Report of the Intelligence Services Commissioner for 2016

The Rt Hon. Sir Mark Waller

Report of the Intelligence Services Commissioner for 2016

The Rt Hon. Sir Mark Waller

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

Ordered by the House of Commons to
be printed on 20 December 2017

Laid before the Scottish Parliament by
the Scottish Ministers on 20 December 2017

House of Commons Number HC/298
Scottish Government Number SG/2017/78

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

Any enquiries regarding this publication should be sent to us at info@ipco.gsi.gov.uk

ISBN 978-1-5286-0175-7

ID CCS1217635040 12/17

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS 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

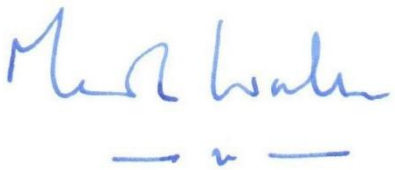
The Rt Hon. Theresa May MP
10 Downing Street
London
SW1A 2AA

I enclose my sixth Annual Report covering my work as Intelligence Services Commissioner between 1 January 2016 and 31 December 2016.

I hope you find it convenient that I have continued to write my report in two parts. The Confidential Annex contains details including techniques and operational matters which is exempt from publication for national security reasons.

It is for you to determine, after consultation with me, how much of this open report should be published without releasing any material which would be contrary to the public interest, or prejudicial to national security, to the prevention or detection of serious crime, to the economic wellbeing of the United Kingdom, or to the discharge of the functions of those public authorities subject to my review.

As this is my final Annual Report as Intelligence Services Commissioner, I would like to add that it has been an honour and a pleasure to hold this post and to offer my successor Sir John Goldring my very best wishes in taking forward this important work.



The Rt Hon. Sir Mark Waller

INTRODUCTION

This is my 6th and final annual report since taking up office as the Intelligence Services Commissioner on 1 January 2011. There have been a number of significant developments since my last report in 2015, not least the passing of the Investigatory Powers Act (2016) which will abolish the Intelligence Services Commissioner's Office and establishes the Investigatory Powers Commissioner to oversee areas of work by the Intelligence Services and Ministry of Defence which have previously fallen under my functions. Later in this introduction I will cover in more detail the key changes that this will make to the oversight function. I will also address important developments over the past year which have had an impact on the work of the Intelligence Services and Ministry of Defence from the perspective of oversight.

My Oversight

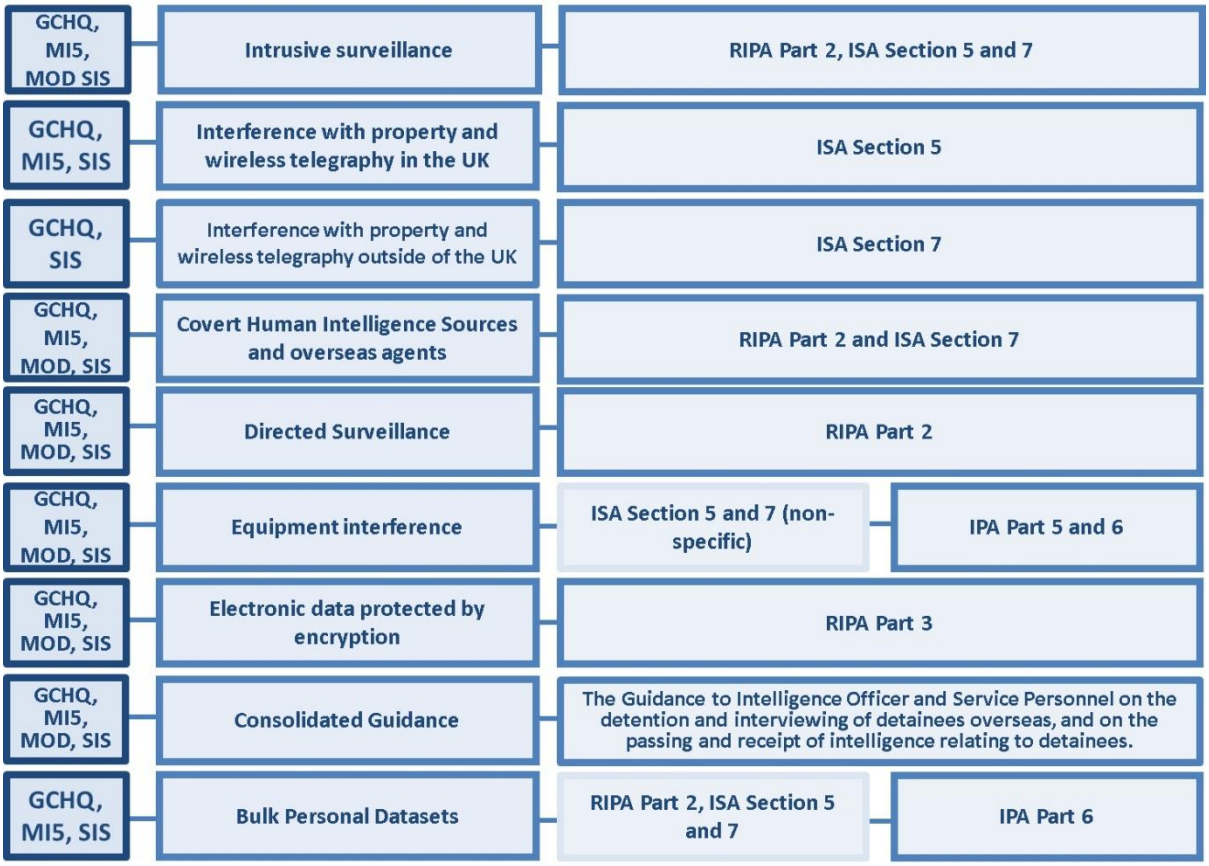
My statutory functions are set out in full on my website. As in previous years, my oversight is conducted by checking warrants and authorisations issued by Secretaries of State and the internal authorisations that to enable the Intelligence Agencies to carry out their functions. In essence I check that the proper consideration has been given to necessity, proportionality, and reasonableness. I also oversee the surveillance activities of the Ministry of Defence conducted under RIPA. In addition to the authorisation paperwork, I examine safeguards in place to prevent unlawful and inappropriate access and scrutinise the policies and procedures in place to deal with acquisition, use, retention and deletion of information.

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. This is a complex area involving difficult decisions relating to intelligence sharing.

The Supplementary Report to the Annual Report for 2015 raised issues relevant to the Consolidated Guidance. This included concerns raised by the Intelligence and Security Committee of Parliament about the government's responsibilities in relation to partner counter terrorism units overseas. While this report raised no suggestion that officials working on behalf of HMG had any role in supporting or enabling mistreatment, I did make certain recommendations regarding the process for

assessing individual cases and making appropriate referrals to ministers. Work is ongoing in this area in consultation with the current Intelligence Service Commissioner.

Below in chart form is a summary of what I oversee and the relevant sections under which authorisations are made.



Terrorism Prevention Investigation Measures (TPIMS) Act 2011

I mentioned in my 2015 report that I advised the Home Office on the propriety of extending the TPIMS regime beyond the initial expiry date of December 2016. As part of the consultation process under section 21(3) of the TPIMS Act I wrote to the Home Secretary in June 2016 to set out my recommendations. My recommendations were based in the main on the detailed review conducted by David Anderson QC as Independent Reviewer of Terrorism Legislation. I concluded that TPIMS were a useful tool for the protection of the public and suggested that the Home Secretary would be justified in extending the regime for a further five years.

Changes from previous annual reports

This report broadly follows the format of the 2015 report, which I structured so as to clarify the key powers of the Intelligence Agencies and Ministry of Defence falling under my oversight. This year, I have added a short section on 'Thematic authorisations'. The use of non-specific authorisations by the Intelligence Agencies has received significant public and parliamentary scrutiny over the past year. I felt it would be valuable to address the use of these broader authorisations directly in view of the changes made by the IPA, which explicitly empowers Secretaries of State to authorise thematic and bulk activities.

The Appendix to this report includes for reference a table of recommendations that I have made to the intelligence agencies throughout 2016. It is worth noting that many of these recommendations have been addressed and resolved. Some of these recommendations, however, relate to ongoing work that the Agencies, Warrantry Units and the MOD are involved in. I would expect that the Intelligence Services Commissioner and Investigatory Powers Commission will oversee the implementation of changes resulting from these recommendations throughout 2017.

Developments since my last annual report

The Investigatory Powers Bill received Royal Assent on 29 November 2016. The Investigatory Powers Act establishes a new legal framework for the more intrusive powers exercised by the Intelligence Agencies in addition to the Intelligence Services Act (1994) and Regulation of Investigatory Powers Act (2000).

A key feature of the Act is to spell out in more detail than ever before the powers needed by the agencies to enable them to deal with terrorism, cyber-warfare, state-sponsored threats and organised and serious crime. The Act acknowledges the pace of technological change, which will present new threats and challenges for the agencies in the future.

The act introduces a judicial pre-approval process in addition to authorisation by a Secretary of State for those powers parliament consider to be most intrusive. This is known as the 'double lock'. Of my areas of oversight only Equipment Interference (EI) and Bulk Personal Data are covered by the 'double lock'. The Act sets out enhanced safeguards and proscribes handling arrangements to prevent the misuse of data, in particular regarding the use of bulk collection powers. This and other covert powers will be overseen by the Investigatory Powers Commission.

I have been encouraged and pleased to note that the Intelligence Agencies have been proactive in their preparations for the implementation of the IPA. A significant programme of work has been initiated to prepare for the new legislation, including extensive systems upgrade and staff training. This work has been sensitive to discussions in Parliament and concerns raised by critics and I believe it will be successful in establishing the necessary safeguards.

Pursuant to the Act 2017 will see the creation of the Investigatory Powers Commissioner's Office, headed by the Investigatory Powers Commissioner, The Right Honourable Lord Justice Adrian Fulford. Lord Justice Fulford will be supported by a number of Judicial Commissioners. Under the Investigatory Powers Commissioner, a newly established team of inspectors will provide oversight of the intelligence services, fulfilling the functions of the Intelligence Services Commissioner's Office. This office will continue to provide rigorous oversight of the agencies' work and will increase rigour and expertise working with the new Technical Advisory Panel and other oversight bodies.

Investigatory Powers Tribunal

During 2016 the Investigatory Powers Tribunal published two judgments which scrutinised areas of oversight by the Intelligence Services Commissioner. The first relates to CNE Operations (now known as Equipment Interference) and the second relates to Bulk Data. The full judgements can be found at the IPT website. The Tribunal commented favourably upon the oversight carried out and guidance given.

Bulk Powers Review

Another noteworthy publication was the Bulk Powers Review published in August 2016 by the Independent Reviewer of Terrorist Legislation. The report evaluates the case for four investigative powers; bulk interception, bulk acquisition, bulk equipment interference and bulk personal datasets.

The report concluded that there was a proven operational case for three of the powers and that there was a distinct but not yet proven operational case for bulk equipment interference. Parliament subsequently made provision for all four powers in the Investigatory Powers Act.

The report recommended that a Technical Advisory Panel of independent academics and industry experts be appointed by the newly formed Investigatory Powers Commission to advise on the impact of changing technology and how the Intelligence agencies could reduce the impact on privacy of their activities. I fully support this recommendation.

EXECUTIVE SUMMARY

Although it is not my role to comment on the operational performance of the intelligence community, in summarising this report and reflecting on my time as Intelligence Services Commissioner I would like to record that the United Kingdom is extremely fortunate with its intelligence agencies. They combine an extremely high level of operational competence with a collaborative approach and a respect for the law which makes them trusted and respected internationally.

The UK Intelligence Community's attitude to ethics in general, and legal compliance specifically, is impressive and reassuring. While there is some legal debate about certain powers, I have never seen any evidence that the agencies institutionally would knowingly break the law. The application of the range of relevant legislation in this area is complex, and courts do not always agree with the position taken by the Government (or indeed by Intelligence Services Commissioners in the interpretations of the law we apply to our oversight). This does not mean they have not shown respect for the law.

In terms of my inspections, I have found that the substantial compliance teams in each organisation and the relevant departments of state think deeply about the application of executive power and the intrusion into the privacy of its citizens. Everyone I inspect approaches the process in an open manner. Indeed, rather than hiding problems, they are often proactive in raising the most difficult issues with me.

