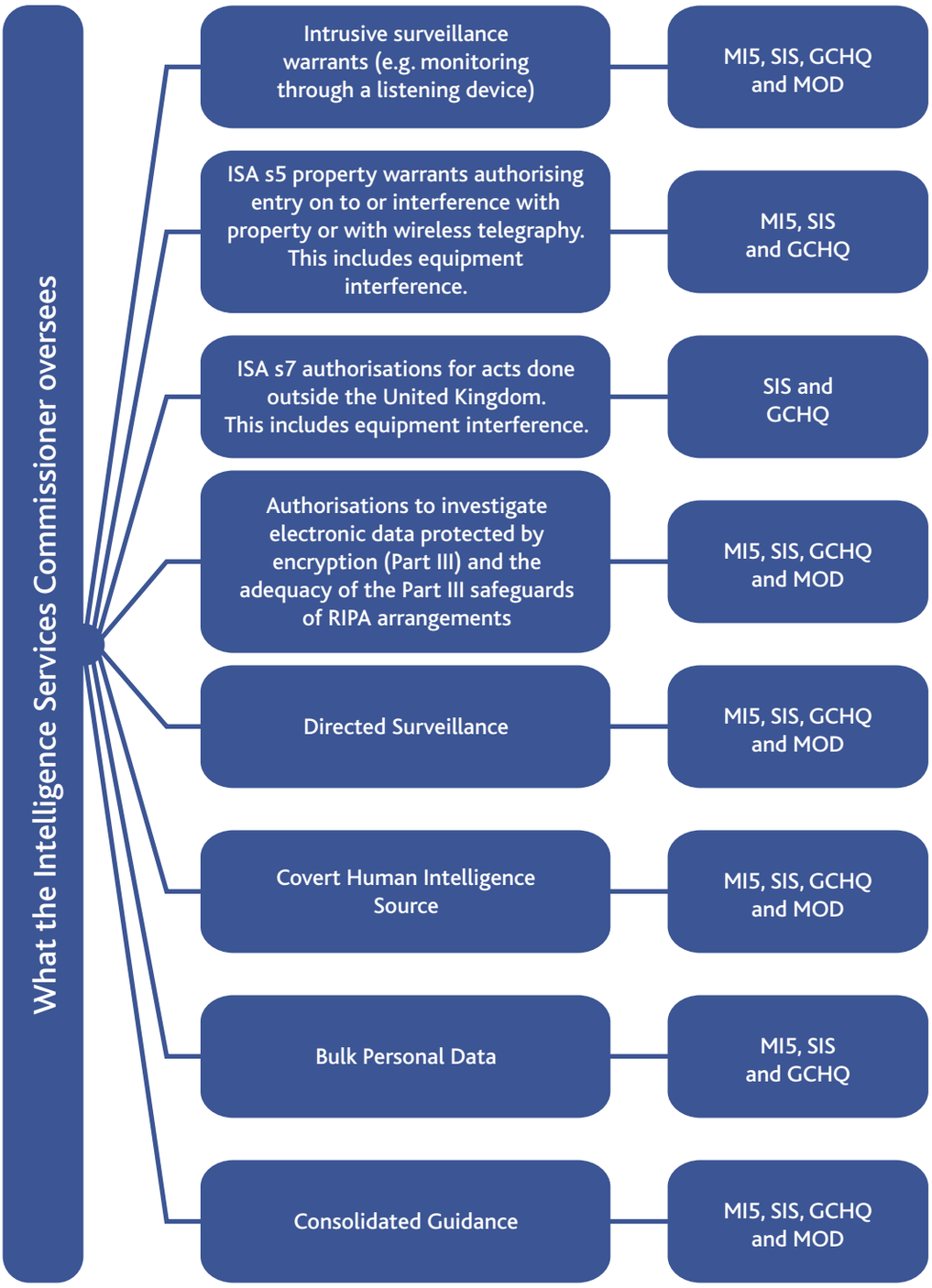
- First, there is the 'after the fact audit' carried out twice a year of all the above about which I have written in detail in my annual reports e.g. those for 2013 and 2014;
- Second, I look at the safeguards in place within the agencies to prevent inappropriate access to and/or use of powers, information or systems; the policies and procedures in place to deal with acquisition, use, retention and deletion of information obtained by use of the powers available to them and to prevent misuse; and the systems and processes officers must go through to access material;
- Third, observing the culture and ethos across the organisations including by, for example, attending training courses for new recruits and established staff.

I am also asked to carry out further activities by the Prime Minister.

A cornerstone of my regime is personal responsibility and I do my job rigorously, independently of government, Parliament and the agencies, without political favour or personal bias. All Commissioners are required to be holders or past holders of high judicial office, meaning that they are independent and will form their own impartial judgement, that they will have had long experience of drawing out the facts and that they should be seen to carry authority because of their position.

Functions

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 act lawfully and appropriately use the intrusive powers available to them including:



Other statutory functions include:

- assisting the Investigatory Powers Tribunal when required;
- reporting to the PM (Annual Report);
- overseeing any other aspects of the functions of the intelligence services, HM Forces or the MOD when directed by the Prime Minister;
- advising the Home Office on the propriety of extending the TPIMS regime.

Terrorism Prevention Investigation Measures (TPIMS) Act 2011

One of my functions is to advise the Home Office on the propriety of extending the TPIMS regime as part of the consolation process under section 21(3) of the TPIMS Act. TPIMS expire 5 years after the date the Act came into force unless an order is made by the Secretary of State to extend or repeal. TPIMS will expire on 15/12/16 which will be the first time such a consultation process will be required.

Section 94 of the Telecommunications Act 1984

In 2010 GCHQ asked my predecessor to oversee the activity of GCHQ in relation to data acquired by means of directions given by the Secretary of State under section 94 of the Telecommunications Act. This oversight was on an extra-statutory basis and was not avowed. When I took up appointment in 2011 I continued to oversee GCHQ's use of section 94 directions. My oversight involved (a) examining the justification for the directions and (b) examining the acquisition and use of the data acquired on the same basis as I oversaw bulk personal data. However, in January 2015 the Interception of Communications Commissioner agreed to formally oversee these directions.

Changes from previous annual reports and my website

In January of 2016 my team revamped the content of my website, adding significantly more information than it previously held. I hope it is a useful resource for those with an interest in the areas I oversee.

In previous annual reports I included detail on my statutory functions, the methods I use to audit warrants and authorisations, my assessment of inspection visits and summaries of relevant legislation among other things. Further details about my statutory functions, the method of my warrant and authorisation review and information about relevant legislation are now available on my website.

Last year I introduced 'thematic' sections to my reports on the various powers that I oversee with the intention of making information about use of those powers by the agencies and MOD clearer and more readily accessible to the layperson. This year I have expanded the thematic sections, provided more detailed statistics and focused on an important element of oversight which risks being lost in discussion of judicial authorisation and auditing after the fact, that is the risk of rogue activity and how the agencies themselves, and I as part of my oversight, work to mitigate that risk.

Inspection Reports and Confidential Annex

In this report I have continued to be as transparent about my oversight role as possible subject to the national security restrictions which are in place for good reason. As intelligence and security services, secrecy is critical to the agencies' ability to function effectively. If I were to disclose certain information in my report, as well as aiding hostile intelligence services doing so could reduce or risk reducing the value of particular methods, techniques or equipment in current or future operations and potentially cause damage to operational capabilities or personnel which would be harmful to the national security of the UK.

After each inspection the head of my secretariat produces an inspection report which is specific to that organisation and sets out the emerging findings from that inspection and any recommendations I have made to demonstrate or to improve compliance. During my inspection I scrutinise ongoing operations so these reports are highly classified. I reflect the general findings from these reports and the various themes that emerge over the year in my annual report and I provide the Prime Minister with a confidential annex containing more classified material including details and techniques.

Developments since my last annual report

Since my last annual report was written in 2015, there have been a number of significant developments affecting the areas I oversee. These developments include two fundamental reviews into the authorities' use of investigatory powers and the Investigatory Powers Bill (IP Bill) which was introduced to Parliament on 1st March 2016. Reports of the reviews, 'A Question of Trust' by David Anderson Q.C. and 'A Democratic Licence to Operate' by the Royal United Services Institute (RUSI), alongside the Intelligence and Security Committee's Privacy and Security Report published in March 2015 were a starting point for many of the provisions in the government's Investigatory Powers Bill. The Government also avowed the existence of powers I oversee which were not previously publically avowed.

A key feature of the Bill, if it is passed, will be to introduce what is termed a double lock in the authorisation process for some but not all authorisations granted by Ministers – the double lock being the necessity to obtain approval by judicial commissioners.

Much of what I at present oversee i.e. authorisations granted to the intelligence agencies to interfere with property other than interference with computers (equipment interference) and authorisations to those agencies to conduct intrusive surveillance is not proposed to be subject to the double lock and is to be authorised and overseen as now.

Some may think that inconsistent in that a listening device in a car or a home might be thought to be as intrusive as an interception of a telephone call. But the important point is that there is a recognition, with which I agree, that ministers can and do properly assess in the national security context necessity and proportionality and that an auditing system by a senior judge or a retired senior judge after the event checking that warrants and authorisations have been and are being granted on a proper legal basis is an effective oversight system.

The reason why it is effective in my judgment is that there is a culture both in the agencies, the MOD and at the offices of the Minister which wants to ensure that they act within the constraints that Parliament has imposed and to get things right – the fact that a senior judge is going to come in and probe and ask questions of all persons involved in the process discourages the pushing of boundaries never mind worse. If the agencies themselves were as institutions determined to act unlawfully that would take a massive conspiracy from top to bottom and they would not be seeking warrants or authorisations to so act. A thing of primary importance is to check that there are systems in place to prevent a rogue using the very powerful tools available without authorisations. But I stress it is important to have a system of oversight which seeks to ensure that the boundaries that the law imposes are strictly complied with and my experience is that the after the event audit does meet that requirement because the authorisers do not want criticism or worse to be told the authorisation was in fact unlawful.

Finally, in November 2014 the Prime Minister requested me to investigate concerns raised by the Intelligence and Security Committee in their report on the murder of Fusilier Lee Rigby. In their report the ISC were critical of SIS for their handling of allegations of Michael Adebolajo's mistreatment in Kenya made during his interview by police under the Terrorism Act 2000 on his return to the UK. My report on that investigation is being published supplementary to my annual report.

2. RISKS

As already indicated what must be guarded against is any individual, or group of individuals, who seek to abuse the systems. They would not seek authorisation. They would try to circumvent the system for their own ends.

So a vitally important part of my oversight is about mitigating that risk. To do so I look at: the safeguards in place within the agencies to prevent inappropriate access to or use of information obtained by the agencies to allow them to carry out their statutory functions; the policies and procedures the agencies have put in place to deal with the acquisition, use, retention and deletion of information obtained by use of the powers available to them and to prevent any misuse; the systems and processes officers must go through to access such material; that individuals are not free to act on their own or without supervision; and the culture and ethos in an organisation.

Of course discussing what these processes and policies are in any detail here would be counter productive, allowing anyone who would attempt to abuse the system the knowledge by which to do so. But I can say that the systems and policies in place in all the agencies are designed to ensure that no one person can act on their own or access information on any of the systems holding sensitive information individually, without someone else knowing about it and without having to go to a more senior officer.

This would deal with a rogue individual. But not with a top down conspiracy, the scale of which would have to be massive to be successful. A further mitigation is an effective appointments process, thorough vetting at the outset and appointing individuals of integrity at the top. The culture and ethos across the agencies must be closely monitored. In addition to my interactions with staff during my inspections, my under the bonnet visits and visits to stations overseas, I regularly attend training courses for new recruits and established staff all of which give me a good insight into the culture and ethos of the organisation and its staff.

3. THEMES

i. Covert Human Intelligence Source (CHIS)

Part II of RIPA and the associated code of practice provide the legal framework for authorising the use and conduct of a CHIS. A CHIS may be a member of the public reporting to one of the agencies, or to the MOD, or an intelligence officer or a member of military personnel operating under an alias. They are authorised to obtain information from people who do not know that this information will reach the intelligence agencies or armed services. CHIS are often referred to as agents.

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 in relation to the use and conduct of CHIS I can see the documentation provided has demonstrated that proper consideration is given to necessity and proportionality and in particular the possible invasion of privacy and the justification for this. Officers have also made themselves available to brief me about their specific agent running or undercover operation and answer my questions. **There are however some points to be made.**

CHIS Reviews

MI5's business model is designed to ensure that the case management team, and in particular the case officer and controller, are constantly reviewing the cases for which they have responsibility and I have no reason to believe this is not taking place. However, I noted that the formal, documented review of the CHIS authorisations I scrutinised was inconsistent including:

- no documented reviews beyond those conducted at renewal for three cases: one renewal stated that no formal review was necessary, although there was a recorded requirement for regular updates on the case to be provided to the authorising officer;
- five new authorisations did not mention reviews;
- one CHIS had been reviewed regularly;
- one had been inherited from the police with no mention of reviews;
- one mentioned a review date but there was no paperwork; and
- two had been reviewed once but there was no record of subsequent review.

This has been an ongoing problem, as I mentioned in my report for 2014. MI5 explained that reviews should have been carried out by the authorising officer in accordance with the code of practice paragraph 5.17. I reminded MI5 that under the code they should review each CHIS regularly. I **recommended** they record these reviews to demonstrate that they have given proper consideration to reviews and completed them, and that the activity still meets necessity and proportionality requirements for oversight purposes. Since my recommendation MI5 have been more consistently conducting formal written reviews, and will extract the information from the decision log and make it available to me at future inspections

MI5 were unable to explain the automatically generated random review dates that appeared in some of the paperwork but believe there was a technical problem and agreed to look into it.

I also saw examples of this in SIS where I **recommended** that the authorising officer set realistic review dates at the point of authorisation in line with the code of practice para 5.17.

Confidential Information

One authorisation was referred to me because it had the potential to obtain confidential information, specifically spiritual counselling. This in fact goes further than the requirement of the code of practice paragraph 4.18 which only requires cases to be referred to me when information has been obtained.

In my view the authority gave good consideration to religious sensitive information and the paperwork showed that confidential material was not the desired intelligence outcome, in fact the CHIS tasking was clear that the information to be gathered should not include spiritual counselling. I agreed that the authorisation was appropriate and had given good consideration to the possibility of obtaining confidential information. In my view it must be possible in such circumstances where there is an immediate threat to life to investigate. Religious cover should not be used to protect criminal behaviour.

Duration of Authorisations

In my 2014 Report I noted 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. In my view it is arguable that it is neither necessary nor proportionate to issue for the full twelve month period when it is known at the outset that the operation will be for a shorter period but I recommended that the code of practice should be applied in all cases and the authorisation cancelled when it is no longer required. This has been monitored throughout my inspections in 2015 and I am confident that this recommendation has been implemented.

Agent Participation in the Commission of an Offence

There may be occasions where a CHIS participates in a criminal offence in order to gather the required intelligence, for example membership of a proscribed organisation or handling stolen goods. However in specific situations where the intelligence dividend justifies it, a good argument can be made that it is in the public interest and for the greater good to become involved. Although such activity cannot be made lawful I have **recommended** that the agency must justify the public interest test.

ii. Directed Surveillance

Directed Surveillance is surveillance which obtains private information in a covert but not intrusive manner. Although directed surveillance is not intrusive, 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 privacy considerations. While Part II of RIPA does not impose a requirement for public authorities to obtain DSAs before conducting directed surveillance, RIPA authorisations are in fact used to authorise such surveillance.

My overall assessment

From the submissions I have examined the applications to undertake directed surveillance have made out a proper case. The documentation provided has demonstrated proper consideration of necessity and considered properly whether any intrusion into privacy is justified and the extent to which it is justified. Officers made themselves available to brief me about their operation and answer my questions. This helps me to confirm that the necessity case is justified and that the operation is limited to what has been authorised in the RIPA application. **There are however certain points to be made.**

Completing Forms

At SIS, once the authorisation has been finalised it is not possible to amend it. This is a good thing and where I did come across a typographical error (such as saying 2015 instead of 2016) I noted that the authorising officer would minute a correction on the day of authorisation so no error occurred.

In one case, a month after the operation, SIS noticed that, although a form had been properly authorised it had not been published; publishing locks the form down. As a consequence SIS explained to me that the original text had degraded and the proportionality box appeared empty. I asked for an explanation how SIS or I could be confident that proper consideration had been given since, with no text in the box, it appeared that proportionality had not been considered. In my view this is not satisfactory and should not happen. The team responsible for legalities and compliance explained that they had a discussion with the authorising officer who had seen a version of the form with this information completed. I requested this version of the form but unfortunately after conducting a search the authorising officer returned to say that it was no longer on their personal drive because it is automatically cleared every three months. Having heard an explanation from the compliance team and the authorising officer, I was satisfied that on a balance of probabilities, this was a failure to follow SIS internal guidance but no error had occurred. However, it should not happen and I **recommended** that these important documents should be "locked down" when they are authorised. In retrospect, it would have been better if SIS had recorded the explanation which they provided to me.

Actions Authorised

By far the majority of directed surveillance authorisations that I see are at MI5 so the majority of points relate to them.

During 2015 MI5 briefed me on their plans to better explain the standard range of actions on the DSA authorisation form. They planned to:

- merge similar actions;
- remove unnecessary or obsolete actions;
- add new actions which had not previously been specified;
- clarify any actions which may have been unclear.

Having reviewed the plans I was content that this should help improve officer's understanding and reduce errors.

Filler Text

I was concerned to see that there continues to be odd occasions where an automatic nonsensical filler text appears in DSA renewal and modification forms. I have spoken to MI5 about this repeatedly throughout the last few years. This filler text must not be used to populate any section of any form and nor should they say 'not applicable' which has appeared in another situation. If, for example, the modification or renewal does not require specific consideration in relation to one part of the form then this should be set out. If for example a DSA is modified and no extra consideration of necessity and proportionality is required I **recommended** that it would be acceptable to say "see previous form". If however, a DSA is modified and another intelligence target is added, within this specific operation, then proper consideration must be given to intrusion into privacy, collateral intrusion or why the intelligence cannot be gained by less intrusive means. Care should be taken to give specific consideration and not to use stock language. Staff have been reminded so I do not expect this to happen again.

Stock Forms

MI5's stock form for cancelling a DSA includes the wording "*Before making this authorisation, the authorising officer satisfied themselves that the actions in question were necessary for the protection of national security and were proportionate to what was sought to be achieved*." This language is obviously not appropriate; the DSA is being cancelled because it is no longer necessary and proportionate so I **recommended** that the form should be amended to correct this.

Modification to DSAs

Directed Surveillance may be broadly termed if for example it authorised surveillance against a particular terrorist operation. The legislation requires that it is

"for the purpose of a specific investigation or a specific operation". In such thematic style surveillance operations, the authorisations should:

- make it clear what the expected outcome is;
- identify the targets, preferably by name;
- keep track of any amendments during the course of the operation through a modification document.

In my report last year I said that although MI5 were diligent in modifying authorisations, it was sometimes difficult to keep track of the amendments. To improve my ability to inspect MI5 gave me and my office access to documents on a computer system which enables us to cross check modifications to ensure they are always accurate. This has been an asset to the scrutiny process.

At the MOD they were re-authorising a DSA rather than modifying the original. This had the potential to cause confusion, particularly if the original DSA was not cancelled. I **recommended** they create and implement a stock form for DSA modifications and advised that the form should set out:

- what had been modified;
- why the purpose of the original DSA is still met;
- why it remains necessary and proportionate and;
- consideration of intrusion into privacy.

I suggested that the MI5 template would be a good starting point. By my second inspection I was pleased to see that MOD had drafted a modification template based on the MI5 form.

Open Source Information

As I indicated last year, the law, including Article 8 of the ECHR, applies to online activity equally as to activity in the physical world and the agencies are obliged to comply with the law when it comes to collecting open source internet data just as much as collecting any other type of intelligence. At the time the agencies were working on clearer guidance which I asked to see. To date the agencies have agreed the broad principles, but do not have a joint policy as yet.

The broad principles recognise that:

> "... human behaviour is shifting rapidly so that far more activity and communication now occurs online than ever before and there is much more concern about privacy online, undermining the traditional concept of putting information on the internet as being akin to publishing in the print media."

It includes the legal basis for authorisation which says:

> "However the collection and retention in a permanent record by MI5 of open source internet data about a person is capable of amounting to an interference with that person's Article 8 rights, because it will arguably exceed a person's reasonable expectation of privacy and give rise to private life considerations, depending on the totality of the retained data.
>
> This is a similar principle to the observation of a person's public movements. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information."

I was pleased to see that my recommendation had been implemented in this way and look forward to a finalised cross agency agreement.

Duration

On a few occasions I have noted that a DSA had been authorised a few days before it was to come into force. I have commented on this above but in summary I have **recommended** that the authority begins on the day it is signed by the authorising officer.

The MOD reported to me at inspection that a DSA operation had deployed before the paperwork was concluded. I advised that this error should be formally reported either as a failure to obtain a DSA or failure to obtain an urgent authority for 72 hours.

Combination

In my previous Annual Report I explained that I had become concerned that there is room for error when directed surveillance is required in combination with a property warrant. As I said last year, 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 relevant agency. Added to this, property warrants and DSAs have different duration periods which means that the warrants and authorisations have different renewal/cancellation deadlines. In view of this I **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. As the IP Bill has not updated part II of RIPA or ISA this opportunity has been missed.

iii. Intrusive Surveillance and Property Warrants

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 deployment of a surveillance device. The agencies must make a strong case to explain why the information to be obtained cannot be obtained by less intrusive means and that the necessity of obtaining the information outweighs the intrusion into privacy.

Surveillance is defined as intrusive or not depending on the location in which that surveillance takes place. So, since surveillance in residential premises or vehicles is likely to involve a greater intrusion into privacy, it is defined as intrusive. The agencies also consider other situations where a person would have a reasonable expectation of privacy. Because intrusive surveillance can take place inside family homes and cars it is the most intrusive power. I keep this in mind when I am reviewing applications and when they come up for renewal I expect to see evidence of the intelligence gained to help justify the continued intrusion into privacy.

Section 5 Property Warrants

Under Section 5 of ISA the Secretary of State may issue warrants authorising MI5, SIS or GCHQ to enter into, go onto, or interfere with property, or to interfere with wireless telegraphy. They are often referred to as property warrants. A property warrant may be used for remote interference with a computer which is covered in my chapter on Equipment Interference.

In this section I am concerned with property warrants used to authorise entry into or interference with a domestic residence for the purpose of concealing a listening device. In such cases a combined warrant is used.

Combined Warrants

The vast majority of intrusive surveillance warrants I see are combined with an ISA Section 5 property warrant. Under section 42(2) of RIPA a Secretary of State may issue a single warrant combining an intrusive surveillance warrant with a property warrant. However, proper and separate consideration must be given in the submission to both the property warrant and the intrusive surveillance. This could be planting an eavesdropping device in a car or residential home.

A combined property and intrusive surveillance warrant can be highly invasive and as such separate consideration must be given to limit any unnecessary intrusion into privacy and specifically collateral intrusion into the privacy of any family members or friends of the person. A strong case must be made to explain why the information cannot be obtained through less invasive means and that the necessity of obtaining the information outweighs the invasion of 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 of privacy authorised has also been justified by the necessity. I am satisfied that the agencies, the warrantry units and ultimately the Secretaries of State recognise the degree of intrusion and great care goes into making and submitting these applications. The agencies must explain why the intelligence cannot be obtained by a less intrusive means.

My only concern during 2015 relates to the fact that submissions do not always set out as fully as they could the steps to be taken to mitigate collateral intrusion.

Collateral Intrusion

Many submissions for Intrusive Surveillance and Section 5 Property Warrants recognised that collateral intrusion was likely to occur but then failed to stipulate what would happen to the unwanted product or steps taken to limit the intrusion. These are standard techniques and recognised procedures are in place for such a situation which the agencies can and do explain to me. However, in order to demonstrate proper compliance I **recommended** that this information is set out clearly in the submission.

Retrieval of Equipment

The code of practice in relation to Property Interference Warrants recognises that it may be necessary to renew a warrant in order to retrieve a device which is no longer needed for intelligence purposes. In such cases it is in fact no longer necessary or proportionate to continue with the matters authorised by the accompanying Intrusive Surveillance Warrant but it has not yet been possible to remove the equipment, and some authorisation is still required.

I have agreed that while a device is awaiting extraction, it is possible to transfer the device onto a thematic warrant which properly reflects the basis for the continued presence of the device.

Thematic Property Warrants

I continue to scrutinise particularly what might be termed thematic property warrants issued under Section 5 of ISA. When a proper case can be made for authorising these broadly termed warrants I have **recommended** that the agencies devise a method of recording any reliance on the warrant in relation to individual operations. Overall I have made it clear that they are the exception rather than the rule and must never be used for operational convenience.

In my previous report I made a number of recommendations in relation to thematic property warrants and said:

> "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."

During my inspections of 2015 I reviewed the revised warrant which better defined the property to be interfered with. I still felt there was room for improvement and my **recommendation** in that regard was also implemented.

My recommendations relating to thematic warrants have largely been accepted and implemented. The lists provided for my inspection have, for the most part, highlighted any which may be considered thematic but on occasion my office has had to remind agencies of this particular requirement. I have kept a close eye on the terms of the warrant to ensure that the Secretary of State is able to assess the necessity and proportionality.

GCHQ have introduced a "record of reliance" document to formally record each occasion on which a thematic warrant is used. This is not a requirement under legislation but I encourage others to implement a similar process. At GCHQ I **recommended** that they include a section in the form to direct the user to give specific consideration to confidential material. This recommendation has now been implemented.

It is the submission applying for the warrant which does and should set out all the limitations to the use of the warrant and identifies, for example, what action is being taken to minimise intrusion into privacy. I have **recommended**, that the warrant instrument should indicate expressly that any activity taking place was on the basis of the terms of the submission. GCHQ have already adopted this recommendation and I strongly encourage SIS and MI5 to do so as well.