I realise that the detail of this report, which mostly sets out the rare examples of non-compliance, might bring the reader to a different conclusion. But while I would be concerned if my report gave a false impression of the performance of the UK intelligence community, I consider it important that the public understands what sort of errors and problems I have uncovered during my oversight, and can be reassured that such improvements as are necessary are being identified and dealt with.

There are some recurring themes which come up throughout the report, that are worth highlighting. SIS's poor record-keeping makes it harder to check their compliance, and exposes them to legal risk. This was a significant criticism in my supplementary report to the Annual Report for 2015 on the allegations of mistreatment set out in the Intelligence and Security Committee's report on the

intelligence relating to the murder of Fusilier Lee Rigby. I have been working closely with their compliance team on improvements. The introduction of a 'Record of Key Decision' process is a significant step, but needs to be more widely understood, and to focus on compliance – as well as operational – considerations. Importantly, even where considerations are not recorded, the interviews I conduct with SIS officers show that necessity and proportionality considerations are usually inherent in operational decision-making. I have reminded SIS and GCHQ that internal controls are vital to ensure that various assurances to the authorising Secretary of State around compliance are being followed.

The agencies' bulk powers, some class authorisations and some thematic warrants are some of the most difficult from an oversight perspective. They can involve collecting and dealing with information which is personal and of no intelligence interest. Indeed many of us are likely to be included in this collection. As a result, for the use of these data sets to be proportionate, the control and auditing of these data sets and the access to them is extremely important.

This may be the last annual report by an Intelligence Services Commissioner. As a result of the Investigatory Powers Act, the Intelligence Services Commissioner's responsibilities are likely to fold into the Investigatory Powers Commissioner during the course of 2017. While the IPA does not substantially increase the intelligence agencies' powers, merely clarifying the use of existing powers, it will make a significant difference to the oversight of the Intelligence Agencies. A number of investigatory powers will require judicial pre-authorisation. Of the powers I inspect, these are equipment interference and bulk personal data. In addition, inspections will be more rigorous, with more dedicated inspectors. In the new organisation my successors will have access to expertise from a technical advisory panel, a dedicated legal advisor, additional judicial commissioners, and from surveillance and interception inspectors. Finally, I wish my successor, Sir John Goldring, and ultimately all those involved in the new Investigatory Powers Commissioner's Office well for the future.

RISKS

The most common risk is that of human or systems errors which could result in the unintentional breach of human rights. It is important that the staff and management of the Intelligence agencies, MOD and warrant granting departments are well aware of the legal framework in which they operate, and that there is a strong culture of compliance. I am confident that this culture exists, however, some errors do occur and I work closely with the agencies to examine the cause and impact of such errors and to ensure that actions are taken to ensure the number of errors is reduced to a minimum. I discuss this in greater detail in the later chapter on Errors.

The most dangerous risk relates to the possibility that an individual or group of individuals would seek to abuse the system. The rigour and transparency of the authorisation processes mean they would need to circumvent the system for their own ends. It is of course vital that each agency has strong procedures in place to ensure that any attempts to deliberately misuse data do not succeed and are quickly detected.

During my inspection visits I seek assurances around the systems that agencies have in place to protect sensitive data and guard against misuse. I maintain a close interest in the culture and ethos of each organisation by meeting staff during my regular inspection visits and by attending training courses.

The systems that the agencies have in place are necessarily sensitive, but I can confirm that I am satisfied that each agency has robust physical, cyber and personnel security measures in place to mitigate against deliberate misuse by an individual.

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 (through monitoring and audit) and without having to go to a more senior officer.

A positive security culture is central to the safeguards in place at each agency. To minimise the risk of rogue personnel, all staff working for the Intelligence agencies are subject to rigorous security vetting on recruitment and this is reviewed on a regular basis. Furthermore staff and managers are encouraged to report suspicious behaviour to their security departments. This selection and regular review of staff security is coupled with a strong focus on ethics with each agency offering ethics

training and access to an ethics councillor who staff can turn to if they have any concerns about their work.

There has been considerable coverage in the media about large scale intelligence leaks in recent years. From what I have seen the UK intelligence agencies have gone to great lengths to ensure that their data is secure and the public should have every confidence that this is the case.

THEMATICS

Thematic warrantry is a complex area that I have scrutinised closely over the past year. I am mindful that the question of "bulk power" has been discussed widely in the context of the Investigatory Powers Act and so felt that is was important to set out my views on how these broader warrants are used by the agencies.

Thematic warrantry is a general term used to cover authorisations where a single defined target is not used. These might range from a section 5 warrant acting against more than three people, to a section 7 authorisation (such as a class authorisation) acting against a great number. So far as possible broadly defined warrants should not be used unless a strong case for necessity is made out.

The greatest challenge with thematic warrantry is for both the agency and the Secretary of State to be satisfied with the level of oversight provided for operations conducted under the authorisation and the rigour of safeguards applied during the operation. At the point of signing, the Secretary of State must satisfy themselves, as with any application for warrantry, of the necessity, proportionality and reasonableness of the operation, of the likely intrusion into privacy and any collateral intrusion, and finally of the likelihood of obtaining any legally privileged or confidential material.

Once the authorisation is in place, both the Secretary of State and the acting agency must take care to ensure that operations conducted are not only within the letter but also within the spirit of what has been authorised. This might mean, for example, that minor changes are made to specific method of delivery or process of an operation but the intelligence obtained remains that set out in the authorisation. Alternatively, where a warrant acts against a terrorist cell, an operation might be planned against an individual who had not been identified at the time of application, but who is clearly part of the group described under warrant. In both of these examples, the language and conditions in the submission should be sufficient to enable these operations to take place under the thematic warrant.

During the authorisation process, the Secretary of State and applying agency will determine the appropriate level of oversight for the lifecycle of the authorisation. For singular, non-thematic authorisations, the Secretary of State will receive updates in relation to the operation through the six monthly renewal process. The renewal submission would set out any relevant information that has come up since the signing, and set out the justification for continuing the operation. In the case of some thematic warrants this process is sufficient to provide adequate oversight for the Secretary

of State. In other cases, it is for the Secretary of State to agree a more rigorous updating process. Mechanisms will typically include an interim submission provided at an agreed frequency, such as a monthly update, or an update whenever an operation has been conducted. These documents are made available to me during my inspections and I am confident that this mechanism is effective.

INVESTIGATORY POWERS

This section addresses findings from my 2016 inspections of the Intelligence Services, the Warrant Granting Departments of the Departments of State and the Ministry of Defence. These findings have been structured by investigatory power, to demonstrate how each organisation is working in relation to each of the available intrusive powers. Further details of these powers are available on my website.

i. Intrusive Surveillance and Property Warrants (covering section 5)

Intrusive Surveillance

Intrusive surveillance is covert surveillance conducted against any residential premises or a private vehicle either by a person or using a monitoring device, such as a CCTV camera. The justification for conducting intrusive surveillance must be strong because of the highly intrusive nature of this technique, which can take place inside someone's home where they would have a high expectation of privacy.

Property warrants

Section 5 of the ISA refers to property interference within the UK. Under section 5 of ISA the Secretary of State may issue warrants authorising MI5, SIS or GCHQ to access, enter into, and interfere with property. Property warrants can also authorise interfere with wireless telegraphy.

Combined warrants

Under section 42(2) of RIPA a Secretary of State may issue a single warrant combining an intrusive surveillance warrant with a property warrant. This might cover, for example, entering a house to install an eavesdropping device. Consideration of the necessity and proportionality of each action authorised must be demonstrated separately, including any interference with privacy and property.

Thematic warrants

I have commented in my previous reports about the agencies' use of thematic section 5 warrants. Following my recommendations, the agencies have continued to work to limit their reliance on these broadly defined warrants in favour of specific applications. I am satisfied that the agencies and

warrant granting departments have worked to bring the remaining thematic casework to my attention.

My overall assessment

During my 2016 inspections I have scrutinised the suite of paperwork used by the agencies in relation to section 5 authorisations. I am satisfied that applications made to the Secretary of State demonstrate due consideration of necessity, proportionality and intrusion into privacy. However, I have noted an inconsistent standard of consideration on internal documents under some of the broader authorisations.

Collateral intrusion

In my 2015 Annual Report I recommended that the agencies should do more to set out in warrant submissions how unwanted product would be handled. This is relevant to Intrusive Surveillance and section 5 warrants under which a certain degree of collateral intrusion is almost inevitable, for example where the target property is a family home. I am satisfied that the agencies are sensitive to this intrusion. However, I have suggested that it should be explicit at the point of application what they will do with any information they obtain that is not judged by them to be of intelligence value, including any programme for deleting that information. This is an area that I gave considerable scrutiny in my 2016 inspections. I **recommend** that the agencies should set this out clearly in applications, including internal paperwork, where appropriate. I would also expect to see the mitigations for collateral intrusion to be set out clearly in the handling arrangements provided to the Secretary of State.

Devices pending extraction

Once any lawful property interference is complete, the relevant agency must seek to remove any devices and where possible cease any property interference in the least intrusive and damaging way available. The section 5 warrant covering the property intrusion will cover this activity. However, because the warrant cannot be amended, renewal of the warrant will continue to authorise the full planned operation, although it will no longer be necessary and proportionate to conduct the full range of actions. For example, a warrant may authorise an agency to install and remove a monitoring device. While the warrant is renewed to enable the agency to remove the device, it would no longer be necessary to install any new devices. During my inspection of MI5 I was pleased to note that the language had been clarified in these instances to explain that no ongoing intelligence collection was taking place.

In my 2015 Annual Report I explained that I had therefore agreed that the agency may transfer the device onto a 'thematic' warrant which only authorises extraction operations, while awaiting extraction.

My inspection of SIS's section 5 authorisations identified that SIS will not explicitly state in a renewal submission that the device is pending extraction. Although it was clear that this was not a substantial area of work for SIS, I **recommended** that SIS should consider using similar language to MI5. In some cases, such devices may be monitored to some extent to support the extraction, or to confirm that the device remains securely in place. I **recommended** that any renewal submissions should set out precisely how any such device or implant is being monitored and should make explicit that the warrant is no longer used to gather intelligence.

Computers as property

During my inspections I have noted several occasions where computer equipment has not been set out adequately as the property specified under a section 5 application. This does not affect the legality of the warrant, where the Secretary of State has clearly understood that equipment interference will take place. However, I have **recommended** that equipment interference should be set out clearly and specific intrusion considerations should be apparent from the submission. I have advised that the warrant granting departments should keep this under close review as we move to the IPA.

A section 5 application will set out the property and actions to be done to that property explained as below. Please note these wordings are an example for clarification only:

Property

1. Computer equipment belonging to [target's name]

Actions

i. Such interference with the property described at 1) as is necessary to access data held upon the property.

ii. […]

In some cases, warrant submissions have authorised officers to interfere with any computers located during the search of a named property as below:

Property

1. [House Number], [Street Name etc.]

Actions

i. Such interference with the property described at 1) as is necessary to gain access to the premises.

ii. Such interference with the property described at 1) as is necessary to access any computer equipment identified within that property.

iii. […]

I have previously **recommended** that any computer equipment to be interfered with should be explicitly set out in the property specifications on the warrant instrument as shown below. This makes explicit that any interference with the non-target's computer is not allowed. I have reminded the Home Office to ensure that this is the case on all warrants authorised.

Property

1. [House Number], [Street Name etc.]
2. Computer equipment belonging to [target's name]

Actions

i. Such interference with the property described at 1) as is necessary to gain access to the premises.

ii. Such interferences with the property described at 2) as is necessary to access any data held upon the property.

iii. […]

Paperwork

During my inspections of GCHQ I scrutinised several section 5 applications, and reviewed the internal paperwork used to record specific operations conducted under broad warrants (see also Thematics). I was pleased that GCHQ presented a new wording to me, which set out necessity and proportionality considerations clearly. I expect that this will improve the clarity of GCHQ's record of activity in the future.

The FCO explained that GCHQ have on occasion allowed a section 5 authorisation to lapse, rather than submitting a cancellation submission. I **reminded** the FCO and GCHQ of the importance of cancelling any authorisation that is no longer necessary and proportionate.

In one case I examined at GCHQ, a paragraph detailing specific planned activities was set out in a renewal submission but not the warrant application for a section 5 authorisation. I am content that

this did not affect the legality of the authorisation because the activities fell within the scope of the original warrant. However, I did **recommend** that the detail should have been included in the original submission and asked GCHQ to review all current warrants to ensure that no other case exists of missing paragraphs amended at renewal. I was satisfied at a later inspection that no similar issues had been identified.