Renewing Warrants

Although the legislation does not require it, when renewing a 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 Secretaries of State have applied their mind to necessity and proportionality when a warrant is renewed. For the most part my recommendation has been implemented but during 2015 I have on occasion noted that the short form renewal is still being used.

iv. Section 7 Authorisations

Under Section 7 of ISA the Secretary of State, in practice normally the Foreign Secretary, may authorise SIS or GCHQ to undertake acts outside the UK which are necessary for the proper discharge of one of their functions. When authorised by the Secretary of State it seeks to remove personal liability under UK law where the officer has been acting in good faith within the parameters of the authorisation. Authorisations under Section 7 can be for a specific act or for a broader class of activity, known as class authorisations.

Oversight of Section 7 can be particularly challenging because of the multitude of possible acts that could be authorised. Some Section 7s have a standard consideration of necessity and proportionality while in others there is no intrusion into privacy but they may require a lengthy legal consideration.

Authorisations may be for a particular operation or may relate to a broader class of operations. As an overview a Section 7 authorisation:

- removes liability;
- can only be issued to GCHQ and SIS;
- can be highly intrusive or may have no intrusive element;
- must relate to the agency's statutory purpose; and
- provides ministerial approval for the acts authorised.

The agencies do not self-task, all of their operations must link back to the intelligence requirement set by government.

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, when appropriate, acting so as not to intrude on privacy any further than justified by the necessity to achieve what is authorised.

An application to the Secretary of State is accompanied by a submission which sets out the planned operation, the potential risks and intended benefits. The accompanying submissions can be long and there is room for cutting the length down, however, the submission must cover all the relevant points for example:

- a summary of what the submission is about;
- necessity for the proposed action;
- proportionality or reasonableness;
- a separate headed paragraph for privacy and intrusion if applicable;
- risks;

- legal issues which should set out the relevant aspect of law from commercial to criminal and international law; and
- at renewal the benefits obtained so far.

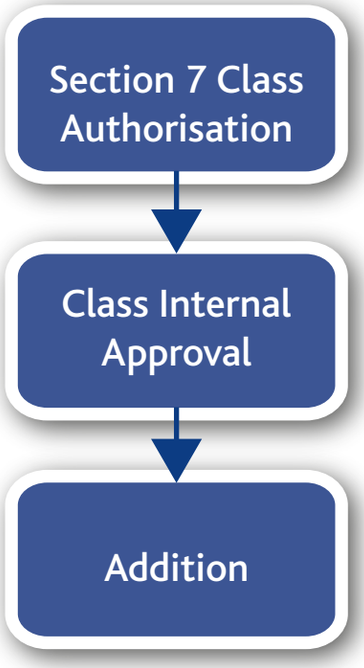
An executive summary may also be useful.

Class Authorisations

Class authorisations cover the core, 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. There are arrangements for the internal approval for the activity under class authorisations.

Government Communications Headquarters (GCHQ) Class Authorisations

Under class authorisations arrangements are in place for internal approvals and beneath those, specific 'additions'. A class authorisation could be for, for example, equipment interference operations overseas to obtain intelligence. An internal approval might be for implant operations within a specific context and then beneath this an addition which could refer in detail to the specific operational activities to be undertaken.



As I said in my previous annual report, I have been impressed with the formality of the audit trail and the level of consideration at GCHQ. It was clear to me that a great deal of thought was given to the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible.
I recommended that these approvals including 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 .

During 2015 I was able to scrutinise additions formally and I again commended GCHQ on their formal audit trail. I was impressed with the consideration given to protecting privacy but believe it could be set out more clearly in the paperwork. These additions made under class authorisations are not a legislative requirement but they are important and I **recommended** that, although necessity and proportionality was being considered, there should be headings in the form so that the consideration of those factors were set out more clearly. GCHQ provided me with updated versions of the forms to implement this recommendation.

These approvals did not have an expiry date but following a **recommendation** I made GCHQ, are conducting an internal review of each one. As they are being reviewed a date is then set for the next review period which may be 6, 12 or 18 months depending, for example, on sensitivities. This is not an expiry date and there is no requirement to set an expiry date but I commend GCHQ for implementing this process.

Secret Intelligence Service (SIS) Class Authorisations

SIS is tasked with operating overseas, dealing with threats and gathering intelligence in order to protect the United Kingdom (UK) and UK interests and the core of their operational work, including agent running, takes place under eight class authorisations. A Section 7 authorisation is there to protect an individual officer from personal civil and criminal liability when acting in the course of their employment. SIS authorisations set out considerations of necessity and reasonableness. When the operation involves intrusion into privacy, they are also required to set out consideration of proportionality and how the intrusion into privacy is justified by the intelligence to be gained.

Record Keeping

As I have said previously, I am keen to see SIS introduce a more formal recording process for decision making. Extensive records are kept in email reports. SIS introduced what was termed a "key decision document" to try and meet my recommendation. That has not been universally implemented. Further forms are in the process of being introduced.

The GCHQ method of internal authorisation may not be applicable to SIS particularly when operating overseas under the authority of a Section 7. However, I have suggested that SIS could, for example, apply the principles of the RIPA authority process so that proper consideration can be given to the same issues and then recorded. It is for SIS to determine how record keeping should be done but I have **recommended** that any process should prompt or guide people through important considerations of necessity and proportionality or reasonableness. In my view this will help to focus the mind at the decision making stage but also help with corporate and formal oversight of operations.

SIS Stations

An important element of my SIS oversight is to visit and scrutinise certain of the overseas stations in which they operate. At stations I am provided with their operational objectives and also technical plans, emails and other documents relating to their current ongoing operations. As I have said previously I am greatly impressed by the professionalism and dedication of the officers in stations often working in difficult conditions.

At one station I scrutinised a directed surveillance operation taking place under the authority of a class authorisation. I asked about collateral intrusion and the SIS officer was able to explain how this was taken into account. However, I noted that there had been no consideration given to this in the planning documents or email correspondence and commented that although RIPA does not apply, the principles should still be considered, and this needed recording.

This was not an isolated incident and highlights to me the importance of putting into place a better audit trail of operations taking place under class authorisations. This needs to come from the top of the organisation to introduce a culture of looking for authority and not relying solely on the Section 7.

v. Equipment Interference

Equipment Interference (EI) is the interference, remotely or otherwise, with computers, servers, routers, laptops, mobile phones and other devices under the authority of ISA Section 5 warrants or Section 7 authorisations.

Essentially EI is an intrusive power which allows the agencies to interfere with electronic equipment to obtain information. This could be, for example:

- interfering remotely or otherwise with computers, mobile phones, servers, routers or other equipment in order to obtain information, including about who owns the equipment, the nature and use of equipment;
- to locate and examine, remove, modify or substitute hardware or software;
- to enable and facilitate surveillance; or
- the creation modification or deletion of information on a device, server or network.

Information obtained may include communications content and/or communications data but all activity must be properly authorised and in pursuit of intelligence requirements.

As long as it is properly authorised, an EI warrant can obtain information stored on a computer or phone, including stored communications before or after its transmission. However, it cannot be used to authorise real time interception of communications. That requires an interception warrant under Part I of RIPA.

A draft EI code of practice was published for consultation in February 2015. An amended version was published in November 2015 and subsequently laid before parliament on 28 January 2016. You can find the code here. In its open response to the Investigatory Powers Tribunal in response to two complaints about EI the government confirmed that the agencies would apply the provisions of the draft code throughout the consultation period. The Code made public the powers and safeguards that existed previously.

The Equipment Interference (EI) or Computer Network Exploitation (CNE) terms have been used interchangeably but for the sake of clarity I have used the term EI throughout. It is worth noting that the activity covered by the EI Code is broader than traditional CNE operations. However, all CNE is EI and the safeguards contained in the EI Code apply to these operations.

Authorisation

The agencies' use of EI is governed by warrants and authorisations issued under the Intelligence Services Act. The EI Code contains guidance the agencies should follow before any EI can take place; it does not confer any new powers.

AUTHORISING EQUIPMENT INTERFERENCE		
WHERE	**WHAT**	**WHO**
UK **(4.1 of the Code)**	ISA Section 5	MI5, SIS and GCHQ
Overseas **(4.2 of the Code)**	ISA Section 5 ISA Section 7	MI5 SIS and GCHQ

Oversight

I have overseen the agencies' use of EI since I first took up post in January 2011 but it has not been possible to report publically on my findings since the existence of this technique had not been publically avowed. Reports of my inspections and oversight of this area have been contained in the confidential annexes to my annual reports.

My oversight is conducted alongside all other ISA warrants and authorisations using the same method as set out on my website and in previous annual reports.

As part of my oversight of this area I require that the agencies designate a senior official responsible for engaging with me during my inspections and overseeing implementation of any post inspection action plans I have recommended or approved, and reporting back as required.

The code of practice requires that particular consideration be given to cases where the subject of an operation might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information includes confidential personal information, confidential journalistic material, communications subject to legal privilege or communications between an MP and another person on constituency business.

As part of my inspections, in accordance with the code of practice, I require that:

- any case where a lawyer is the subject of EI be drawn to my attention during the next inspection and that legally privileged material which has been retained be made available to me;
- where legally privileged material has been acquired and retained it should be reported to me as soon as reasonably practicable – as defined by and agreed with me. Any material still retained should be made available if I request it including detail of whether it has been disseminated;
- where confidential material is retained it should be reported to me as soon as is reasonably practicable as agreed with me, and any material which has been retained be made available at my request;

- the agencies have in place additional internal handling arrangements to safeguard the processing, retention, disclosure and destruction of all information obtained by EI which should be made available to me; and
- all breaches of these handling arrangements must be reported to me.

Points Raised During 2015

Action and Property to be Interfered With

In an application for a warrant the agencies are required to detail the property which is the subject of the warrant, for example vehicles or residential houses, and the actions to be carried out in respect of the property i.e. techniques used by the agencies. Property and actions must be clearly set out so that the Secretary of State is clear what he or she is being asked to authorise. This information is used to construct the warrant instrument signed by the Secretary of State.

On occasion I have noticed that interference with computers is described in the section relating to actions when it should clearly be described as property to be interfered with. This will tend to happen when a warrant is required to enter a house and it is not known at the outset whether there will be a computer inside. I continue to **recommend** that computers must be an identified property on the face of the warrant instrument as property authorised and not an ancillary reference as action authorised. It could be argued that the warrant did not authorise such interference where a computer is not set out clearly as the property identified. MI5 have since implemented a process to address this problem.

It is not possible to amend a warrant issued under ISA so in relation to existing warrants I have **recommended** that the renewal submission should properly attribute electronic media as property to be interfered with. The danger is that the renewal will not pick up the "actions" section since renewals tend only to repeat the relevant property so computers will no longer be set out.

Under the proposals set out in the IP Bill such activity would require a separate Equipment Interference warrant to cover opportunities such as this.

Mobile Media

I voiced my concerns regarding the use of the wording "or other locations" in a warrant. I felt this to be too broad an interpretation of "property so specified". However, I have been persuaded that this has to be a standard requirement for mobile media.

GCHQ Technical Planning Meeting

At GCHQ I attended one of their weekly technical planning meetings. The meeting provides all relevant parties, including GCHQ's policy and legal, with oversight and assurance that EI tools, techniques and usage have been assessed as necessary given the potential benefit to be gained, and that they have been risk assessed.

This assurance and oversight is provided by peer assessment, covering development, infrastructure, operations and policy implications. Key agreements and decisions made during the meetings are documented to provide an audit trail and may be used in submissions to support the necessity and proportionality of using the technique in specific operations.

The meeting spent some time on the technical capabilities of using the technique and the challenges from peer review were at times adversarial. These are obviously bespoke techniques which are very technical but the meeting had to be in plain English so that the legal and policy people could also understand the proposal.

Bulk Equipment Interference

Current legislation does not allow for a bulk EI warrant. Overseas this can be authorised through a Section 7 class authorisation. In the UK it would be a thematic property warrant but the legislation requires that property covered must "be so specified", I discussed this in detail in my 2014 annual report. I would not expect to see a broadly termed warrant which authorises EI against an unspecified target. Individual consideration must be given to the necessity and proportionality of the EI.

vi. Bulk Personal Datasets (BPDs)

Under section 59A of RIPA, the Prime Minister published a direction on 12 March 2015 which put on a statutory footing my oversight of the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets, including any misuse of data and how this is prevented. There is a considerable public interest relating to the agencies holding of BPD and I would like this to be set out in greater detail than heretofore the way in which BPD is dealt with and how my oversight works.

Although at present there is no *statutory* definition of BPDs they are defined as sets of data which contain personal information about a wide range of individuals, the majority of whom are unlikely to be of intelligence interest. These datasets are often very large and cannot be processed or manipulated manually, and so they are held on analytical systems in the intelligence agencies.

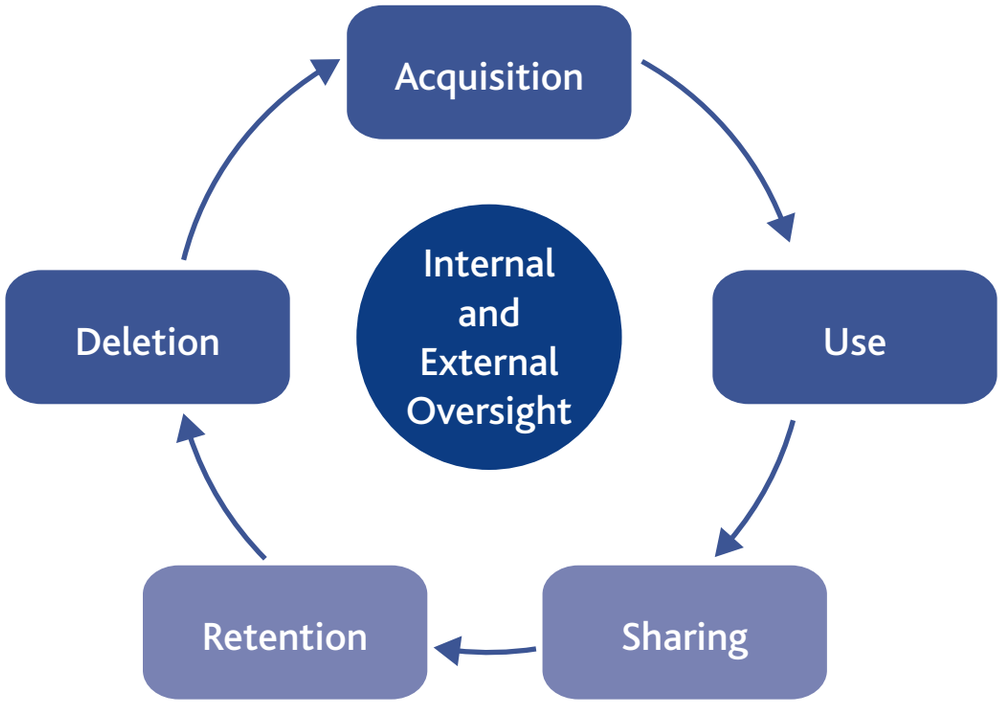
Section 2(2)(a) of the Security Service Act 1989, section 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994, also known as the "information gateway provisions", and section 19 of the Counter-Terrorism Act 2008 allow for the agencies to acquire and retain Bulk Personal Datasets (BPDs) overtly or covertly.

In order to carry out their statutory functions the agencies collect and draw on the datasets using them in conjunction with other information, which could include other datasets that are not bulk personal data, to for example: to fully identify a subject of interest; to obtain travel information of subjects of interest; to find links between them and other individuals or groups of interest; and to validate intelligence acquired by other methods. This capability enables threats to national security to be identified quickly. In my view this capability is a vital tool in the agencies fight against terrorism.

The BPD Lifecycle

Over the last few years a considerable amount of effort has been put into developing and implementing effective processes and policies to manage bulk personal datasets. The agencies have sought guidance and advice from me along the way to ensure that I am content.

There is an overall SIA Bulk Personal Data Policy which guides staff through all stages of the BPD lifecycle: Acquisition; Use; Sharing; Retention; and Deletion, as well as the oversight of BPD. Each agency has their own tailored BPD guidance which is aligned to the joint policy.



Sensitive Personal Data

In handling BPDs the agencies use the definition of 'Sensitive Personal Data' as it is defined in the Data Protection Act 1998 (DPA) and so the following types of information would all be classed as 'sensitive': racial or ethnic origin; political opinions; religious beliefs; membership of trade unions; physical or mental health conditions, sexual life; commission or alleged commission of any offence and any such proceedings for these. In addition to these types of information, the agencies must also record if information on the following is likely to be contained in a BPD:

- UK nationals
- Minors (under 16s)
- Journalistic Sources
- Legal Professional Privilege (LPP)
- Financial

If datasets are likely to include any data which could fall under one of these categories it must be clearly stated on the form requesting authorisation of the dataset. Datasets which contain sensitive information require a more robust justification to evidence why it is necessary and proportionate to acquire and retain the data.

Categories of BPDs

Bulk personal datasets generally fall into the categories below and can be obtained through various channels including: government, law enforcement and covert acquisition. At MI5 I queried that if the BPD is a government database, why they could not just ask the government department for the specific information required rather than holding a copy themselves. MI5 explained that by holding data in house they can fuse it with other sources of data and carry out complex analysis without having to employ more intrusive techniques to receive the same intelligence.

- Population/Biographical
- Travel
- Financial
- Communications
- Commercial

Acquisition of BPDs

In all three agencies before a BPD can be used for operational purposes a senior manager must authorise the use of the dataset. The authorisation form must make clear arguments that acquiring the dataset is justifiable, as well as both necessary and proportionate, in pursuit of the agency's statutory functions. It must also lay out the specific details of the dataset including whether it is likely to include any sensitive information. The agency will assess both the level of intrusion and the level of corporate risk of holding the dataset; which will determine how frequently the BPD is formally reviewed. The form must be endorsed by a legal adviser and a responsible officer designated.

When assessing the level of intrusion of a dataset, careful consideration is given to what the likely expectation of an average person would be about the data, for example would they expect an intelligence agency to hold that information on them. Several factors are taken into account including the expectation of privacy and the level of intrusion that the dataset is likely to represent, the agencies also consider collateral intrusion. This is reflected in whether the dataset is given a high, medium or low intrusiveness rating.

When considering whether to approve or reject an authorisation request, the authorising officer will look at the intrusiveness and sensitivity of the data and the level of corporate risk the agency will bear in holding and using it balanced against the necessity and proportionality case made to acquire and use the data.

If a request is rejected the dataset must not be acquired, or if the dataset is already in the agency's possession then it must be deleted or returned. A BPD cannot be operationally exploited unless the dataset has been authorised.

Use of BPD

Each search the agencies make of BPD must be necessary and proportionate to enable it to fulfil its statutory function. Staff are advised to exhaust less intrusive sources of information before using BPD. BPD is often used to try and identify a subject of interest and to eliminate the need to use more intrusive techniques. The use of BPD is increasingly important to the agencies as the magnitude of the threat increases and other means of acquiring intelligence are made more difficult for example by encryption.

There must be appropriate physical, technical and administrative safeguards in place to prevent and detect misuse of BPD and the analytical system it is held on. Datasets must be hosted on the most appropriate analytical system, taking into account the level of intrusion and the sensitivity of the data. Officers must take the relevant mandatory training and accept the appropriate code of practice or terms and conditions before they can access the systems. Access will only be granted if there is a clear business need and the individual has the correct security clearance.

The position is different as between the agencies. All three have technical systems in place which log all uses of analytical systems and with certain features (which for obvious reasons I am not going to expand on) that identify possible misuse. At SIS for example users have to justify and record the justification for each search of BPD. When I conduct my formal inspections officers know that I can pick any of their searches at random for further scrutiny, they then have to justify why they carried out the search, as well as explain to me why the search was both necessary and proportionate. In addition officers are made aware that disciplinary action will be taken against any staff abusing or misusing the BPDs, more information on the protective monitoring of BPD is covered later in this chapter.

At MI5 all desk officers can apply for access to basic BPD, but their access is limited by their specific role in the organisation and they can only access data that is relevant to their work. There are a much smaller number of 'advanced' users who have access to a larger number of datasets, including those containing more sensitive data. These advanced users are in specialist posts as some of these datasets require more advanced skills to interrogate and are used under a stricter range of security controls. These posts are often subject to sensitive post checks. SIS use a similar regime, they also have advanced analysts who can conduct more complex analysis or search data of a more sensitive nature. If desk officers need such a search they must complete a tasking form setting out the justification for the search.

At GCHQ only a small proportion of the staff have access to BPD, again this depends on the user's specific role, the majority of staff will never have access. Unlike MI5 and SIS, GCHQ does not have advanced users able to conduct more complex searches. Access to a greater number of datasets, or those of a more sensitive nature, is granted on a case by case basis determined by whether the

analyst has a genuine business requirement. Staff who have greater access undergo more comprehensive training on how to undertake complex analysis appropriately.

Sharing

All three agencies have an interest in acquiring and searching BPDs, but they will only seek to acquire a dataset once and will coordinate to prevent duplication of acquisition efforts. Before sharing a dataset with another agency the supplying agency must have justified that it is both necessary and proportionate to do so as well as confirming that it is for the proper discharge of their statutory functions, the receiving agency must do the same for receiving the data. These requests must be approved by a senior staff member at both agencies before any data can be shared.

If the agencies think there is merit in sharing datasets externally then it must meet the necessity and proportionality tests under the Security Service Act or the Intelligence Services Act as well as considering any wider legal, political or operational risks.

Retention

The agencies must keep under review the necessity and proportionality of continuing to retain each dataset. Each agency has a review panel that meets at least every 6 months and invites representatives from the other agencies to ensure consistency across the SIA, as well as legal advisers, technical teams, compliance teams or staff from the relevant business area.

The level of intrusion and the level of corporate risk of the dataset determine how frequently it is formally reviewed. If either level is rated as high the dataset will be assessed by the panel every six months; medium every 12 months; and low every 24 months. MI5 have also implemented additional meetings every two months so that any issues can be raised and discussed straight away, without having to wait for the next formal review panel.

Ahead of the formal review of a BPD at the review panel, the officer responsible for the dataset must update its record to include a retention case including details of how frequently it has been used and, where possible, examples of the operational value it has provided. If a dataset is not being used the review panel can request more frequent reviews to monitor the dataset more closely. They can also revise the levels of intrusiveness or corporate risk if they assess them to have changed since the authorisation or last review, this will also affect the period until the dataset's next review.

In their decision as to whether continued retention should be authorised the panel will consider various factors including: how often the BPD is used; the value of these searches; whether continued retention is necessary and proportionate; the levels of intrusiveness and sensitivity; the currency of the data and how unique it is;

and whether the intelligence benefit could have been achieved by other less intrusive means. If they agree to authorise they can add whether certain caveats or restrictions should be added, or if they reject the case made they will request that the data be deleted. If a retention case is not put forward for a BPD due for review then the panel will want to see evidence of its deletion.

After a dataset has been reviewed by the panel its records are updated with any comments or requests, the date of its next review if authorised or the date of deletion if rejected.

Where a copy of the same dataset is held by more than one of the agencies, each agency must make its own case for its continued retention.

Deletion

The agencies must not hold BPDs for longer than is necessary and proportionate. If the review panel reject the continued retention of a dataset then the appropriate team will be instructed to delete the data as soon as reasonably possible. They usually confirm at the next panel meeting that these datasets have now been removed from all systems.

Similarly if the officer responsible for the dataset can no longer justify the retention of the dataset they request that it be deleted and do not just wait for the next review panel. Or if there is only part of a dataset for which continued retention cannot be justified, then they can request that the appropriate sections be deleted rather than the entire dataset.

When requesting a dataset be deleted the responsible officer must consider whether the dataset has been shared. If the BPD has been shared with another agency the officer must contact them to agree future data ownership responsibilities. The other agency may be able to justify their continued retention if it has a different case.

Oversight

Prior to my inspections I request a list of the BPDs held by each agency. In this list I like to see: a short description of each dataset; the date it was acquired; the date ingested onto an analytical system; the levels of intrusion and corporate risk; when the BPD was last reviewed by a review panel; and if and when I last inspected the BPD. From this list I select a number of datasets at random to inspect in further detail. At the inspection I will be provided with all of the relevant documents and records in relation these datasets to scrutinise, I also speak to the individuals responsible for the dataset. In addition to inspecting individual datasets I also review all of the policies relevant to BPD, I request to see copies of the minutes from recent review panels, as well as overseeing the protective monitoring of the BPD.

At SIS inspections I also make a random selection from the total number of actual searches of BPD that have been conducted by officers since my last visit. I then interview the individuals who have carried out the searches and they must explain how they justified their search to me. It is important that they demonstrate to me: the necessity of why they needed to run the search; why the information could not have been obtained using a less intrusive method; how they narrowed their search criteria to reduce collateral intrusion; as well as explaining the outcome of the search and how the results contributed to their operation. If GCHQ and MI5 could also make this possible during their inspections I would find this particularly useful.

In the list of BPDs provided to me to make my selection the agencies must identify which datasets have been acquired by the interception of communications. I have agreed with the Interception of Communications Commissioner that any BPD acquired via interception, which once processed into a bulk personal dataset no longer identifies itself as intercept product, will be overseen by me in line with my oversight of Bulk Personal Datasets. If the object of an interception is to obtain BPD, the BPD authorisation process will have run in parallel to seeking the warrant. The Interception of Communications Commissioner will of course continue to oversee the interception warrant for obtaining the dataset. I will then oversee the authorisation of the dataset as BPD and its handling in accordance with the BPD Handling Arrangements. If either the Interception Commissioner or I have any concerns about the parts of the process which we individually oversee we have agreed to raise those matters with one another.

In addition to my oversight of BPD, the agencies have a number of internal oversight mechanisms which include controls such as completing mandatory training and signing terms and conditions or codes of practice before access is granted, internal monitoring and audits, this includes the audit of the individual search justifications at SIS and GCHQ.

Findings of the 2015 BPD Inspections

Security Service (MI5)

At the reading days I reviewed the paperwork for each bulk personal dataset that had been reviewed at the most recent BPD Review Panels. For the formal inspections I selected a number of datasets for discussion and closer scrutiny.

On the whole I was very pleased with the level of detail provided in the paperwork and only made some minor points. One of these was around a dataset the ingestion of which into an analytical system had been delayed; I reminded MI5 that the longer the period before the dataset is ingested onto the analytical systems; the harder it is to make a case for retaining the data.