I remain concerned about SIS's formal recording of decisions. As I said last year, a system of 'key decision documents' was introduced in an attempt to meet my recommendations. Further forms were also introduced to capture the decision making process. Still in some areas an e-mail stream remains the record. I have **recommended** that more should be done, both as good business practice and to help with oversight, to record formally in one document the relevant considerations. I have requested that a greater number of such Decision Documents should be presented to the Commissioner for oversight in the future. I have also **requested** sight of the internal training and guidance regarding the use of Decision Documents. I expect that my successor, and subsequently the Investigatory Powers Commissioner, will focus on working with SIS to improve this area in the future.

With regard to thematic warrants, there is an apparent discrepancy between the provisions under RIPA and those under the ISA which result in a different means of specifying the subject of the warrant. RIPA sets out that "persons" may be the subject of the warrant while the ISA requires "property so specified". I have **suggested** that the Home Office should present submissions to the Home Secretary in such a way as to make this difference clear. I have **recommended** that the Home Office should present all thematic warrants for oversight in the future.

Letters of clarification

During my inspection of MI5 I scrutinised a case where a letter of clarification had been sent to the Secretary of State but no reference was made to this in the renewal document. A letter of clarification is a formal document sent to the Secretary of State by MI5 where a point of clarification should be made in relation to an individual submission. It does not seek to alter the authorisation or materially affect the considerations set out in the original submission, but it for example draws attention to a change in the handling arrangements or collateral intrusion consideration which MI5 judges it necessary to update the Secretary of State on. I have **suggested** that in the future MI5 should take care to ensure that the gist of the letter of clarification is reflected in any subsequent renewal paperwork.

In another case I noted that the language used in a letter of clarification implied that it was being used to amend a warrant (which would not be possible as these warrants cannot be modified) and which would leave the warrant open to legal challenge. I **recommended** that this be clarified at renewal. I was subsequently shown redrafted wording and was content that this remedied the issue.

In certain circumstances where a thematic warrant is in place, MI5 may agree with the Secretary of State to provide a letter of clarification to highlight where individual deployments have taken place (see also Thematics). This agreement may be set out in the submission or as a policy agreement, but is notably not a specific term of the warrant instrument. As an example, an authorisation might allow MI5 to conduct specific technical operations against individuals associated with a specific plot, but they may undertake to inform the Secretary of State of any specific deployments via a letter of clarification within a week. I noted one case where MI5 had failed to provide the Secretary of State with a letter of clarification noting a deployment within the timescale that they had set out for themselves in the submission. I understand that there may be some cases, for example under extreme operational pressure or where a Secretary of State is not available, where MI5 may reasonably not meet the proposed timescale. I have taken the view that a failure to meet such an agreed timescale does not affect the lawfulness of the activity authorised but I have **recommended** that MI5 should continue to ensure that any such letters of clarification are provided to the Secretary of State as soon as realistically possible, and that any failure should be reported to the Commissioner as an error.

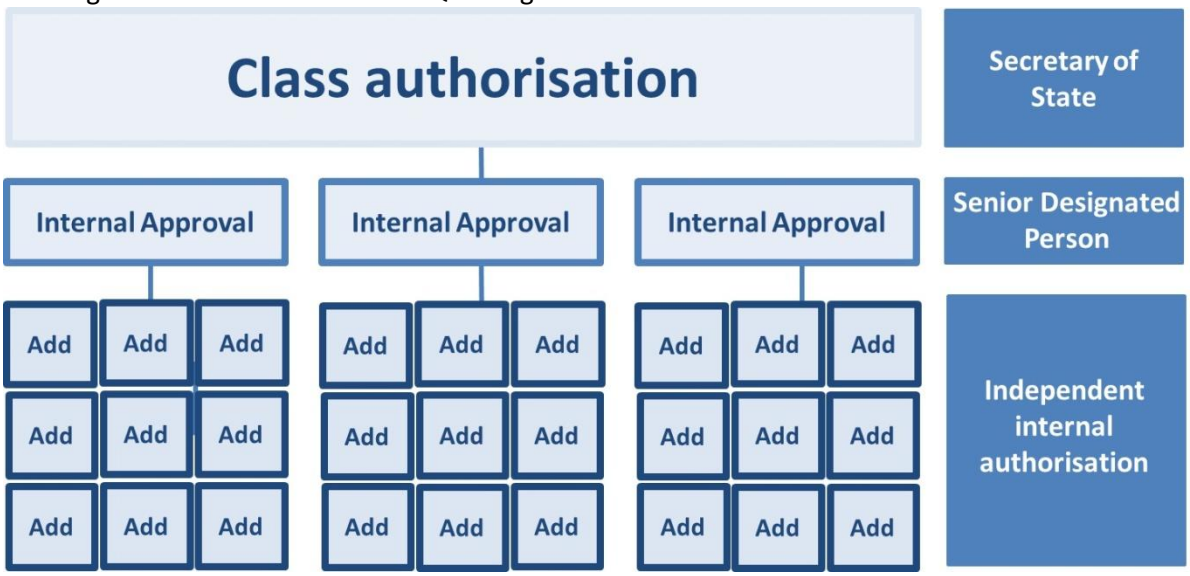
ii. Section 7 Authorisations

Section 7 of ISA refers to activity outside of the UK, actions under section 7 are therefore normally authorised by the Foreign Secretary. Under section 7 the Secretary of State may authorise SIS or GCHQ to undertake a specific act or a range of activities. The requirements and priorities for GCHQ and SIS are set centrally by government. When applying for authorisation, each agency will demonstrate to the Secretary of State how planned activities will meet government's priorities in line with their statutory functions. In addition to ensuring agencies only act with the authorisation from the Secretary of State, the authorisation under section 7 removes personal liability under UK law where the officer has been acting in good faith within the parameters of the authorisation. The activities available under section 7 are broad in scope, the actions authorised may be highly intrusive or include no intrusion into privacy. Where the activity is intrusive, the requesting agency will make this clear to the Secretary of State at application and will rely on a process of senior-level scrutiny within the organisation to demonstrate necessity and proportionality considerations.

Class authorisations

Class authorisations are broad section 7 authorisations under which GCHQ and SIS conduct the bulk of their routine work overseas. In addition to establishing protection for liability under UK law, class authorisations enable political approval for the activities they cover. Within a class authorisation, senior-level scrutiny is provided for individual activities, and where necessary a submission will be provided to the Secretary of State to ensure specific oversight of highly intrusive acts, for example.

The diagram below shows how GCHQ manages class authorisations under section 7:



My overall assessment

Given the broad scope of section 7 authorisations, I have focused close attention on SIS and GCHQ's documentation and am generally satisfied that both organisations are clear in their obligations regarding necessity, proportionality and reasonableness and that these principles are applied before any activity is conducted. But I remain concerned that more formal documentation recording decisions is not produced by SIS. As regards GCHQ, I requested and was provided with many of what are termed 'additions' i.e. particular internal authorisations. These show that when relying on general authorisations to conduct particular activities consideration is given as to its necessity and proportionality in relation to this particular task.

GCHQ thus maintains a clear and structured process of authorising and recording activity under section 7 class authorisations. Internal Approvals and Additions set narrowed parameters for activity and are authorised by a senior designated person or independent authorising officer respectively. Within the structure of the approvals and additions process, GCHQ officers will set out the necessity and proportionality of individual operations in relation to particular activities. I have been pleased to see that at GCHQ privacy considerations are carefully considered at this stage.

SIS however have a less structured and rigorous approach when authorising actions under the section 7 class authorisations. I have **recommended** that SIS improve the standard of internal approval documentation.

Liaison partnerships

In the course of their work, each of the agencies works closely with foreign liaison partners. This involves routine intelligence sharing and at times collaborative operations. I am satisfied that the agencies are sensitive to the implications of working with partners acting under different legal systems and note that UKIC working overseas are careful to apply the principles of UK law as far as possible.

Agent authorisations

The majority of SIS's agent-related activity is conducted outside of the UK and is therefore conducted under section 7 class authorisations. I have previously **recommended** that the principles of the CHIS Code of Practice, which applies to UK-based agent conduct authorised under RIPA part 2, should be applied by SIS to their overseas agent casework. I acknowledge that it is not accepted that RIPA applies to agent running outside the UK but that SIS seek to apply certain principles of the CHIS

code of practice, for example relating to safeguarding minors and LPP material. I have suggested that more formal record keeping will improve the clarity with which SIS applies these principles and will document decision making and how they apply their own human rights and legal considerations under section 7 authorisations. (See also CHIS).

I have been impressed by the consideration given by SIS officers working overseas and their diligent application of necessity and proportionality principles, particular while working in cooperation or collaboration with a liaison partner. It can be difficult for SIS officers working alongside liaison units who adopt a different, and at times conflicting, legal framework. I **recommended** that when working with liaison partners to task CHIS, SIS officers should keep a written record of what the CHIS is, and is not, tasked to do. Where possible, the record should be shared and agreed with the liaison unit.

Templates and paperwork

I have impressed upon both GCHQ and SIS the importance of cancelling any authorisations, including section 7 authorisations, as soon as they are no longer necessary. There are differing legal opinions on this issue; some hold that it is not necessary to complete full cancellation paperwork if all activity under the authorisation has ceased. However, I continue to **recommend** that it is best practice to cancel section 7 authorisations in line with ISA section 7(8). (See also section 5).

iii. Equipment Interference

Equipment Interference (EI) is any interference, remotely or otherwise, with computers, servers, routers, laptops, mobile phones and other devices in order to obtain information from the equipment. Information obtained may include communications content and communications data[1], and information about the equipment to allow an intelligence service to examine or modify the equipment, or to conduct surveillance. This area of activity is currently authorised under the authority of ISA section 5 warrants or section 7 authorisations but will fall under the IPA Part 5 in the future. The authorisation can be used in tandem, but not combination, with a RIPA Part 1 authorisation, which would cover any interception of communications, whether deliberate or incidental, during Equipment Interference activity.

In my 2015 report I outlined the oversight process for EI, including how I work with the agencies to provide oversight and I explained that particular consideration is given where an operation is likely to obtain confidential personal information, confidential journalistic material, communications subject to legal privilege or communications between an MP and another person on constituency business. I highlighted that the current interference does not provide for bulk EI authorisations other than under section 7. Part 6 Chapter 3 of the IP Act sets out new powers to obtain bulk EI warrants. It is vital that any authorisations made in this area set out full consideration of necessity and proportionality principles, and maintain appropriate handling of confidential data.

My overall assessment

The EI code under RIPA was finalised in January 2016. That code made public the powers and safeguards that existed previously. I believe that changes brought in under the Investigatory Powers Act will provide greater clarity. I have been pleased to see that the agencies are proactively engaging with recommendations I have made in the past and taking steps to improve compliance with the Code of Practice. In general, I am satisfied that necessity and proportionality considerations are carefully considered, and that the case for intrusion into privacy is made clear to the authorising officer in relation to EI authorisations.

[1] An EI warrant cannot be used to authorise real time interception of communications because RIPA s1(1) makes it an offence to intercept communications without lawful authority "in the course of its transmission."

[2] Section 2(2)(a) of the Security Service Act 1989, section 2(2)(a) and 4(2)(a) of the Intelligence Services Act

Confidential information

Part 3.27 of the Equipment Interference code requires the Intelligence Services Commissioner to be notified of any cases where confidential or legally privileged material is retained by an intelligence agency. During my inspections, the agencies each explained to me their internal processes for identifying and handling confidential material. I am satisfied that this material is being handled appropriately and in accordance with the Code of Practice and noted that GCHQ and MI5 demonstrated a cautious approach using a low threshold for identifying confidential material.

The scope of GCHQ's work means that it is likely that a certain amount of confidential material will be obtained, even where this material is not deliberately targeted. However, virtually none of this would be accessed by any officer other than to assess and safeguard the material. GCHQ provided sight of any such reports to me during my inspection and I was satisfied with how they are being handled.

During my inspection of MI5 I was given sight of a number of cases where an analyst had flagged potentially confidential or privileged material for further scrutiny. I am satisfied that MI5 are also handling this material appropriately.

SIS confirmed that they did not have any confidential or privileged EI material to report to me.

Misdirected implants

During my inspection of MI5 I was concerned to discover that one submission authorised MI5 to continue interference even if the implant got onto the wrong computer. They would then assess if the product is of intelligence interest. In my view product should be deleted without assessment as a default position. I **recommended** that MI5 should consider how authorisations might be framed under the new EI provisions for computers that are incorrectly implanted but where MI5 judge it necessary to review the new intelligence.