Prior to the inspection MI5 had written to me to report an error in relation to three datasets which, due to an internal error, had not been incorporated into the BPD Review process and so had not been formally reviewed by the review panel, nor had

they been made available for me to inspect. MI5 explained how this had happened and the mitigation now in place to ensure it did not happen again. As soon as this error was noticed the datasets were entered into the next formal review panel. I read the records for these three datasets, and although I made clear that they should have faced a formal review at the correct time, I was content with the justifications detailed in the paperwork for acquiring and retaining them.

At the second inspection I noticed in two instances that despite the paperwork indicating the datasets had been used, in the free text fields of the forms there were comments stating that the dataset had not been used. MI5 explained that although answering the question of how many times the dataset has been used is mandatory, there is not an option to select "No use", therefore officers are selecting the box which states the minimum use possible and adding in as a comment in a free text box that there has not been any use. For clarity I **recommended** that a "No use" box should be added.

I also noticed some inconsistencies in the forms used when a dataset is to be deleted. In some instances a Data Deletion Form had been submitted, whereas in other instances the Data Retention Form was amended to say that there was no longer a case to retain and the BPD Review panel had taken a decision to delete. Following my **recommendation** to be consistent in the forms used for deletion, MI5 have confirmed that there is now one simplified Data Deletion Form which will be used for the deletion of both full and partial datasets.

Secret Intelligence Service (SIS)

During my inspections I was given SIS's updated internal code of practice for conducting BPD searches. This contained some very good information which would go a long way in providing reassurance to the public and would be very useful if this could be published externally. SIS told me that they were looking into how much could be made open.

At SIS staff must complete a justification box for each search to justify that it is necessary and proportionate for the purpose the user has selected, and confirm the intelligence requirement for the search. I requested to see these justifications for the individual searches I had selected for inspection. I advised that the text provided must be enough to evidence that necessity and proportionality were properly considered and users must explain how privacy has been taken into consideration, especially if the search is likely to return results for people of no intelligence interest. On challenging the officers who had conducted the searches I had selected, I was very pleased to see that the necessity and proportionality cases were thoroughly considered. However, I **recommended** that this be recorded, not just for oversight purposes but also for management information purposes. Following my advice SIS have since separated the justification box into 'necessity' and 'proportionality' boxes to ensure both are properly considered.

At SIS I looked at a number of searches conducted by the advanced analysts. I **recommended** that the recorded justifications for each search should specifically give consideration into privacy and that the tasking form should include separate sections for necessity and proportionality. SIS confirmed that advanced analysts always consider ways to minimise intrusion into privacy before they conduct each search. The responsible team communicates regularly with BPD users to encourage them to concentrate on the proportionality of their searches and remind them a disproportionate search would lead to a breach. I **recommended** that the advanced analysts should formally record the ways in which they have minimised intrusion into privacy.

As I reported in my annual report last year I was concerned about the number of datasets that had been acquired but were waiting to be authorised and loaded onto the appropriate analytical system. I was very clear that SIS could not justify the necessity for retaining datasets which they were not exploiting beyond a reasonable period. I am now happy to report that SIS have cleared this backlog and to prevent this problem from reoccurring they have set a target that all datasets will be authorised within six months of acquisition and have implemented a new team to manage this process.

As part of my inspection I was provided with the minutes from the recent review panel. I was very pleased to see that at the SIS BPD review panel held at the end of 2015 a large proportion of the datasets held were reviewed, and all those due for review had been considered.

When I visit stations overseas I speak to the officers who have access to BPD. I question them to confirm they have received the proper training and have signed the code of practice. From their response I was confident the officers understood the need to justify individual searches and that they were happy to request further justifications or refuse requests made by colleagues without BPD access. They explained that this is because users are personally responsible for their searches and that individual searches are subject to random auditing as well as protective monitoring checks, and therefore they would not be willing to take the risk of running a search that was not fully justified.

In my view SIS have made tremendous progress with the internal controls they have implemented for the use of BPD. These processes ensure that all use of BPD is necessary and proportionate and that the considerations are recorded at all stages of the BPD lifecycle.

Government Communications Headquarters (GCHQ)

On the whole I was content with the BPD paperwork provided for my inspections this year. However during the second inspection I discovered a BPD form which was not dated and there were apparent gaps where the internal processes and paperwork had not been properly completed in accordance with the GCHQ BPD

handling arrangements. Despite paperwork in 2013 stating that there was not a sufficient case to retain this particular dataset it remained on the analytical system for a further two years. GCHQ explained that this error had been caused by the dataset not having a nominated responsible officer. When ownership was transferred to another officer they immediately discovered the error and requested the dataset to be deleted. I was very clear that this is exactly what should not happen and was deeply concerned that there might be other examples. I **recommended** that all of the BPD paperwork should be searched to confirm that there were no other cases such as this. GCHQ have since confirmed that they have conducted this search and I expect to see the results at my next inspection.

During the inspection GCHQ brought to my attention a dataset where authorisation was not sought before it was shared with the other agencies, this is not in compliance with the BPD Handling Arrangements which require authorisation to be sought before any BPD is shared. Retrospective authorisation was sought after the error was discovered. I welcomed the fact that GCHQ raised this error, I acknowledged the urgent nature of this particular situation, but made clear the Handling Arrangements are clear and must be followed even in urgent situations.

Protective Monitoring

As I touched on earlier, the agencies employ a number of internal controls to prevent misuse of BPD; protective monitoring is one of these. Protective monitoring is the term given to the audit of BPD including both access to the analytical systems as well as the actual use. I like to see where possible the results of protective monitoring across all systems so I can be sure that the system as a whole works.

At all three agencies there are automatic processes in place to monitor and record each search of BPD in analytical systems. Searches can be triggered for investigation if, for example, a search is made which includes a term which is pre-defined by the protective monitoring team or if an officer attempts to search datasets which are not permitted within their current access rights. There are also random audits on individual searches.

During my inspections the protective monitoring teams at each agency present all of the investigations into possible cases of misuse and the results of random audits they have conducted since my last inspection. From this I am able to discuss any investigations which I feel are particularly concerning, or if I would like further information to determine that the investigations conducted have been thorough and that the correct conclusion has been reached. I am also very interested in what actions have been taken as a result of the investigation conclusions.

Summary by agency

MI5

When I inspect protective monitoring at MI5 this extends beyond the use of BPD and I look at protective monitoring measures in place across the organisation. This provides me with reassurance that the system as a whole works. I saw the results of all of the protective monitoring mechanisms in place, including the "false positives" where potential misuse has been flagged but on investigation a valid business justification was provided for the search.

In relation to non-BPD investigations a large proportion of the breaches issued were for searches of operational data which fell outside of the officer's specific remit of work. Throughout the year there were six instances where unauthorised devices had been inserted into MI5 systems, for example charging a mobile phone. I take these breaches very seriously and I wanted to know what actions had been taken to prevent reoccurrence. MI5 explained that a notice has been circulated re-emphasising that phones cannot be charged at computer terminals. I was also concerned to see that a number of the breaches issued in relation to these non-BPD misuse investigations, as well as one BPD breach, were by individuals who were not permanent MI5 staff. It is very important that the parent organisations treat breaches as seriously as MI5 do when a breach is issued to a member of their own staff. MI5 explained that they had written to the organisations concerned stressing the gravity of the issue and expressed their displeasure at the situation.

I was also keen to understand why the number of breaches had significantly increased in relation to one particular non-BPD database. MI5 explained that this was due to a change in the policy which governs what staff are permitted to search for on this database. Staff were not applying the new policy when they ran their searches. I recommended that a warning could be added to the system, or if this was not possible, then a notice should be circulated to remind staff of the new policy and inform them that I am very concerned about the high number of breaches. At my next inspection I do not expect to see such a high number of breaches.

SIS

The protective monitoring arrangements at SIS are highly classified, access to and knowledge of the techniques is highly controlled. Staff who work in this area are subject to additional security screenings before they gain access to the systems or understand the actual checks that are in operation to detect anomalies and misuse of BPD. The results of these checks are monitored by the team who seek additional information or launch investigations if there are any concerns of misuse. They also provide advice and answer any queries from officers in relation to their searches and the justifications required before a search can be run.

In the first half of the year there were no disciplinary cases, moderate or minor breaches at SIS in regards to their use of BPD. In the second half of the year protective monitoring tripwires led to two moderate breaches being issued. Across both periods SIS carried out regular random investigations. These investigations are not generated by protective monitoring tripwires but look at the justifications given for each search to ensure each search is necessary and proportionate. No breaches were issued as a result of these investigations.

Two breaches have occurred in SIS where users were able to use their previous access to BPD in a different role within the organisation. Use of BPD is job specific and BPD access restrictions must be manually updated each time users change roles. To try and prevent such breaches SIS have briefed the IT Access Management team to ensure they are following the correct procedures when users move roles and have updated their BPD Code of Practice and informed all BPD users to say: "If your role changes and you are required to do work that is different to the role described on your original BPD application form, you must consult the data compliance team".

I am particularly impressed at how rigorously the team monitor the use of BPD, the only point I will continue to repeat is that the disciplinary measures for misuse need to be consistent across all three agencies.

In relation to overseeing the use of protective monitoring across areas other than BPD, I was given a summary of the results of protective monitoring and investigations conducted across SIS' corporate network, which was very useful in showing how effective and comprehensive the protective monitoring checks in place are.

GCHQ

Similarly to SIS the protective monitoring arrangements at GCHQ are highly classified and subject to additional security clearance.

This year I was shown the protective monitoring checks that are in place at GCHQ and I was very pleased to see that the level of monitoring in place was exactly what I would want to see. These do not extend over all operational systems, but they do cover all of the key systems including BPD. Although I recognise my statutory oversight in respect to protective monitoring is limited to bulk personal data I would like access to protective monitoring of personal data across all operational systems at GCHQ. As I have discussed in relation to the other two agencies having sight of investigations and breaches detected in other areas outside of BPD helps to provide assurance that the system as a whole is robust. This year GCHQ have shared with me the results of protective monitoring across a number of their other operational systems

In the first half of the year there was no misuse of GCHQ's BPD holdings. There were however 14 investigations which were triggered as a result of the protective monitoring systems. Although GCHQ confirmed that on investigation all of these searches had a legitimate business reason and were both necessary and proportionate, I requested further information about these flagged searches as well as the investigations conducted.

In the second half of the year there was no misuse of GCHQ's BPD holdings, the results of protective monitoring on another operational system were brought to my attention for which there were four investigations, none of which resulted in a breach.

I raised the point as I also did at MI5 and SIS that I am keen to see the agencies work together to ensure that misuse of data is sanctioned in the same way. In response to this the agencies have set up a working group to align SIA breach and disciplinary policies and I look forward to learning of its progress in 2016.

vii. Consolidated Guidance

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 Guidance).

The express focus of the Consolidated Guidance is on torture and cruel, inhumane or degrading treatment (CIDT) and this is consistent with there being an absolute prohibition in national and international law on any such conduct and with the fact that the practical concern is with extremely vulnerable individuals, namely, those in State detention outside the UK.

In November 2014 the Prime Minister tasked me to examine the concerns the Intelligence and Security Committee of Parliament (ISC) raised on the Government's responsibilities in relation to partner counter-terrorism units overseas. This report is being published supplementary to my annual report. In this section I report on compliance with the Guidance during 2015.

Overseas Security and Justice Assistance (OSJA) Guidance

On 28 February 2014 a revised version of the OSJA guidance was published which applies to all HMG officials including the intelligence services. During 2015 I have seen that the agencies and MOD take OSJA into account when they share intelligence or receive intelligence. I am required to keep under review compliance with the Consolidated Guidance so I have limited my observations to that. However, I have said more about this in my supplementary report relating to the concerns of the ISC.

What I Oversee

a) When a detainee in the custody of a foreign liaison service is interviewed;

b) When information is sought from a detainee in the custody a liaison service;

c) When detention is solicited;

d) When information is shared with a liaison service relating to a detainee; and

e) When unsolicited information is received from a liaison service relating to a detainee.

With regards to the first three it is normally quite easy to see that the Guidance applies and must be taken into consideration. I have made it clear to the agencies and to the MOD that when information is shared they must also consider if detention is the likely outcome and not just that it relates to a detainee. When unsolicited intelligence is received the agencies must consider if continued receipt of intelligence might be perceived as encouragement to continue sharing or of the methods used to obtain it.

How I Oversee the Guidance

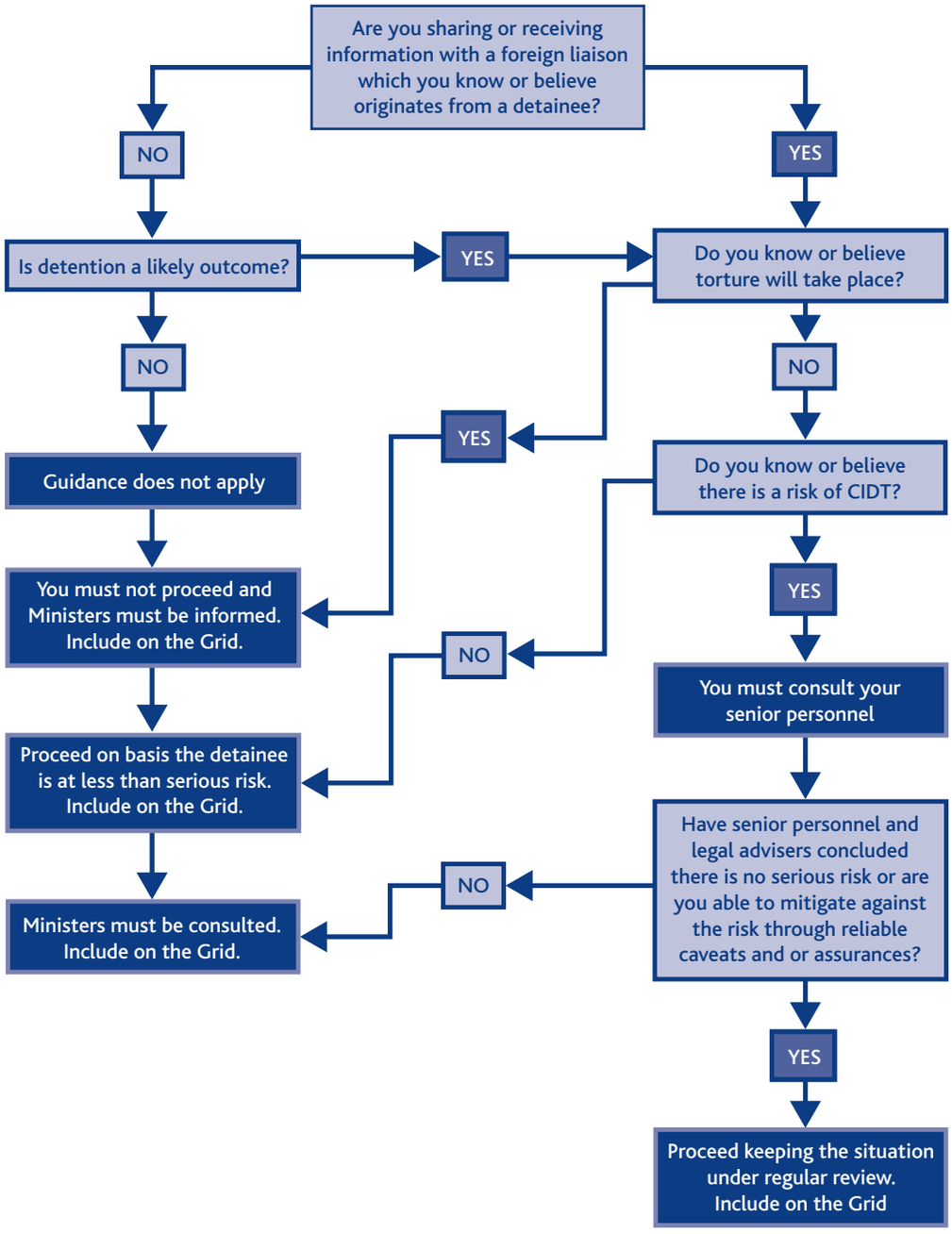
In my oversight of the Consolidated Guidance I seek to monitor whether the guidance is being followed properly so that when a detainee held by a third party is involved staff know and understand immediately that the Guidance applies and that decisions are then taken at the correct level. To do this I apply the judicial review principle so I do not second guess the decision to share or not to share intelligence or consider whether I would come to the same conclusion. Instead I check to see that a reasonable decision was made and the correct tests are applied. I have explained in previous reports that I conduct this oversight though a grid which sets out individual operational cases where the Guidance has been considered and the level at which the decision was taken. I encourage the agencies to include cases where they considered the guidance but determined that it did not apply, either because intelligence would not be shared/received or because the country has a good human rights record and proper due process. For the most part the grids were accurate. Errors were minor and tended to be because the agency was attempting to be helpful. I have **made it clear** the grid must set out what was done at the time and not what the agency now knows to have occurred.

I selected some cases for closer scrutiny. The agencies provided me with supporting documents and/or Ministerial decisions to help demonstrate compliance.

Following my inspection the head of my secretariat produces a separate inspection report relating to the Guidance covering points made during the inspection and recommendations made to either improve or demonstrate compliance.

Does the Guidance Apply?

The Consolidated Guidance provides further information relating to passive receipt of unsolicited intelligence and questioning a detainee but in the majority of situations the officer concerned must consider:



I also expect to see cases included on the grid if at any stage a decision is taken not to proceed because the likely risk of CIDT does not justify sharing intelligence.

Forms

I was content that both the MOD and MI5 had good forms which guided users through the process of considering the Guidance and recorded that consideration and compliance with the guidance. GCHQ had different paperwork and I **recommended** they consider the forms used by MI5 and MOD to guide their application of the Guidance with a view to incorporating it into their process.

At SIS I noted that their record keeping in relation to the Guidance had greatly improved and they were now in line with the grid format. I **requested** that they flag up if they were relying on a Ministerial submission.

Mitigating Against Risk: Liaison Relationships and Assurances

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 of CIDT. Given that SIS own the liaison relationships, MI5 and GCHQ use their assessments.

When SIS believe that they are able to work with a liaison partner because they have been able to mitigate against risk through reliable caveats and assurances they will submit to the Foreign Secretary setting out the reasons why they believe that there is a less than serious risk. The guidance only requires submission to a Minister if there is a risk of mistreatment but in this way the Foreign Secretary is made aware of possible risks and how SIS have mitigated them.

I have continued to re-iterate that, when obtaining assurances to mitigate against CIDT by liaison partners, best practice is to obtain them in writing wherever possible. If it is not possible to obtain written assurances from the liaison partner then a written record of oral assurances should be sent to the liaison partner. At a very minimum there must be a written record of any oral assurances. Obtaining written assurances signed by a liaison partner can be difficult and has to be delicately and diplomatically handled. I **recommended** to SIS that they reconsider their form of words used when they seek assurances and tailor them to each situation so that liaison services would be more likely to sign them.

It is important that compliance with assurances is monitored. I was shown evidence that SIS investigate if an allegation is received to suggest that a liaison partner is not complying with the assurances received. If a credible allegation is made they will cease intelligence sharing while the allegations are investigated through diplomatic channels.

Where SIS write to Ministers to set out their belief that there is no serious risk of mistreatment or CIDT because they have received assurances, MI5, GCHQ and MOD often rely on this assessment. When this happens I have asked that this is reflected in the paperwork provided to me and in the grid for oversight. I expect to see that individual assessment is made to ensure that the particular incident of intelligence sharing falls within the parameter of SIS's ministerial submission.

Due Process

In situations involving serious risk of CIDT the Guidance is clear that Ministers must be informed and decisions should be taken on a case by case basis. The Guidance is clear that the lawfulness of arrest and detention must be taken into consideration as unacceptable treatment.

There are occasions where there has not been proper due process because every day inefficiencies in the system caused a detaining authority to miss their own deadline by a day or two, for example for bringing the detainee before a judge. The Guidance does not differentiate between minor failures and more major procedural failures.

In relation to due process, I have discussed with SIS at what point they should revert to the Foreign Secretary on detainee issues when the lack of due process is being considered. Do they have to revert to a minister in each case or could the minister consider the situation in a 'framework' submission? My advice has been that if the consistent point relates to minor issues like missing a deadline by a day, a framework submission could be used, otherwise particular situations must be referred to the minister if the Guidance is to be complied with.

Unsolicited Receipt

The Guidance covers receipt of unsolicited intelligence from countries detaining an individual. If the agencies know or believe the intelligence has come from a detainee who has been mistreated they must not continue to request further intelligence so as to encourage the detaining country to understand they approve of the mistreatment. The agencies also have to deal with situations in which it is a third party country which has received information and has passed it to the agencies. The consolidated guidance does not apply but in such situations I **encourage** the agencies to apply the Guidance as far as they practically can and they are keen to do so. If in doubt a minister should be consulted and the minister should be supplied with all steps being taken to mitigate the risk of mistreatment.

Non-State Armed Groups

The Guidance also does not apply in relation to non-state armed groups. However, in a paper published by Chatham House they recognised that these groups may need to be engaged with for the sake of the people who live in the territories they control. Although the Guidance does not apply I again encourage the agencies to apply the principles of the Guidance as far as they practically can. There are situations where not engaging with these groups would be difficult to defend, for example if they are detaining or have information about the detention of an aid worker. Again Ministers should be informed and that should include action taken to mitigate against risk of mistreatment.

Continued Oversight

The IP Bill does not make provision for oversight of the Consolidated Guidance under the proposed Investigatory Powers Commissioner. However, there is provision for the Prime Minister to issue directions in the same way he has done previously. I hope that such a direction is made and that oversight of the Guidance continues after the Bill is implemented. The agencies welcome oversight of this complex area so I believe they would also prefer for it to continue.

Statistics

These statistics require a strong caveat. The cases provided in the grid include cases when the Guidance was considered but a decision was taken that the Guidance did not apply or cases where the UK was confident that there was a less than serious risk of CIDT. These figures simply reflect that proper consideration of the Guidance was applied and nothing more in these cases.

The total number of cases where the Consolidated Guidance was considered during 2015 was **442**. Of these I reviewed **68** cases.

Conclusion

At MI5, GCHQ, MOD and SIS I was content that in all instances I reviewed agency and MOD staff had considered the risk of mistreatment or unacceptable conduct as set out in the Guidance. Staff demonstrated that they had considered the risk of mistreatment or unacceptable conduct of any detainee as set out in paragraphs 9 – 11 of the Guidance. I found that the grids presented to me had, for the most part, been completed properly. Any errors were minor.

GCHQ reported a number of occasions where the duty officer had not considered that the Guidance applied before sharing intelligence with a foreign liaison. In each case GCHQ quickly recognised that this had happened and conducted a retrospective assessment. All of this was set out for me in the grid and available for my oversight. Although this is unacceptable, GCHQ assured me that it is being reviewed as part of a wider review of the duty officer's functions.

4. PRODUCT OBTAINED AND HANDLING ARRANGEMENTS

In my report last year I said that for the last two years I have asked that my oversight be extended to the use by the agencies of operational data obtained under Part II of RIPA or ISA Sections 5 and 7. This is now an explicit part of my oversight of Equipment Interference and, as I said last year, 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 my remit.

Last year I asked the agencies and the MOD to be clearer about:

- 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 not of intelligence interest;
- the procedure to handle information not to be retained;
- the policy for deletion of all product;
- procedures enforcing compliance with handling arrangements.

With that in mind I asked the agencies to provide me with their handling arrangements and I have been provided with them by all three agencies and the MOD.

Initially I was supplied with arrangements relating to the rules in place for dissemination of intelligence. I was pleased to see that these arrangements were in place but I also wished to see arrangements in place regarding retention, storage and deletion. This intelligence may relate to an individual's private or family life and may constitute an interference with their Article 8 rights. The authorisation process provides consideration of the necessity and proportionality of obtaining the intelligence but similar consideration must be given to disclosure and retention.

The arrangements are set out in a number of different documents so I have recommended that there should be one document which can then be referenced in submissions. Rather than saying that intelligence will be retained "in accordance with the normal handling arrangements" it ought to reference which section of the arrangements apply and these arrangements should be made available to the Secretary of State, the warrantry units and to the relevant oversight body.

5. ERRORS

The Equipment Interference (EI) code of practice introduced a new, mandatory, category of error reporting any breach of the EI handling arrangements. This is additional to the error reporting process already in place and set out in previous reports. However, in view of this new requirement I have reviewed the categories of error reporting and clarified what I require from the agencies and the MOD.

Category A Errors

Administrative errors are an obvious "slip" where no unauthorised intrusion into privacy had taken place as a result of the slip.

An administrative error occurs where:

- it is clear on the face of a document that a typing error has occurred,
- the correction is obvious, and
- a court would amend it under its "slip rule".

The "slip rule" allows a court to correct an accidental slip or omission in a judgement at any time if it does not reflect the court's intention. In this context, administrative errors could be an obvious administrative mistake such as a misspelling, incorrect year or failure to update a template.

I have asked that when discovered, these administrative errors are bought to my attention. This should be done in writing bi-annually at inspection.

Category B Errors

As I set out in my 2014 Annual Report, as part of my oversight function and in addition to my bi-annual inspection, I require the agencies to report to me any errors that are discovered to have occurred inadvertently during a warrant application, authorisation or during the operation of the warrant.

These could be, for example:

- an inadvertent failure to obtain an authorisation;
- operating under a lapsed authorisation, an inadvertent failure to renew an authorisation;
- operating outside the parameters set out in the authorisation in the mistaken belief that it was authorised; or
- failure to comply with other requirements of the Codes of Practice such as record keeping.

In these cases, but for the inadvertence, the application would have been granted and/or any conduct would have been properly authorised.

In relation to Equipment Interference any breach of handling arrangements must be reported to me in accordance with the code of practice.

For Category B errors the error should be reported formally to me within three months of the date the error was discovered. I expect the report to explain:

1. when the error occurred
2. when it was discovered
3. the nature of the error
4. how it happened
5. what, if any, unauthorised intrusion into privacy resulted
6. what, if any, product has been obtained and what has happened to this product
7. the steps taken to prevent a reoccurrence of this error.

If it is not possible to report the error within this time because of the investigation required then I require the agencies to send an interim notification to my office.

Category C Errors

This would be a deliberate decision taken to obtain information without proper authorisation or in any way to act irresponsibly. Once again this year, I have not found or had reported to me any Category "C" errors. Such deliberate acts must be reported to me immediately upon discovery. If such a deliberate act were to be committed, those involved would be subject to disciplinary action and possible criminal charges.