Handling arrangements

The Equipment Interference Code of Practice, paragraph 6.3 and 6.4 state that the Secretary of State must approve the handling arrangements for each agency. I have **recommended** that the Home Office should ensure that the Home Secretary has seen and approved all of the relevant documents. I have **recommended** that that Home Office and FCO should work with the agencies to make sure

that the handling arrangements are appropriately referenced in submissions relating to equipment interference.

Internal authorisations

During my inspection of GCHQ I scrutinised the Internal Approval documents used under section 7 class authorisations. Class authorisations are renewed on a six-monthly basis by the Secretary of State, while Internal Approvals will be renewed on a 6, 12 or 18 month basis. I was pleased to note that this process provides a consistent documentation of necessity and proportionality considerations, as well as a review of intrusion. I **recommended** that GCHQ should amend the wording of their forms for the Designated Senior Official, who authorises the renewal, to clarify that this process is in line with the EI Code of Practice.

With regard to Internal Approvals, EI Code of Practice paragraphs 7.12 and 7.13 set out that "particular operations" should be authorised by one Senior Designated Officer. This ensures that the necessity and proportionality considerations for a single operation are considered by the same senior authorising officer where possible so that maintenance of the highest standard for all is established. I **recommended** that GCHQ should conduct a review to identify any instances where this has not been the case and in the future should aim to provide oversight of individual operations to a specific Senior Designated Officer.

iv. Covert Human Intelligence Source (CHIS) and overseas agents

CHIS or agents are persons acting on behalf of an intelligence agency or the MOD, including members of the public or officers working under alias. Part II of RIPA and the associated code of practice provide the legal framework for authorising the use and conduct of a CHIS. Under RIPA, a CHIS can be authorised to obtain information from people who have no knowledge that the information will be passed to the intelligence agencies or armed services. Outside of the UK, agent activities which might otherwise be authorised by a CHIS authorisation will be conducted under a section 7 authorisation.

This is a highly sensitive area of work because of the risks undertaken by the CHIS, including personal risk to themselves and their family. Any application to authorise a CHIS must demonstrate strong consideration of the necessity and proportionality of tasking a CHIS and of risk to that individual. Continued consideration of these principles should be demonstrated through a process of internal scrutiny.

Real-world CHIS

In my 2013 Annual Report I stated that GCHQ may be authorised under Part II of RIPA to conduct activities by use of a CHIS but that those activities would be lawful if conducted by electronic means, given GCHQ's statutory powers. In consultation with GCHQ I have considered whether RIPA provides for GCHQ to conduct real-life CHIS operations where the objective is to obtain and provide information that is derived from or relates to the types of emissions and equipment described in the Intelligence Services Act section 3(1)(a). Contrary to my previous statement, I am now content that GCHQ can obtain legal authorisation to conduct real-world CHIS activity in accordance with the organisation's statutory functions.

My overall assessment

My review of CHIS paperwork provided by the Agencies shows some progress against the recommendations I have made in recent annual reports, in particular around internal record keeping. It is clear that the agencies conduct CHIS activities with due consideration to necessity and proportionality. The records provided to me relating to the process of authorising a CHIS have made this clear, although I would expect that this documentation sets these considerations out with greater clarity and individual consideration in the future. I expect that my successor and the

Investigatory Powers Commissioner will be provided a record of full and regular reviews in the future.

In my 2015 Annual Report I explained that the review process is a key element of agent running, and is required by CHIS code of practice (s5.17 and 5.18). I reminded the agencies of the importance of conducting regular reviews and making a written record of this. I would expect that my successor and subsequently the Investigatory Powers Commissioner will see a marked improvement in this area over the next year.

Obtaining CHIS authorisations

During my inspection of SIS I noted some instances where SIS maintained a relationship with an individual who had not been made the subject of a CHIS authorisation. I asked SIS to explain to me the timeline that they use while establishing a CHIS and to explain what criteria they use to determine whether a CHIS authorisation is necessary. SIS explained that their officers are trained to apply caution and to apply for an authorisation at the earliest opportunity where they judge that a proper source relationship has been established. My inspection of GCHQ identified a similar culture of erring on the side of caution and obtaining CHIS authorisations before a CHIS relationship is fully established.

In my view this approach is consistent with the CHIS code of practice chapter 2, which sets out that an individual is defined as a CHIS only if "*a relationship is established and maintained for a covert purpose*" and "*one of the parties of the relationship is unaware of the use or disclosure*" of information resulting from that relationship. It is important that proper authorisations are in place. SIS provided me with their "record of contact" paperwork, which records contact between SIS officers and individuals who may fall below the threshold for a CHIS authorisation and in my view evidences their cautionary approach.

Online CHIS

I have previously noted that GCHQ's work using online CHIS is conducted to a very high standard. During my inspection of MI5 I was pleased to hear that they have sought advice from GCHQ on the best practice of conducting agent activity online. I am satisfied that both MI5 and GCHQ have engaged proactively with legal advisors to ensure that any online CHIS activity is compliant with legal standards.

Confidential material

I take great interest in any activity which may have a bearing on legal privilege or may produce confidential material. During my inspection at MI5 I discussed the question of whether an individual working with the agencies could waive the right to privilege or confidential treatment. I was satisfied with MI5's view that this could not happen, and that all material should be treated as confidential even where an individual has knowingly provided intelligence to an agency. For example, journalistically confidential material provided knowingly by a CHIS should be treated as sensitively as intelligence obtained covertly without the knowledge of that individual. During my review, I was confident that this standard was maintained by MI5 across all intelligence collection.

Paperwork

I identified that in one case, an SIS officer had written "N/A" in a box asking for a comment on legal and compliance issues on an internal document relating to agent conduct. I **recommended** that reference should always be made to the relevant section 7 authorisation, and any compliance considerations should be documented.

I noted that SIS had completed renewal paperwork for certain CHIS cases months before the authorisation was due for renewal consideration. SIS explained that officers are automatically reminded to complete renewal paperwork ahead of the original expiry data in order to ensure that all renewals were made in a timely fashion. I commented that this would make it difficult for an officer to give adequate consideration to the necessity and proportionality case for renewing the authorisation. I **recommended** that as far as possible SIS should seek to renew any CHIS paperwork shortly before it is due to expire.

I reviewed several sets of casework where expiry dates for authorisations had been incorrectly calculated. In one such case, an authorisation was recorded with the expiry date of 26/10/16 but where a manual note showed that the date should have read 2/11/17. This second date was the correct date; the date on which the warrant would have expired if it had not been renewed. I agreed that this second date was correct, but was concerned by the practice of manually amending the formal authorisation. SIS explained the intention to issue an office-wide refresher notice, reminding staff of RIPA requirements.

I noted certain cases where MI5's casework workflow system set the expiry date at 00:00 after one calendar year; for example authorised on 01/01/15 and expires 01/01/16 at 00:00. The authorisation

would in fact expire at 31/12/15 at 23:59. This has resulted in some renewal paperwork being erroneously completed on the day after the authorisation has expired. MI5 believe this error may have resulted from a technical glitch in their workflow system, but are confident that no unlawful activity took place during the lapse. I have **recommended** that MI5 should investigate this as a wider issue with their workflow system.

Casework reviews

While reviewing SIS's and MI5's CHIS paperwork, I noted a number of instances where expiry, review and renewal dates were inaccurate or inconsistent.

One case set out by SIS highlighted that an officer authorising a CHIS suggested that a six-monthly review process should be instigated but put an incorrect review date on the form. I understand that instances of this nature will stem occasionally from human error, but **recommend** that SIS should impress upon their staff the vital role of CHIS reviews to ensuring the continued necessity and proportionality of any actions authorised. I also made this point clear when reviewing casework at GCHQ.

I reviewed GCHQ's internal authorisations, including CHIS authorisations and joint operational proposal and risk assessment (JOPRA) paperwork. I noted that GCHQ's combined forms did not include a review box. I **recommended** that any CHIS-related paperwork should explicitly set out the obligation to conduct regular reviews.

In my 2015 Annual Report I said that MI5 were unable to explain the automatic generation of random review dates that appeared on paperwork. MI5 investigated the issue; they believe that it was a technical fault but have been unable to pin down the cause of the problem. There have been no further instances and so I am satisfied that this is not an ongoing problem.

I also explained last year that I was concerned that MI5 were not consistently documenting CHIS reviews. Since then, MI5 have shown me their decision log for CHIS authorisations, which includes details of any decisions taken at review. I am satisfied that this records casework considerations, but continue to urge MI5, and the other agencies, to create a thorough record of CHIS review discussions and considerations.

v. Directed Surveillance

Directed Surveillance is covert surveillance which obtains private information other than within a residential property or private vehicle. Directed surveillance is typically authorised within the requesting organisation, because of the lower level of intrusion, but the same standards of necessity and proportionality must be applied.

My overall assessment

Directed surveillance is a technique that has been used routinely by the Intelligence Agencies for some decades. My review of paperwork provided by the agencies has demonstrated a continued high standard of submission, setting out the case for necessity and proportionality clearly. The agencies have responded cautiously to the challenges of online surveillance activities. I expect work to be ongoing in this area to ensure that all online surveillance is recognised and recorded with an adequate record of necessity, proportionality and collateral intrusion considerations, particularly where a non-specific authorisation is maintained.

Actions authorised

In my last report I noted that MI5 intended to streamline directed surveillance applications and assure that actions set out under the authorisation align with the specific planned operation. I have been pleased to see significant progress in this area. However, I have **suggested** to MI5 that it would be valuable for DSA paperwork to make reference to the existence of any relevant property warrants. For example, where a CCTV camera is installed under a property warrant and monitored under a DSA, the DSA paperwork should reference the property warrant.

My inspection of directed surveillance conducted by the MOD has noted that collateral intrusion, where individuals other than the subject of the surveillance are monitored, is handled sensitively, and all relevant intelligence has been deleted in line with MOD internal policies.

Calculation of expiry

It is unfortunate that there are discrepancies in the current legislation to guide officers calculating the duration of directed surveillance authorisations; this has led to some confusion. I am confident that this will no longer be the case under the IPA and codes of practice.

I have **recommended** that GCHQ in particular apply a standard approach to eliminate any confusion from this process. I have suggested GCHQ should use the date of signature as the start date for any

directed surveillance authorisations, and should not post-date authorisations (seeking thereby to commence the same from the date when the activity is to be conducted). Where possible, the authorisation should be obtained close to the planned deployment, to ensure that the necessity, proportionality and intrusion considerations are as accurate as they can be.

When examining the directed surveillance authorisations presented to me by SIS, I noted that in some cases officers had mis-calculated the expiry date. One authorisation had been set for six months rather than three. In this instance the authorisation was cancelled and no unlawful activity took place. I have **reminded** SIS that an initial directed surveillance authorisation is valid for a period of three months only.

I noted one case of MOD paperwork where the authorisation was recorded as running from 11:00 on 17/6/16 to 11:00 17/9/16. The Directed Surveillance Code of practice sets out that the authorisation will expire at the end of last full calendar day of the three month period. In this case this should have been 23:59 on 16/9/16. In this case, no unlawful surveillance was conducted.

Open source surveillance

In my 2015 Annual Report I set out the legal basis for online surveillance using open source data. This might include monitoring or observing a targets conversations and activities online, such as forum postings or chatroom use, where access is publically available. I noted that the agencies were in the process of drawing up a joint policy on monitoring data available online; this work is ongoing. In conversation with the agencies, I **recommended** that the same principles of privacy and collateral intrusion considerations should be applied when conducting surveillance online as when conducting real-world surveillance.

When I inspected GCHQ I reviewed their online surveillance activity and was pleased to see that officers were cautious in applying surveillance principles and were applying for a directed surveillance authorisation where the situation was ambiguous. GCHQ demonstrated to me that they keep a thorough log of all online surveillance activities under a broad directed surveillance authorisation.

Filler text

In last year's Annual Report I commented that I had spoken to MI5 repeatedly about not using filler text in DSA forms. MI5 have now made changes to the workflow forms to ensure that filler text is

not present. MI5 have issued new guidance to ensure that staff are giving appropriate consideration to each element of the form. I would expect future inspectors to maintain close scrutiny in this area, but believe that this issue should be largely resolved. I have **recommended** that MI5 should continue to train staff to record considerations fully on DSA paperwork.