Reporting Errors

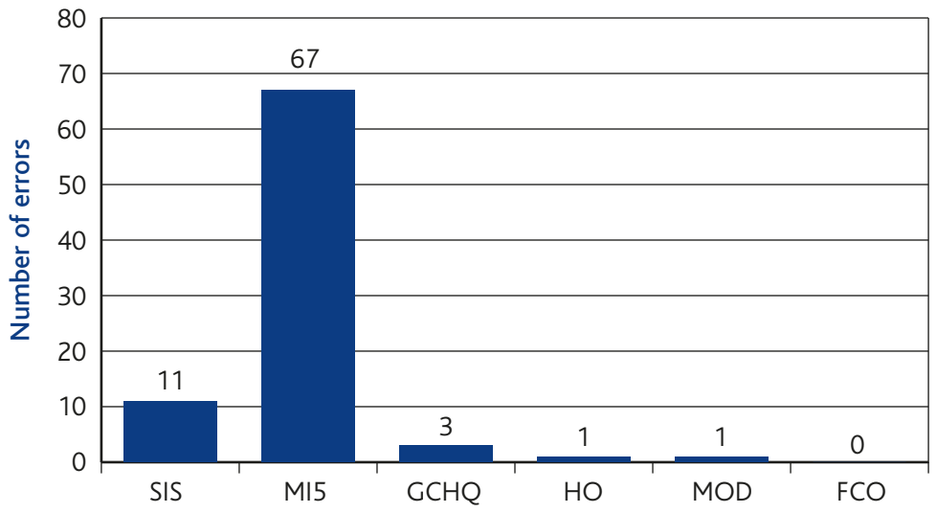
My main concern has been the time taken to report errors. I have agreed with all agencies a procedure by which they notify any potential error they discover which may take longer to investigate and then agree with my office a timescale for reporting if an error has occurred. As I requested last year the agencies now notify me when they anticipate an error investigation will take longer than the three month time limit for reporting errors, and that is an improvement from 2014.

Unfortunately sometimes the agencies still exceed the agreed timescales. For example in one case at GCHQ I was informed that a potential error had occurred in January and following a rigorous and extensive investigation it was then only formally reported in July. But on the whole there has been an improvement and the agencies are conscious of the need to report as early as possible.

Summary of 2015 Errors

In 2015 there were a total of 83 errors. This is quite a significant rise from the 43 errors of 2014.

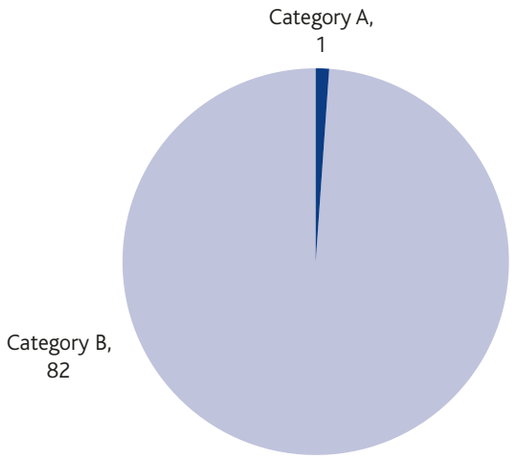
Errors reported in 2015 by organisation



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

82 were Category "B" errors or inadvertent errors and only one was a category "A" or administrative error. There were no Category "C" errors which was the same as 2014.

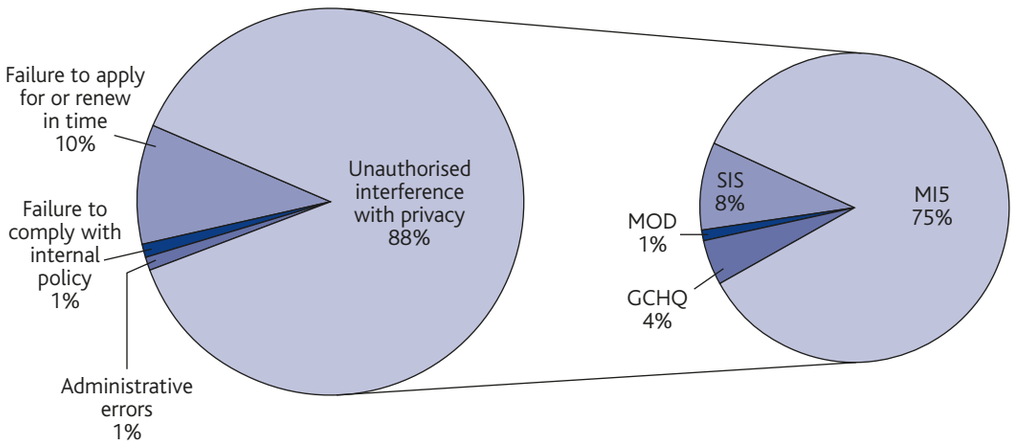
Errors reported in 2015 by category



Of all the errors, the most common error was because of an unauthorised interference with privacy. The least common errors in 2015 were due to administrative reasons. There were no recorded errors that were due to unauthorised disclosure in 2015.

If we look at the breakdown of errors due to unauthorised interference with privacy then we see the majority of these were made and reported by MI5.

Breakdown of 2015 Errors by Type and further breakdown of the unauthorised interference with privacy



Breakdown of errors by organisation

Security Service (MI5)

In 2015, MI5 reported 67 errors to me. Of the 67 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;
- if proper authorisation or proper procedures had been followed the authorisations would have been granted;
- these errors were caused by a variety of reasons for example allowing an authorisation to expire, failure to apply in sufficient time or misnaming.

Secret Intelligence Service (SIS)

In 2015, SIS reported 11 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 11 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.

Government Communications Headquarters (GCHQ)

In 2015, GCHQ reported three errors to me which resulted in unauthorised interference with privacy. None were caused with the intent to obtain information without the proper authority.

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.

Home Office

During my inspections of the Home Office Warrantry Unit, one administrative error or Category "A" error was brought to my attention which I asked the Home Office to write formally to me about.

MI5 had reported to the Home Office that they had made a slip on the wording on the face of the warrant. I advised that the Home Secretary could correct in manuscript and initial and date the amendment, but the Home Office explained that it had been renewed since then so a new warrant had been sought. In that circumstance I accepted that this was the correct thing to do, advising them to report an administrative error.

Ministry of Defence

The Ministry of Defence reported one error to me during an inspection, which I asked that they formally report to me.

The error occurred during two periods of directed surveillance which took place without any formal authorisation where surveillance teams were deployed for a length of time believing a DSA was in place. Once the error was recognised surveillance stopped until a DSA was in place.

6. RIPA/ISA STATISTICS

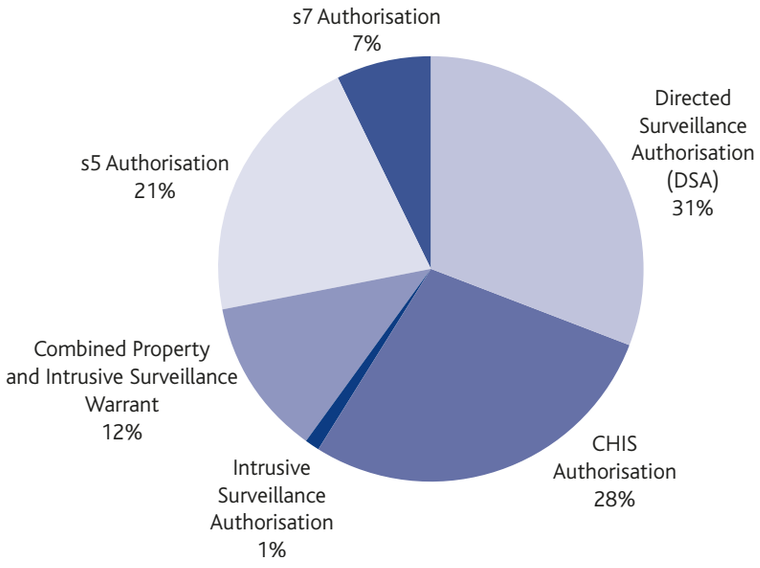
I select warrants to scrutinise from a full list of extant warrants and authorisations provided by the agencies and the MOD. Included in these lists is a short description of each warrant and authorisation. In this list I see *all* authorisations and warrants presently in place. I then select a number of these for closer scrutiny at my formal inspections where I examine the authorisation or warrant itself, as well as all of the supporting documentation including, for example, the submissions written to Ministers.

The total number of RIPA/ISA warrants and authorisations extant at the end of 2015, across the agencies and MOD, was **1,560**.

This figure does *not* include renewals so, for example, if it is necessary and proportionate for the activity to continue a DSA needs to be renewed every six months. The first authorisation is only for three months, each renewal after this is for a six month period. So a DSA could fall for renewal twice in one year.

In broad terms the types of warrants and authorisations I oversee which were authorised during the year, including renewals, are as follows:

Breakdown of Warrants/Authorisations issued during 2015



Of the RIPA and ISA warrants and authorisations in effect in 2015 I scrutinised **499**. Each authorisation or warrant has multiple supporting documents so the number of documents I scrutinise is much higher. I also scrutinise a number of internal approvals made or issued under certain Section 7 authorisations which are not included in the figure above.

7. BRIEF SUMMARY OF ASSESSMENTS

Security Service (MI5)

	Round 1	Round 2
Selection	11 May	20 October
Pre-Reading days	1-3 June	24-28 November
Inspection days	24 June	16 December
Under the bonnet	13 January	29 September

MI5 Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made the case for necessity in the individual cases.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out in the paperwork I selected for scrutiny.
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 separately and properly weighted in the paperwork I selected for reading. I would like to see the case set out how MI5 will minimise intrusion into privacy which is not required to meet the intelligence need.

Prior to inspection MI5 informed me about their proposed Retention, Review and Disposal (RRD) policy for warrants, submissions and associated paperwork. They previously stored all paperwork in hard copy at a secure storage facility which was running out of space. They proposed that:

- Live warrants be kept in hard copy;
- Cancelled warrants be retained in hard copy for 5 years then scanned onto their system and kept in soft copy only;
- Pre-existing warrants cancelled more than five years previously would be destroyed;
- Submissions would remain available if required;
- The product obtained through warrants is covered by separate arrangements.

I **agreed** that the proposals appeared both sensible and in line with the code of practice but suggested waiting until IOCCO completed their review of retention of warrantry documentation before taking a final decision.

I raised a number of other issues:

- I asked MI5 and the Home Office to ensure that applications to renew a warrant be made shortly before expiry and the Home Secretary be provided with the most up to date information to consider.
- Ensure training and guidance is sufficient to make sure the correct form of words is used when a device is waiting for extraction so that it reflects that it is no longer proportionate to use the device for intelligence purposes.
- I noted that MI5 often fail to set out in their submissions consideration of the steps taken to minimise or mitigate intrusion into privacy and record what they will do with any product obtained which is not of intelligence interest. I am satisfied that this takes place but believe it should be better recorded.

Secret Intelligence Service (SIS)

	Round 1	Round 2
Selection	8 April	20 October
Pre-Reading days	6-7 May	10-11 November
Inspection days	13-14 May	17-18 November
Station Visits	9-10 March (Europe)	27-29 October (Europe)
Under the bonnet	28 May	18 November

SIS Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made out the case for necessity in the individual cases.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The cases for proportionality were set out in the cases I selected for scrutiny. There was one Section 5 warrant which I recommended required further work to ensure the property covered is more specific.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected. In one overseas station visit the cases for privacy were mostly set out in the paperwork viewed although improvements could be made in recording this. In addition collateral intrusion was not evidenced in one particular DSA authorisation.

I assessed that the operations I selected for scrutiny were lawful but in some cases the argument for necessity, proportionality and privacy could have been set out more clearly in the paperwork.

At each inspection, both in the UK and at overseas stations, I discussed SIS substandard paperwork and the need to introduce a more formal process to record decision making and provide a better audit trail. When operating overseas under the authority of an ISA Section 7, SIS should apply the same principles as the RIPA authorisation process so that proper consideration was given to the key issues including necessity and proportionality, and this consideration recorded. Doing so would allow for improved accountability, proper management and facilitate oversight. Although I was confident that proper consideration was given it was not possible to see this set out in one document.

I also raised a point at the FCO. If the Foreign Secretary had commented so as to restrict the use of a warrant then this should be properly reflected on the face of the warrant and, if it was not, SIS should return the warrant to the FCO to reflect this.

At SIS I emphasised that with the advent of the Investigatory Powers Commission it would be more important than ever to ensure record keeping across the organisation is done to a consistently high standard. SIS introduced a 'key decision document' to be used to record decisions. That has not been very effective and recently a further set of forms has been produced which hopefully will produce better records of decisions and how they were reached.

Government Communications Headquarters (GCHQ)

	Round 1	Round 2
Selection	12 March	17 September
Inspection days	21-23 April	21-23 October

GCHQ Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made out the case for necessity although this could have been set out more clearly in the Section 7 electronic addition process.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out in the cases I selected for scrutiny although this could have been set out more clearly in the Section 7 electronic addition process.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected apart from additions which did set out separate consideration.

I believe that GCHQ are doing a very difficult job well and that staff are working hard to get things right. GCHQ paperwork was of good quality and the various forms were much improved. The Director of GCHQ said that oversight was useful in emphasising to staff the importance of full and accurate documentation.

The operations I selected to scrutinise were lawful and the paperwork was generally in good order but in some cases the argument for necessity, proportionality and privacy could be set out more clearly in that paperwork.

GCHQ briefed me on their compliance review which took place in April-May 2015. It covered everything from authorisation and storage to retention and deletion of product. One issue the review highlighted was analysts retaining data outside of corporate repositories, for example on local drives, which was not then deleted at the appropriate time in accordance with GCHQ policy. The GCHQ Board strongly endorsed the recommendations made. I asked to see this formal report and GCHQ provided it for me.

Following my earlier **recommendation** GCHQ now sets out clearly in their warrants that they are subject to the conditions described in the accompanying submission.

Ministry of Defence (MOD)

	Round 1	Round 2
Selection	12 May	2 November
Inspection days	4 June	19 November

MOD Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The cases I selected for scrutiny made out the case for necessity.
PROPORTIONALITY **Was the case for proportionality made In each case inspected?**	The case for proportionality was set out in the paperwork I selected for scrutiny.
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 scrutiny.

HMG does not accept that RIPA Part II applies to activities outside the United Kingdom but the authorisations are obtained as if it did. I was impressed by the high quality paperwork produced in the areas I oversee at the MOD, particularly by the Special Forces.

The MOD voluntarily apply a high compliance standard to RIPA principles. I noted that the paperwork was good and that necessity and proportionality had been properly considered. As a minor point I would like to see some more detail setting out what would happen to intelligence obtained through the use of intrusive techniques. However, I was satisfied that arrangements were in place. I asked that the MOD make their data retention policy available during my scrutiny visits in future and also asked the MOD to set out in the "intrusion" section of the RIPA forms details of how product would be managed, and this could refer to paragraphs of the data retention policy.

I **recommended** they create a stock form to allow them to modify a DSA authorisation.

Home Office

	Round 1	Round 2
Selection	10 June	27 November
Inspection days	25 June	10 December

Home Office Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The submissions provided for the warrants I selected made 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 scrutinised, although consideration of LPP material was missing from one property warrant which I requested be followed up.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected. However, consideration of how to mitigate against unwanted intrusion into privacy was not always evident.

On the whole I commended the Home office for the quality of its paperwork, including comments on applications and appropriate push back to MI5. They provided me with a useful document 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 well with a few recommendations which I will continue to monitor. I saw evidence that the warrantry unit questioned the submissions made by MI5 as and when appropriate.

On one occasion I noted that where a number of people were mentioned in a submission it was not reflected on the face of the warrant. It would be better to name the individuals when known. The Home Office agreed and explained that they would normally do so but there had been an oversight in this case.

There were a number of warrants in which interference with computers was mentioned in the section relating to actions when it should clearly be described as property to be interfered with. I was clear that this was not satisfactory and interference with computers must be set out as property to be interfered with. As the Home Office are responsible for drafting the warrant instrument I asked them to ensure this does not happen in future.

The Home Secretary takes her responsibility to consider the necessity and proportionality of what she will be authorising very seriously. In addition to the submission from MI5 her staff do a detailed one considering the case necessity and the question of proportionality. She applies herself personally to the appropriate considerations.

Northern Ireland Office (NIO)

	Round 1	Round 2
Selection	14 May	29 September
Inspection days	8-9 June	4-5 November

NIO Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The paperwork provided made a case for necessity.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was mostly set out clearly in the paperwork I reviewed. Proportionality could be improved by setting out what will happen to product obtained which is not of intelligence interest.
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 I reviewed. Consideration of collateral intrusion, ways to mitigate against this and what would happen to any product obtained was sporadic.

I was satisfied that the paperwork provided was in good order and there were no slips or errors. NIO generally put a lot of care into the papers presented to me and make themselves available to answer any questions or produce any documents I request. I observed that the NIO are thorough and careful when looking at submissions from MI5 and ask for clarification as needed before submitting to the Secretary of State.

I raised points around privacy, collateral intrusion and management of product obtained. Most of the submissions I scrutinised highlighted the potential for collateral intrusion, whether this was into family members', co-habitants' or others' privacy. But many did not then go on to specify how this intrusion would be limited or mitigated and what would be done with any product of collateral intrusion. I **recommended** that NIO and MI5 work together on the description of collateral intrusion and the steps they can take to limit it, as well detailing how any collaterally obtained product would be dealt with. NIO agreed to take this forward with MI5.

Foreign and Commonwealth Office (FCO) for SIS

	Round 1	Round 2
Selection	8 April	20 October
Inspection days	14 April	18 December

FCO (SIS) Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The submissions I scrutinised mostly set out a case of necessity. In one case this could have been set out better.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork I reviewed.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?** **Has privacy been set out as a separate consideration?**	Privacy considerations were set out in the cases I selected.

Foreign and Commonwealth Office (FCO) for GCHQ

	Round 1	Round 2
Selection	13 April	11 November
Inspection days	17 April	30 November

FCO (GCHQ) Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The submissions provided for the warrants and authorisations I selected for inspections made the 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.
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 inspected.

Foreign and Commonwealth Office (FCO)

At the FCO I covered in detail how the FCO ensured and oversaw that assurances contained in submissions are met. FCO explained how they tracked conditions against the Secretary of State's requirements including that any such conditions are set out in renewals. I advised that the FCO formalise their policy so they are in a position to demonstrate the tracking process to the new oversight body.

In relation to record keeping the FCO agreed to speak to SIS again about it. I **recommended** that the FCO monitor that GCHQ review internal approvals made under class authorisations appropriately.

I reviewed a sample of GCHQ's monthly update notes to the FCO containing details of the authorisations under a number of class authorisations and was satisfied that the FCO were discharging their duty overseeing this area of operation.

General Points for all Warrants and Authorisations

This section is concerned with general points which apply to all warrants and authorisations.

Information in the Warrant

When I ask to see a particular warrant I have to be provided with the accompanying submission to fully understand what is involved and restrictions accepted. Key features are set out in the submission including necessity, proportionality, privacy considerations and why the action proposed is justified by the intelligence to be received and any restrictions. I have **recommended** that a warrant or authorisation instrument which is signed by a Secretary of State should state that any activity taking place was subject to and in accordance with terms constrained in the submission. GCHQ have already adopted this course and I strongly encourage SIS and MI5 to do so as well.

RIPA PART II Authorisations – Date of Effect

The code of practice for Directed Surveillance states that the authorisation begins on the day "when the authorisation was granted" (para 5.10). RIPA says: "beginning with the day on which the grant of the authorisation or, as the case may be, its latest renewal takes effect ..." RIPA 43(3)(c).

The code of practice for Covert Human Intelligence Sources states that the authorisation begins on "the day on which it took effect ..." (para 5.14). RIPA 43(3)(b) states "beginning with the day on which the grant of the authorisation or, as the case may be, its latest renewal takes effect.."

The legislation allows an authorisation to be made on the day, to take effect at a later date. The codes appear not to. It must be more practical to be able to sign a RIPA Part II form on the day to take effect on a later date when the operation begins. Clearly the date of authorisation should be "shortly" before the date when the operation begins. In my view the codes of practice need to be changed but I have **recommended** that because of the language of the codes the only safe course is to calculate the time from the day of signing i.e. date of authorisation.

Cancelling Warrants

ISA s6(3) and RIPA s45 requires that warrants must be cancelled if they are no longer necessary. I noted that this does not happen as a matter of routine and sometimes departments had no effective system in place to check when warrants were no longer required. Instead the warrant is allowed to lapse. I **recommended** that warrantry units and the agencies establish a mechanism to check for warrants no longer in use and to cancel the warrant when the purpose for which it was obtained has been completed so that the information is available to the appropriate oversight body.

8. CONCLUSIONS AND RECOMMENDATIONS

My overall conclusion is that authorisations and warrants are only granted on the basis of a proper case being made for necessity and a proper consideration of proportionality all set out in detailed submissions. It is evident that the agencies, MOD and Ministers together with their officials all take compliance very seriously and put a great deal of effort into ensuring that each interference with privacy is fully justified. I have however made clear that in their submissions it is important where collateral intrusion into privacy is recognised, the mitigating steps should be clearly spelt out.

I have suggested that because submissions contain the important conditions on which warrants and authorisations are granted that there should be an express reference to those terms on the face of the warrant or authorisation. This suggestion has been taken up by GCHQ and I hope that others will follow suit.

So far as DSAs and CHIS authorisations are concerned there are differences in the language between the codes of practice and the legislation. The codes appear to provide that time runs from the date of signature. The legislation would appear to allow for signature and the period to run from a specified date thereafter. The latter allows for sensible planning. The former means that if signing takes place the date prior to the day of the expiry of a previous authorisation, there is a danger of a miscalculation. I have advised that the only safe course it to follow the codes of practice, but I suggest that the language of the codes of practice is brought into line with the statute.

Recommendations I have made previously relating to thematic warrants have largely been accepted and implemented, however I will continue to keep a close eye on the terms of these warrants to ensure they are only being used when absolutely necessary.

I have made several references in this report to inadequacies in the way SIS record their decisions. It is right to record that there have been improvements particularly in relation to the application of the Consolidated Guidance. I have also been shown drafts of forms which if implemented will further improve matters.

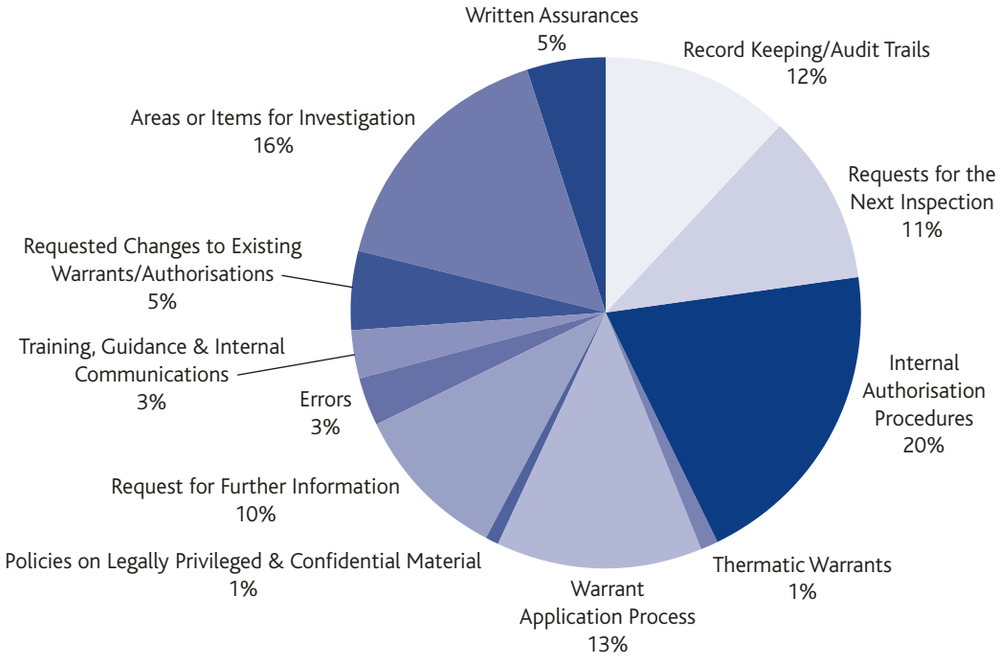
I have drawn attention to "errors". It is right to emphasise that I have not found any evidence of deliberate disregard of the requirements to obtain proper authorisation, and the "errors" found are not more than would be expected in any large organisations required to act at speed and under pressure.

In relation to the agencies use of bulk personal datasets I am satisfied that the agencies have very good systems in place to ensure that no datasets are acquired, exploited or retained where it is not necessary and proportionate to do so, as well as effective protective monitoring systems in place to prevent their misuse.

With regards to the application of the Consolidated Guidance, I am satisfied that the agencies and the MOD take all steps they can to make their personnel aware of the terms of the guidance. It is clear to me that extremely careful consideration is given to its application in increasingly complex situations. In some instances the Guidance may not expressly apply and I am reassured that in such situations the agencies and the MOD follow it and its spirit so far as they practically can. As I mentioned earlier the IP Bill does not currently make provision for the oversight of the Consolidated Guidance. There is a provision for the Prime Minister to issue directions as heretofore and I hope that such a direction will be issued to ensure continued oversight of this very complex area when the new Bill comes into effect.

Throughout the year I have made a total of 143 recommendations to the Security Service, SIS, GCHQ, MOD, Home Office, Foreign Office and the Northern Ireland Office. I have touched on the key recommendations in the relevant sections of my report; the chart below shows a summary of the categories under which all of the recommendations fall.

Recommendations by Category



APPENDIX

Expenditure

My office's total expenditure for the financial year 2015/16 was £408,399.24. The table below provides a breakdown of this expenditure. This expenditure includes costs of the report into 'Concerns Raised by the Intelligence and Security Committee of Parliament about the Government's Responsibilities in Relation to Counter-Terrorism Units Overseas' incurred in the financial year 2015/16.

Description	Total (£)
Staff costs	320,729.42
Travel & Subsistence	17,706.89
Legal fees	49,345.60
IT	17,568.41
Office Costs (including stationery and printing costs)	3,048.92
Total	**408,399.24**

ISBN 978-1-4741-3553-5