Cross-referencing

I **recommended** to MI5 that DSA forms should consider making reference to other relevant authorisations acting against the same target(s). This is the case for property warrants, for example where the property warrant authorises the installation of a monitoring device which will obtain intelligence which would be examined under a DSA. This might be the case for a CCTV camera, for example, which was not installed within a residential property. I suggested that this would be helpful to ensure that the authorising officer was able to take full consideration of the relevant intrusions.

vi. Bulk Personal Datasets (BPDs)

In my 2015 Annual Report I set out in detail how my oversight of bulk personal data holdings works. This is an area which attracted significant attention in 2016. In August 2016, David Anderson QC, the Independent Reviewer of Terrorism Legislation, published his review into the operational case for bulk powers, including the retention and use of Bulk Personal Datasets (BPDs). The findings of this review informed the detail of the IPA, section 7 of which sets out the power to obtain, retain, use, and delete bulk personal datasets for the first time. This welcome change will replace the current legislation[2] under which the agencies obtain and use bulk data, placing this activity on a statutory footing under the continued oversight of the Investigatory Powers Commissioner. I have **recommended** that the agencies should work proactively to prepare for the requirements under the IPA to ensure that procedures are tried and tested before the implementation data.

The Act sets out that *an intelligence service retains a bulk personal dataset if-*

a) the intelligence service obtains a set of information that includes personal data relating to a number of individuals,

b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions,

c) after any initial examination of the contents, the intelligence service retains the set for the purpose of the exercise of its functions, and

d) the set is held, or is to be held, electronically for analysis in the exercise of those functions.

Each agency holding any BPD must set out a clear case for obtaining and retaining the BPD and ensure protective safeguards are in place to prevent misuse. Datasets which contain sensitive personal information, as defined by the Data Protection Act (1998) require a more robust justification to evidence why it is necessary and proportionate to acquire and retain the data, and where necessary additional protective safeguards. In all cases, the agencies must not hold BPDs for longer than is necessary for the proper exercise of their functions.

I conducted a specific review of BPDs at each agency during both of the annual inspection rounds.

[2] 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.

My overall assessment

During my inspection of the agencies, I review the usage of each BPD to satisfy myself of the case for retaining and using each dataset. I was pleased to see the safeguards in place at each agency and am confident in each agency's record of use. I noted that the agencies set out access controls and limitations and commend the close attention paid to maintaining standards in this sensitive area. In the paperwork I reviewed, good consideration had been given to the necessity and proportionality to holding BPDs, however in some cases I would like to have seen a clearer demonstration of privacy considerations.

Financial dataset issue

In 2015, GCHQ reported to me that they had identified a potential error, whereby a small number of financial datasets had not been correctly deleted. The lack of clear process around handling and deleting datasets at the time meant that the deletion process had not been properly approved and recorded. During 2016, GCHQ provided an update to me, following an internal investigation. I have been pleased to see that GCHQ have taken lessons from this process and have instigated a clear mechanism to prevent errors of this kind in the future. GCHQ have confirmed that this problem is now resolved.

Ingestion delays

In my 2015 report, I noted concerns around the dataset ingestion process at the agencies, which in some cases had led to a significant delay in datasets becoming available in analytical systems. I commented that this undermined the case for the necessity of obtaining the dataset. During my inspections in 2016 I was pleased to see fewer instances of delayed ingestion, however at MI5 I noted two cases where ingestion had taken over a year. I was advised that in one case this was because the investigative area in question was of a lower priority**.** I was persuaded to accept the case for retention but worried that a significant delay seriously weakened the case for retention.

Duplication

In my previous Annual Report, I highlighted my concerns about the agencies holding duplicated datasets, including other government data holdings. I am satisfied by the need for the agencies to hold copies of datasets to enable proper analysis. I am pleased to see that the agencies have worked to streamline dataset holdings, and are making progress towards centralised, shared holdings. While I understand that this is technically complex, I am pleased to see the agencies working to establish comparable safeguards and sanctions against misuse of data. I **recommended** that where the

agencies are able technically to maintain a shared BPD holding, that the BPD is presented only once to the Commissioner for tri-agency oversight.

Privacy considerations

During my inspection SIS showed me that they had introduced standard forms, which set out proportionality and necessity considerations clearly following comments that I had made during my 2015 inspections. I felt that this was a sensible approach, but **recommended** that the justification box on applications for BPD holdings should be used to address any intrusion into privacy. I was confident as a result of conversations I had with individual officers whilst inspecting SIS, that necessity considerations are held to a very high standard, but I continue to **recommend** that analysts should make a better record of the steps they have taken to minimise the intrusion into privacy.

Review of GCHQ datasets

In my 2015 Report I referred to a case at GCHQ where there were apparent gaps where the internal processes and paperwork had not been properly completed in accordance with the GCHQ BPD handling arrangements. GCHQ explained that this error had been caused by the dataset not having a nominated responsible officer. 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 conducted this search. Two instances were brought to my attention where the BPDs had been authorised retrospectively and I examined these cases during my 2016 inspections. In one case a dataset which was acquired in 2013 was not authorised until 2015. This was the result of an administrative error and a lack of understanding of the authorisation process. Access to this dataset was very limited but this was a clear failure to comply with GCHQ internal authorisation policy for BPD. In the second case the dataset was previously held under a different regime with retention authorised under the DPA (see definitions above) and it was not defined as a BPD until 2016. No further instances were found and I was content that this action has been closed.

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; Mi5 have confirmed that this has been changed and that this issue will not arise again in the future.

vii. Consolidated Guidance

In November 2014 I was asked by the Prime Minister to provide oversight for the Intelligence Agencies and MOD applying the Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees (the Consolidated Guidance). The Consolidated Guidance sets out safeguards against the risk of torture and cruel, inhumane or degrading treatment (CIDT) for individuals detained overseas. The Consolidated Guidance is consistent with an absolute prohibition of torture and CIDT in UK and international law. The process for application of the Consolidated Guidance is set out at Appendix B.

I conduct a specific review of Consolidated Guidance application at each agency during both of the annual inspection rounds. The Investigatory Powers Commissioner will have responsibility for this oversight under direction from the Prime Minister when the Act comes into force.

UKIC and the MOD reported 921 cases where the Consolidated Guidance was considered during 2016. This number includes all recorded cases where the Consolidated Guidance was considered, including where the decision was taken that the Guidance did not apply and cases where a judgement was made that there was a less than serious risk of CIDT. The statistics do not show the number of individuals these cases apply to; they simply reflect that proper consideration of the Guidance was applied.

UKIC will apply the principles of the Consolidated Guidance to intelligence requests, including from close trusted liaison partners, where this relates to an individual who has been detained or is likely to be detained overseas. For example, in seeking to counter the threat from IS both in Europe and further afield, UKIC will work with a variety of partners and share intelligence as required. In the course of doing this, UKIC will assess whether individuals are detained or are likely to be detained and will consider whether those individuals would be subject to CIDT. Based on this, UKIC will consider on a case-by-case basis whether to share intelligence with partners, taking a conservative approach to the guidance, which I welcome.

My overall assessment

In my 2015 report I recommended that GCHQ and SIS reviewed their processes for identifying and recording cases where the Consolidated Guidance has been used. I have been pleased to note

significant improvement in this area. The agencies and the MOD have consistently shown that the Consolidated Guidance is being applied thoughtfully and that there is a general commitment to continual improvement of process to support officers taking decisions in this area.

It is I think important to stress that in my view the existence of the Consolidated Guidance is well known to all individuals who have to deal with circumstances to which it may apply. It is indeed in every individual's own interest to make sure that the guidance is complied with, because as the guidance itself says, compliance gives the best chance of an individual not being complicit in what might otherwise be a criminal offence or an offence under International Humanitarian Law. It is for this reason that I have confidence that individuals and the agencies are making every effort to draw to my attention all cases when the guidance should be considered. There are however points to be made below.

During my inspection of MI5 I noted that the forms used to record decisions and considerations relating to foreign liaison intelligence requests set out a consistent and high standard of application when the Consolidated Guidance is engaged.

GCHQ processes a high volume of intelligence requests from liaison partners, these include requests to pass GCHQ intelligence on to a third party. GCHQ's internal process comprises an initial assessment by the 24/7 response team, which identifies whether the Consolidated Guidance principles should be applied, ie where the intelligence relates to a detainee or there is a possibility of detention as the result of intelligence being passed. Where the triage assessment determines that a further consideration under the Consolidated Guidance should be made, the request is passed to the International Policy team.

During my inspections, GCHQ flagged for my attention that they had identified a total of 35 instances where the 24/7 response team had not successfully identified that the Consolidated Guidance review process should have been followed. Further investigation suggested that in eight of these cases, the intelligence should not have been shared. GCHQ have stated that they have no reason to believe that passing the intelligence would have made a material contribution to detention. I commended GCHQ's resolution to change the internal referral process and initiate a more extensive training programme. I would expect that this will lead to a reduction of errors in the future. I was pleased to see that GCHQ is proactively monitoring and reviewing referrals in this way.

In some instances, I noted that GCHQ's Consolidated Guidance Grid was amended retrospectively. Although there is no evidence that GCHQ had not given full consideration to the Guidance at the appropriate time, I **recommended** that a full and accurate record should be completed to document considerations at the time of decision making and not amended retrospectively.

SIS follow a similar process, whereby all requests and decisions relevant to the Consolidated Guidance should be referred to a central team. SIS compiled a grid of relevant cases for scrutiny. I **recommended** that the process for centrally referring Consolidated Guidance-related decisions, and for compiling the grid should be more comprehensive, because it was clear from my inspection that some instances were not fully recorded. However, I noted that the application of the Consolidated Guidance by SIS officers was exemplary. SIS are also in the process of updating their systems and processes; I expect that this will enable full capture of relevant decisions in the future.

During my inspection, SIS were proactive about drawing my attention to cases, such as those relevant to non-State actors, which fall beyond the scope of the Consolidated Guidance but to which they planned to apply the principles of the guidance. I have previously **recommended** that this approach should be taken, applying caution where necessary. I have asked SIS to highlight in the grid for selection any cases which are unusual or where policy or the guidance has not been complied with to improve the oversight process.

Assurances

I have discussed the practice of obtaining assurances from liaison partners with the agencies. In my 2015 Annual report 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 are content to sign them. Gaining assurances from liaison partners is clearly a delicate balance between maintaining a standard and reacting sensitively to specific relationships. SIS maintain an assurances template for officers to use while working with overseas liaison. I have **recommended** that the central team managing the template should make clear to overseas officers that this is a "gold standard" template and should not be restrictive; stations must take a final decision based on local knowledge. I **recommended** that in addition to case-by-case consideration of the risks to any detainee, MI5 would benefit from recording any instances of possible mistreatment or denial of due process in relation to European countries. I suggested that enabling staff to cross-referenced this data would improve the confidence of any risk assessment provided on the relevant form.

I **recommend** that where possible it is best practice to obtain written assurances, but in situations where verbal assurances have been received these should be followed up with a written response. I have **recommended** that a record of verbal assurances should always be made and centrally recorded. I have further **recommended** to SIS that they should obtain renewed assurances from the liaison partners at least annually during periods of ongoing cooperation. I noted that this could take the form of a letter from SIS to confirm what the assurances are in place and that there are no changes. I also suggested that SIS should ensure that any new liaison interlocutors or assurance providers are aware of the assurances, and that assurances remain up to date. The Foreign Secretary has asked for details of SIS processes in place for dealing with certain liaison partners. I have **recommended** that the FCO should obtain a copy of assurances obtained in relation to detainees and make these available to the Foreign Secretary.

WARRANTS AND AUTHORISATIONS

During my inspections I noted a number of broader points which apply to the process of applying to authorisations more generally.

Cancelling Warrants

As mentioned above and in my 2015 Annual report, ISA s6(3) and RIPA s45 requires that warrants must be cancelled if they are no longer necessary. I have asked the warrantry units and the agencies to improve their processes for checking when a warrant is no longer in use. I **recommend** that a consistent mechanism for cancelling warrants should be implemented by each agency.

My inspection of MI5 identified one case where a warrant had not been cancelled at the earliest opportunity because of resource constraints during a busy period. While I understand that the agencies must focus resources on high priority work, I **reminded** MI5 that the cancellation process must not be neglected simply as a result of competing operational pressures.

Error reporting

Each agency notifies me of errors throughout the year and in some cases raises specific errors for consideration during my inspections. I noted that GCHQ was not providing timely error reporting and had built up a backlog of errors. In some cases, this resulted from the desire to complete an internal investigation into the error before providing me with a thorough report. I **recommended** that GCHQ should establish a mechanism for ensuring all errors were reported at the time of discovery, pending investigation. I was pleased that GCHQ responded quickly to this recommendation and am satisfied that there is no longer a backlog.

Reliance on the warrant submission

The warrant submission provided to the Secretary of State provides details of the operational plan and case for necessity and proportionality as well as privacy considerations. The submission document will outline certain restrictions and make specific undertakings which form the basis of the authorisation. I have **recommended** to MI5 that it would be a good idea to set out in the warrant that the activity authorised was subject to the conditions and terms in the accompanying submission. I have also **suggested** that the NIO should consider including a caveat on the warrant instrument to set out that the warrant is reliant on the details provided in the submission.

Collateral intrusion considerations

In my inspections I have scrutinised whether each agency has provided precise details regarding the mitigations in place to limit collateral intrusion. While I understand that it is not straightforward to set out the anticipated collateral intrusion with absolute accuracy ahead of any planned operation, I have been particularly anxious that it should be made clear what should happen to any material which is collected but not of intelligence interest. A general reference to handling arrangements I have suggested is not satisfactory (see further below). I have **recommended** that the warrantry units should provide oversight in this area and should encourage the agencies to make explicit i) likely collateral intrusion and mitigations in each submission and separately ii) how any information what is not of intelligence value will be handled.

Jargon

Each of the agencies use codewords and jargon as part of their everyday business and I understand that this is an important part of safeguarding sensitive intelligence and techniques. I reminded MI5 in particular of the importance of using plain English in submissions. This will be vital to effective judicial pre-authorisation.

PROTECTIVE MONITORING

In my 2015 Annual Report I provided details of my inspection of the internal controls in place at each intelligence agency. These controls are designed to prevent misuse of data by restricting staff access and ensuring all access to the data is necessary and proportionate, minimising the intrusion into privacy. Each agency proactively conducts protective monitoring to identify any misuse of data, and reports to me instances of misuse.

I am confident that this regime identified misuse of data by staff. The agencies have reported to me any instances of misuse and detailed their investigations into this activity. The breaches identified are typically minor, and I commend the approach taken by the agencies where they have any concerns about the individual involved.

I have been pleased that UKIC has worked to manage the risk of external individuals, such as contractors or secondees working with access to sensitive datasets. The agencies have demonstrated that access controls and safeguards are in place to prevent misuse by these individuals, but have suggested that this continues to be a vital piece of work. I have **recommended** that MI5 should make it plain to secondees and contractors that they are subject to MI5 rules of conduct regarding access to data and ensure all people working on MI5 premises know the consequences of misuse. This also applies to the other agencies.

PRODUCT OBTAINED AND HANDLING ARRANGEMENTS

In 2015 I asked the Intelligence Agencies and the MOD to provide me with a comprehensive breakdown of their handling arrangements. The handling arrangements set out how the agencies obtain, retain, store and delete information. Work is ongoing to establish a set of handling arrangements which can be referenced in submissions such that any Secretary of State is clear on how any intelligence obtained under a warrant will be handled.

During my inspection of MI5 I noted that a number of submissions stated that intelligence would be treated in accordance with the "normal handling arrangements". It is important that at the point of authorisation the Secretary of State is clear as to precisely how any intelligence obtained will be handled. The agencies should therefore be as specific as possible about how they intend to store, retain, access and delete any intelligence obtained under any authorisation. I have **recommended** to the warrantry units that they should consider encouraging the agencies to refer to particular paragraphs of the handling arrangements in submissions.

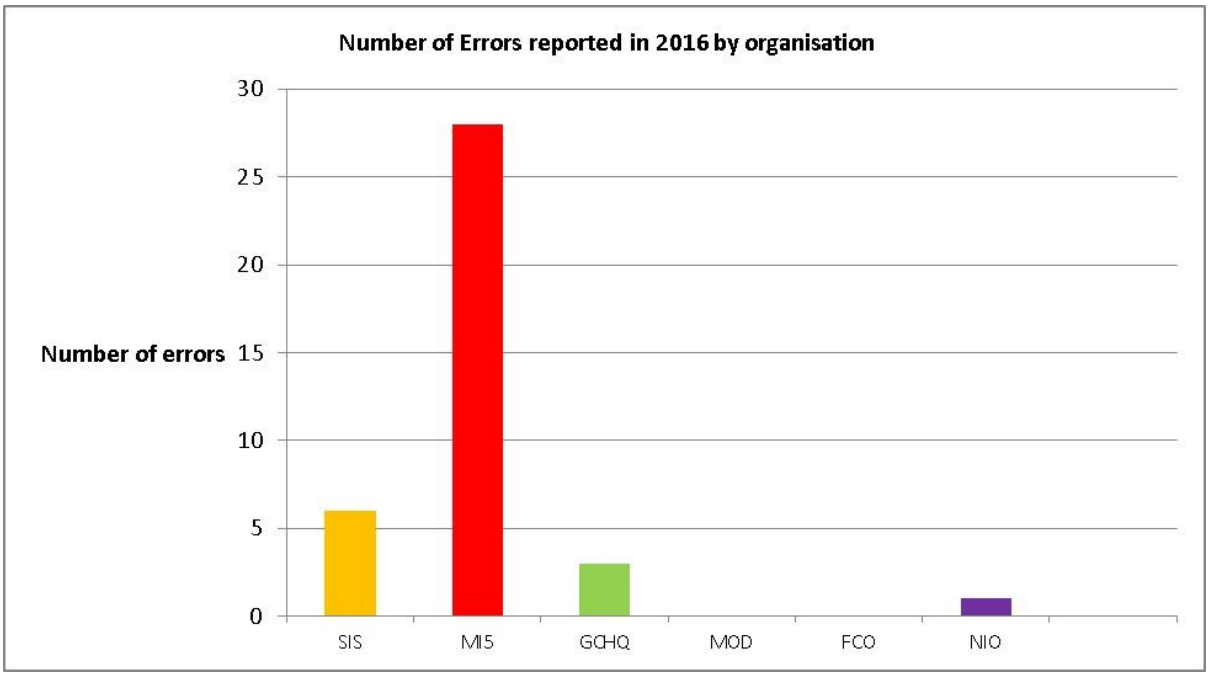
ERRORS

Summary of 2016 errors

I require the agencies to report to me any errors that might have occurred during a warrant application, authorisation or when the warrant was put into operation. Examining these reports is an important element of my oversight of how the agencies use their intrusive powers. I expect the reports to explain:

1) When an error occurred
2) When it was discovered
3) The nature of the error
4) How it happened and
5) What, if any, unauthorised invasion of privacy resulted
6) Steps taken to avoid errors happening again.

In 2016 there were 38 errors reported in total. This is a significant drop of 54% from the 83 errors reported in 2015.

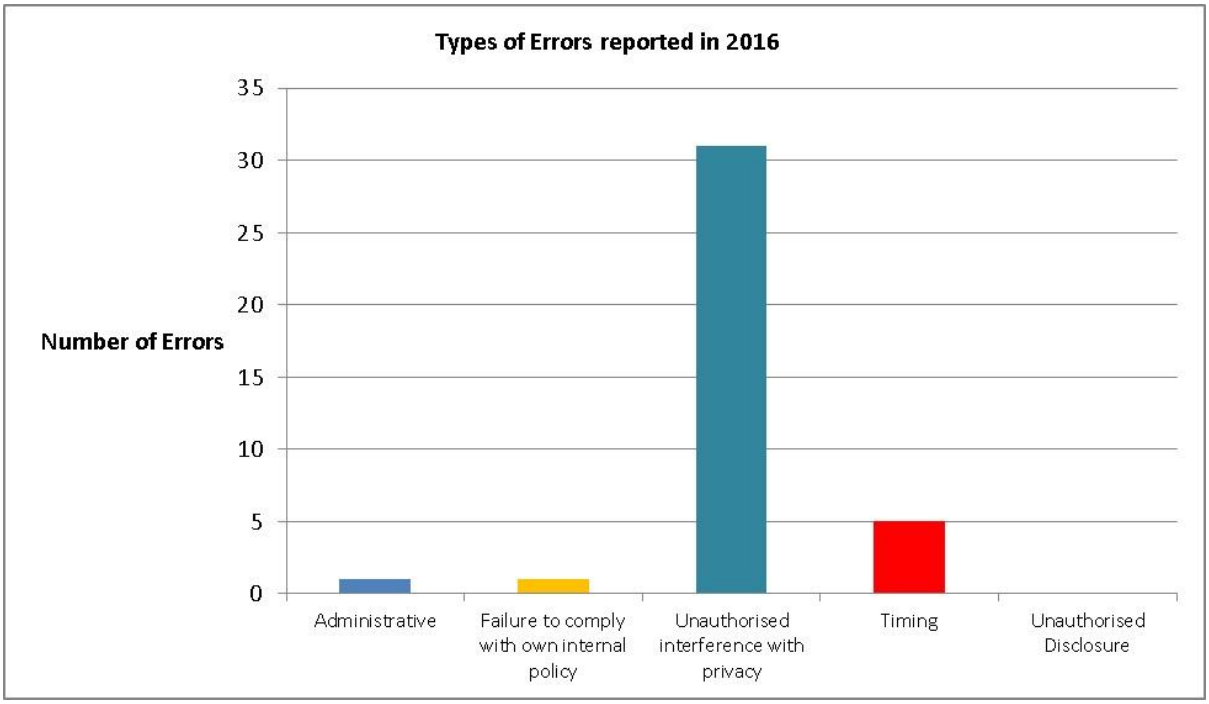


Please note that MI5 obtain a significantly larger number of warrants and authorisations than the other agencies, and their error rate is in fact low as a proportion of authorisations.

Categories of errors

Category A	Category B	Category C
An administrative error such as where a typing error has occurred and the correction is obvious	A situation where there has been, for example, an inadvertent failure to renew a warrant or obtain authorisation in time and where, if done properly, the application would have been granted	A deliberate decision to obtain information without proper authority and with no

In 2016, 37 errors were Category "B" errors or inadvertent errors and only one was a category "A" or administrative error. There were no category "C" error which was the same as 2015.



Breakdown of errors by organisation

Of all the errors, the most common error was an unauthorised interference with privacy. There were no recorded errors that were due to unauthorised disclosure in 2016.

Security Service (MI5)

In 2016, MI5 reported 28 errors to me, including a non-MI5 error by another Public Authority

Of the 28 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, or failure to apply in sufficient time
- A non-MI5 error is included in their total amount of reported errors. The error occurred when a Public Authority failed to remove a target from the Automatic Number Plate Recognition (ANPR) list on time as requested by MI5. As a result continued reporting was generated on the target, even though this was no longer necessary or proportionate and the DSA had been cancelled by MI5. This was an unauthorised interference with privacy and the product collected was later destroyed.

Example error: I highlight this error in particular, as typical of the kind of Category B errors that are reported to me.

In 2016, MI5 reported to my office a CCTV error whereby the investigative team judged that it was no longer necessary and proportionate to conduct surveillance against a target. Because of this judgement, MI5 stopped conducting full surveillance against the target. In this case, surveillance was conducted using a device that had been installed under a property warrant and which needed to be removed. During the period before the device could be extracted, MI5 technical officers needed to turn the device on occasionally to make sure it was still working correctly and to help them to plan an extraction. It is clearly not necessary and proportionate to maintain a full surveillance authorisation against the target and so MI5 maintain a thematic DSA authorisation (see above) to cover devices awaiting extraction and cancel the individual DSA.

In this instance, an error occurred because the device was not added to the thematic authorisation before the DSA was cancelled. Three days of unauthorised surveillance, in the form of device checks only, were conducted before the error was identified and rectified. The data obtained during this time has since been deleted, and MI5 have undertaken to review this process to ensure that future errors of this kind do not occur.

Secret Intelligence Service (SIS)

In 2016, SIS reported 6 errors to me in total. During my inspections all the submissions and authorisations I scrutinised were in good order and I did not identify any Category “A” errors.

Of the 6 errors:

- almost all were caused by human error and resulted in intrusion into privacy to some degree, with two separate cases where it was the timing that was the issue for example, warrants not been sourced on time, or failure to apply in sufficient time
- none were caused with the intention to obtain information without the proper authority.

Example error: I highlight this error as an example of an instance where SIS officers have reported an issue to me, which is representative of the kind of Category B errors that are reported.

In 2016, SIS reported that an officer had completed a RIPA CHIS authorisation form before going to conduct an agent meeting within the UK. This is a rare occasion, where SIS acted within the UK to meet their functions and so RIPA paperwork was completed with attention to any necessity and proportionality considerations. The officer realised that the form had not been signed by his superior officer ahead of the meeting, although they had discussed the operation in detail. This failure to complete the paperwork had resulted in an unauthorised operation and was reported to me.

Government Communications Headquarters (GCHQ)

In 2016, GCHQ reported two errors to me which resulted in unauthorised interference with privacy. None were caused with the intent to obtain information without the proper authority. Due to the small number and sensitivity of errors at GCHQ it is not possible to provide an example.

Home Office, Foreign Office, Ministry of Defence and Northern Ireland Office

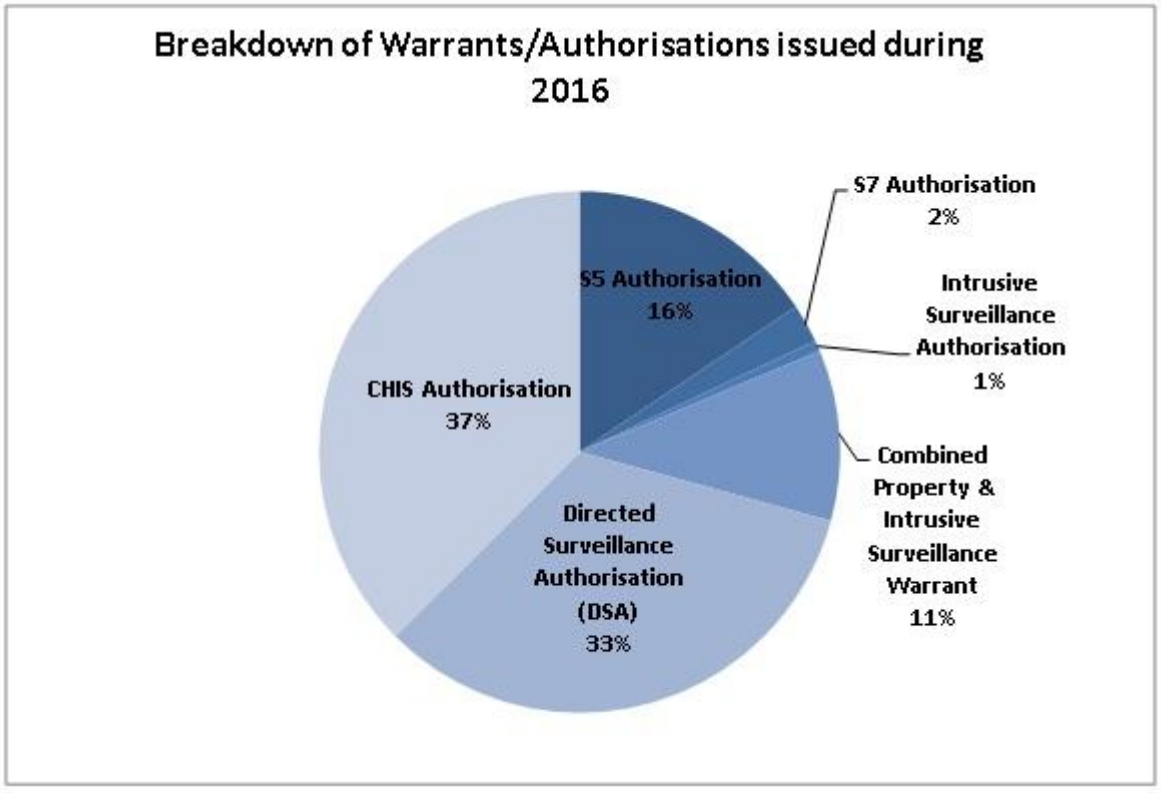
In 2016, the Home Office Warrantry Unit, Ministry of Defence and Northern Ireland Office did not report any errors to me, nor did I uncover any during my inspections.

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 part 2/ISA warrants and authorisations extant at the end of 2016, across the agencies and MOD, was 1926. 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:



Of the RIPA and ISA warrants and authorisations in effect in 2016 I scrutinised 423. 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.

BRIEF SUMMARY OF ASSESSMENTS

MI5

	Round 1	Round 2
Selection	9 May 2016	
Pre-Reading days	7-9 June 2016	8-11 November 2016
Inspection days	30 June 2016	1 December 2016
Under the bonnet		

MI5 Summary	
Necessity **Was the case for necessity made in each case inspected?**	The case for necessity was well set out in the paperwork I reviewed.
Proportionality **Was the case for proportionality made in each case inspected?**	I was content with the demonstration of proportionality in the cases I selected for scrutiny.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?**	This is generally well represented. However, I have continued to suggest that MI5 should pay greater attention to steps taken to mitigate intrusion.

My inspections at MI5 led to a number of conversations about challenging legal issues; I was pleased with MI5's proactive engagement with my office on these matters. In particular, I noted that MI5's lawyers were keen to discuss operations that were not foreseen by current legislation. I will expect MI5 to work closely with the IPC to ensure that these challenging areas are adequately considered under the new legislation.

I identified a small number of process problems, including around incorrect renewal dates, but on the whole have seen significant progress in MI5's use of authorisation workflows. I am pleased that the issue of filler text has finally been resolved.

I have made **recommendations** relating to interdependency of authorisations, which I believe will help MI5 to establish greater clarity going forward. This includes making reference to existing warrants in DSA submissions and to letters of clarification in renewal paperwork.

I was content with the LPP processes that MI5 showed me. I have commended MI5's clear application of consolidated guidance considerations. I have suggested that there may be merit in establishing a central holding for concerns around due diligence and the risk of mistreatment for European partners in particular. I believe that this would support staff making risk assessments and enable them to between share concerns between sections.

SIS

	Round 1	Round 2
Selection	21 April	24 October
Pre-Reading days	12-13 May	14-15 November
Inspection days	18-19 May	16-17 November
Under the bonnet	8 February	

SIS Summary	
NECESSITY **Was the case for necessity made in each case inspected?**	The case for necessity was set out in each case I selected for scrutiny. In one case I inspected, it could have been more explicitly set out in terms of the National Security benefit.
PROPORTIONALITY **Was the case for proportionality made In each case inspected?**	In each of the cases I selected for review, the case for proportionality was set out.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?**	The balance of intelligence gained against intrusion into privacy was mostly set out in the paperwork provided for reading to demonstrate how the intelligence gained outweighed the intrusion. In one instance, I recommended that intrusion considerations should be set out more clearly to a liaison partner.

As well as SIS Head Office in London, I visited three stations in 2016. My Inspections at SIS have continued to reveal an inconsistent approach to record keeping. I am confident that SIS is committed to improving the quality of written records made by staff, but continue to note that staff are inconsistently applying standards set out. I expect that this will continue to be a focus of consideration for the Intelligence Services Commissioner in the future.

I have been very impressed by the standard of consideration given by SIS officers, including those I have met working overseas, to the risks of working with foreign liaison and with the care taken by officers to ensure high standards of necessity and proportionality. However, I continue to believe that poor record keeping, particularly with regard to CHIS activity outside of the UK, means that these considerations are not adequately set out. I have urged SIS to ensure that renewal paperwork for CHIS is completed at the appropriate time, and that they should be careful to make sure expiry dates are accurately recorded on any CHIS authorisation paperwork.

It is important to note, however, that this criticism does not extend to SIS's consideration of the consolidated guidance. I have been pleased to note that officers apply the guidance cautiously. I am confident that SIS have provided accurate and timely submissions to Ministers and that the level of oversight and consideration in this area is excellent. I have been pleased to see that SIS have worked with liaison partners to obtain written assurances, where possible, in relation to detainee treatment. I have suggested to the FCO and SIS that where possible it would be helpful to provide these documents to the Foreign Secretary.

With regard to LPP material, I am content that SIS identifies and handles LPP and confidential material appropriately.

GCHQ

	Round 1	Round 2
Selection	15 February	15 August
Inspection days	18-20 April	10-12 October
Under the Bonnet	11 February	5 September

Detail GCHQ	
Necessity **Was the case for necessity made in each case inspected?**	The "Record of Reliance" could more explicitly set out the case for necessity, but the necessity case was made out in the authorisation paperwork.
Proportionality **Was the case for proportionality made in each case inspected?**	I have recommended that more specific warrants and authorisations should be used under the IPA to ensure that proportionality is addressed fully. The proportionality case was set out in the cases I selected for scrutiny.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?**	Privacy considerations were set out in the cases I selected for reading.

During my inspections I noted that GCHQ has improved the standard of internal paperwork. I was pleased that the internal investigation into the existence of certain financial datasets has been completed and I am satisfied that GCHQ is maintaining high standards around data handling.

GCHQ works closely with liaison partners and is involved in regular intelligence sharing and at times collaborative work. This is a complex area for both GCHQ and SIS, where agency staff work with partners who are applying different and sometimes incompatible legal frameworks. I have been impressed by the efforts of GCHQ's staff to gain assurances from partners, particularly with regard to the consolidated guidance. I have recommended that GCHQ should consider making reference in relevant submissions to the fact of local laws which will affect any partner's activity. UK law cannot

overwrite the local laws for a foreign partner, nor can UK law make lawful any activity by a foreign agency in the UK, unless they are acting as a third party on behalf of GCHQ. In my view, it would be beneficial to set out where an independent legal system is also in play on any operation.

I was satisfied that GCHQ is applying the principles of the consolidated guidance sensitively, and am pleased that changes made to the training for 24/7 staff are raising the already high standard of the referrals process. I noted that on occasion GCHQ officers updated the consolidated guidance log after the fact to clarify judgements or details. While it is important to represent the fullest available facts, I recommended that GCHQ should set out points of clarification in addition to and not amendment to the original log entry. GCHQ subsequently confirmed that this has been implemented.

I have no concerns about GCHQ's identification and treatment of LPP and confidential material. I have been pleased to see that GCHQ's recent investment in this process has been successful in improving the referral and designation process more effective.

MOD

	Round 1	Round 2
Selection	2 June	14 November
Inspection days	14 June	28 November

Detail MOD	
NECESSITY **Was the case for necessity made in each case inspected?**	The necessity was set out in all cases provided to me for scrutiny.
PROPORTIONALITY **Was the case for proportionality made In each case inspected?**	In the paperwork I selected for review the proportionality case was set out.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?**	The paperwork provided demonstrated the weighing up of the intrusion into privacy against the intelligence to be gained.

My inspection of the MOD confirmed that the consolidated guidance is being applied consistently by staff and that an excellent record of considerations has been applied. I have been pleased to see that the MOD's submissions to the Defence Minister have clearly set out the risks of any planned operations where there is a risk of detention.

I made several recommendations in my last Annual Report in relation to the MOD's use of directed surveillance authorisations. I have been pleased to see that they have been applied. During my inspection, I was satisfied that the MOD is handling surveillance-related intelligence in line with their internal handling arrangements.

Home Office

	Round 1	Round 2
Selection	16 May	22 November
Inspection days	21 June	7 December

Detail Home Office	
Necessity **Was the case for necessity made in each case inspected?**	The case for necessity was set out in all of the paperwork I selected for scrutiny.
Proportionality **Was the case for proportionality made in each case inspected?**	In all of the cases I reviewed, the case for proportionality was set out.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?**	The balance of intrusion in relation to the intelligence gained was demonstrated in all of the cases provided to me for review. However, there was not always sufficient detail on the actions to be taken to reduce collateral intrusion. Cases where officers do not use standard wordings typically provide a better description of this detail.

The Home Office is responsible for handling a large number of warrants from MI5, which include a number of thematic warrants. Because of the complexity of these warrants, I have asked in the future that the Home Office should provide all thematic warrants for scrutiny during inspections.

The provisions under ISA section 5 and RIPA with regards to what is now termed electronic interference are complex. As a result, MI5 are often required to obtain several authorisations in tandem relating to an individual activity. I have previously recommended that the Home Office should take care to ensure that any computer equipment is identified in the property detail, rather than the actions of the warrant. I would urge the Home Office to continue to scrutinise any electronic equipment-related warrantry during the transition to the IPA.

I have suggested to each of the warrant granting departments should work with the agencies to agree the Handling Arrangements for specific operations. The Home Office should ensure that these have been signed off by the Home Secretary and are used to inform her consideration of the intrusion into privacy relevant to any warrant submission.

NIO

	Round 1	Round 2
Selection	15 April	24 October
Inspection days	23 May	20 – 21 October

Detail NIO	
NECESSITY **Was the case for necessity made in each case inspected?**	The paperwork provided to me for scrutiny made a case for necessity.
PROPORTIONALITY **Was the case for proportionality made in each case inspected?**	The cases I reviewed set out the case for proportionality.
INTRUSION **Did the intelligence to be gained outweigh the invasion of privacy?**	There continues to be sporadic considerations of how collateral intrusion will be mitigated in the paperwork provided to me. However, the case for intrusion into privacy is mostly set out and weighed against the intelligence gained.

My inspection of the NIO noted a high standard of paperwork, which I was pleased to note demonstrated the appropriate necessity, proportionality and privacy considerations. I did note, however, that submissions from MI5 to the Secretary of State for Northern Ireland assumed a certain level of knowledge about the target. I would like to see set out in more precise detail the relationship between the subject of the warrant and the relevant terrorist group, as well as the operation's stated aims. While I have every confidence that the Secretary of State is well versed in the threat picture, I believe this measure would improve independent oversight and will smooth the process of judicial pre-authorisation under the IPA.

I have recommended that, for clarity, the Northern Ireland Office should consider including a caveat on the warrant instrument to state that the warrant is subject to certain terms of the submission. I

am aware, however, of certain legal arguments against this and so expect that this matter will be discussed further with my successor and subsequently the new IPC.

Foreign and Commonwealth Office for SIS

	Round 1	Round 2
Selection	21 April	24 October
Inspection days	20 June	5 December

Foreign and Commonwealth Office for GCHQ

GCHQ	Round 1	Round 2
Selection	1 June	19 October
Inspection days	17 June	7 November

Detail Foreign and Commonwealth Office	
Necessity **Was the case for necessity made in each case inspected?**	The case for necessity was clearly set out in the paperwork provided to me for scrutiny.
Proportionality **Was the case for proportionality made in each case inspected?**	The case for proportionality was set out clearly in the paperwork provided to me for review.
Intrusion **Did the intelligence to be gained outweigh the invasion of privacy?**	The case for privacy was set out in the paperwork I inspected. However, the submission must set out how material that is not of intelligence interest will be handled.

During my inspection of the FCO I examined their processes and practice of oversight of GCHQ and SIS warrantry. My primary concern was whether sufficient information was provided to the Foreign Secretary during this process to ensure that he could make fully informed considerations of necessity and proportionality and was aware of the intrusion into privacy that would likely result. This latter consideration is of particular note with broader warrants, where the detail of planned

operations may not be set out in the original submission. I suggested that the FCO, along with the other warrant granting departments, should work with the agencies to agree the Handling Arrangements for specific operations and make sure these have been signed off by the Foreign Secretary. I believe that this would provide additional reassurance to the Foreign Secretary on precisely how any intelligence obtained will be handled by the agencies.

The Foreign Secretary is also responsible for providing ministerial oversight on occasions where the consolidated guidance has been engaged and the agencies intend to proceed, either with intelligence sharing or a live operation. I have recommended that the FCO should obtain a copy of any assurances that SIS have obtained from a liaison partner. I would advise that these should be made available for the Foreign Secretary to scrutinise while considering any consolidated guidance-related submissions.

Recommendations by organisation

The table below provides a breakdown of recommendations made during the 2016 inspection rounds. The recommendations are not set out in order of priority. Please note that the majority of these recommendations have been actioned and will be business as usual at time of writing. It is also worth noting that these recommendations are, in the main, made on the basis of individual cases and do not necessarily reflect widespread issues. It is usual for the organisation to conduct a broader review, however, to ensure that any issue raised during an inspection is not replicated in cases that have not been provided for scrutiny.

Organisation	Category	Recommendation
GCHQ	Section 7	I requested more detail on the internal authorisations within a section 7 class authorisation to assist my understanding of internal documentation of necessity and proportionality. I requested to see minutes of a senior planning meeting and paperwork for internal records and an internal approval document.
GCHQ	Directed Surveillance	I questioned how GCHQ were calculating the duration of DSA Authorisations – the Code of Practice and RIPA imply that the authorisation runs either from the date signed or from the date it takes effect. The IPA codes of practice will clarify this point. I recommended that GCHQ should use the day of signature as the start date and not to post-date authorisations.
GCHQ	Equipment Interference	EI Code of Practice paragraphs 7.12 and 7.13 state that a senior designated official should approve "particular operations" such that the same official has reviewed the necessity and proportionality case for Approvals and Additions relating to a single operation. I recommended that GCHQ should review any instances where this has not been the case.
GCHQ	Section 5	GCHQ's "Record of Reliance" template for recording activity conducted under a 'thematic' section 5 warrant should include a box for necessity and proportionality.
GCHQ	General	I noted that GCHQ had a backlog of errors which were not reported in a sufficiently timely manner. GCHQ were asked to establish a mechanism for ensuring all errors were reported at the time of discovery, pending investigation.
GCHQ	BPD	GCHQ reported to me the existence of a number of financial datasets which were discussed in an email conversation in 2015 but which were not formally recorded. GCHQ explained that historically, there have been instances where data had been authorised and requested but not obtained and ingested into analytical systems. I requested that GCHQ should conduct a review to confirm whether these datasets were obtained by GCHQ at any point. GCHQ undertook to complete an investigation and to inform me if the datasets were found and deleted.
GCHQ	Consolidated Guidance	In some instances, I noted that GCHQ's Consolidated Guidance Grid was completed retrospectively. Although there is no question that GCHQ had not

		given full consideration to the Guidance at the appropriate time, I recommended that a full and accurate record should be completed to document considerations at the time of decision making and not updated retrospectively.
GCHQ	Section 5	I identified that in one case a paragraph providing detail on planned activities was set out in the renewal but not the warrant application for a section 5 authorisation. Although this did not affect the legality of the authorisation, I asked GCHQ to check all current warrants to ensure that no other case exists of missing paragraphs amended at renewal.
GCHQ	Equipment Interference	I recommended that GCHQ should amend the wording at the end of the Designated Senior Official section of the Internal Approval template to make explicit what exactly is being reviewed in line with the Equipment Interference Code of Practice.
GCHQ	CHIS	I recommended that GCHQ should replicate the CHIS authorisation's review box on internal paperwork to ensure the obligation to conduct regular reviews is explicit.
GCHQ	BPD	I recommended that where the agencies are able technically to maintain a shared BPD holding, that the BPD is presented only once to me for tri-agency oversight.
GCHQ	BPD	I recommended that GCHQ should establish a working definition of BPDs with consideration to the definition of personal data which comes under the Data Protection Act.
MI5	Property Warrant	I asked MI5 to investigate a potential error: MI5 submitted to cancel a warrant which expired on 31/01/15. The warrant authorised the installation and extraction of monitoring equipment. MI5 did not apply to include this device under a thematic warrant until 21/2/16.
MI5	General	I reminded MI5 that it would be a good idea to set out in the warrant that the activity authorised was subject to the conditions and terms in the accompanying submission.
MI5	General	I recommended that MI5 should ensure that any submission clearly sets out how intrusion into privacy, particularly collateral intrusion, will be mitigated.
MI5	Consolidated Guidance	I recommended that in addition to case-by-case consideration of the risks to any detainee, MI5 would benefit from recording any instances of possible mistreatment or denial of due process in relation to EU countries. I suggested that enabling staff to cross-reference this data would improve the confidence of the documented risk assessment.
MI5	CHIS	I recommended that MI5 should look into whether there is a workflow problem around CHIS authorisation expiry dates which is leading staff to renew paperwork after the authorisation has expired.
MI5	CHIS	I recommended that MI5 should urge staff to record all CHIS reviews.
MI5	General	I recommended that MI5 should remind staff to use plain English in all submissions.
MI5	DSA	I recommended that MI5 should continue to train staff to better complete the DSA forms.
MI5	Protective Monitoring	MI5 should make it plain to secondees and contractors that they are subject to MI5 rules of conduct regarding access to data and ensure all people working on MI5 premises know the consequences of misuse.
SIS	Section 5 and Section 7	I requested that a greater number of Key Decision Documents be presented for review to enable more effective oversight in the future. In addition I requested sight of the internal guidance regarding the use of Key Decision Documents.
SIS	Section 5 and Section 7	I suggested that the use of key decision documents should become standard practice for all thematic warrants.
SIS	Section 5	I recommended that the necessity and proportionality cases should be set out

		in separate sections in submissions for section 5 warrants.
SIS	Section 7	I examined a section 7 authorisation which SIS obtained in relation to a possible detainee scenario. SIS had separately obtained assurances from the liaison partner in accordance with the Consolidated Guidance. I suggested that it should be set out in the warrant that any activity would cease if any evidence of mistreatment was identified.
SIS	CHIS	I advised that SIS should follow the CHIS code of practice, which says renewal should be made shortly before expiry and not pre-emptively, as it becomes difficult to make a necessity and proportionality case months in advance.
SIS	CHIS	I recommended that CHIS authorisations should set out how any collateral intrusion data will be handled, even where this detail is provided in subsidiary paperwork.
SIS	BPD	The justification box on applications for BPD holdings must adequately address any intrusion into privacy.
SIS	Consolidated Guidance	The central team should make it explicit to SIS officers that individual cases must be reviewed with reference to local knowledge and that the 'gold standard template' provided to them may not always apply when assessing risks relating to the Consolidated Guidance.
SIS	Consolidated Guidance	I asked SIS to highlight in the grid for selection any cases which are unusual or where policy or the guidance has not been complied with to improve the oversight process.
SIS	Consolidated Guidance	I recommended that good practice in situations where verbal assurances have been received would be to follow them up with a written response. A record of verbal assurances should always be sent to the central Consolidated Guidance team.
SIS	Section 7	I asked SIS to ensure that warrants in place pending extraction of devices or implants reflect this and do not imply that the warrant is still used to gather intelligence.
SIS	Section 5	I suggested that SIS should mirror GCHQ's submissions where similar technical activities are undertaken. I further recommended that SIS should refer to GCHQ for considerations of intellectual property interference relating to technical activities.
SIS	Directed Surveillance and CHIS	I reminded SIS to ensure officers are aware that an original DSA is only valid for three months and that CHIS are for 12 months.
SIS	CHIS	I recommended that when working with liaison partners to task agents, officers should keep a written record of what the agent is, and is not, tasked to do. The record should be shared and agreed with the liaison unit.
SIS	Consolidated Guidance	I recommended that SIS should obtain renewed assurances from the liaison partners at least annually during periods of ongoing cooperation. I noted that this could take the form of a letter from SIS to confirm what the assurances are in place and that there are no changes.
SIS	Consolidated Guidance	I recommended that SIS should ensure that any new liaison interlocutors or assurance providers are aware of the assurances, and that assurances remain up to date.
SIS	Section 7	I acknowledged differing legal opinions on the need to explicitly cancel authorisations but recommended that SIS should continue to cancel section 7 authorisations in line with ISA section 7(8).

SIS	CHIS	I suggested that officers should not write "N/A" in the "legal and compliance box" of internal notes relating to CHIS activity but that the relevant section 7 authorisation should be referenced, along with any relevant compliance considerations.
FCO (GCHQ)	Section 5 and Section 7	I recommended that, if a cancellation request arrives late, the FCO remind GCHQ that they need to apply for cancellation quickly.
FCO (GCHQ)	Section 5 and Section 7	I suggested that submissions must be clear what will happen to information obtained which is not of intelligence interest.
FCO (SIS and GCHQ)	General	I suggested that the FCO could consider encouraging the agencies to refer to particular paragraphs of the handling arrangements in submissions.
FCO (SIS and GCHQ)	Consolidated Guidance	I noted that the FCO could consider obtaining a copy of assurances obtained in relation to detainees and making these available to the Foreign Secretary.
FCO (SIS)	General	I noted that the FCO should ensure that the drafting is clear on warrant renewals so that the paperwork does not imply that the renewal is subject to an accompanying submission when in reality they are subject to the original submission.
FCO (SIS)	Equipment Interference	I recommended that the FCO should ensure that SIS consider the EI code and refer to it in submissions.
Home Office	Property Warrants	I asked the Home Office to highlight all thematic warrants for selection.
Home Office	Property Warrants	I asked the Home Office to separate ISA thematic warrants from thematic intercept warrants when drafting the summary for the Home Secretary. Where RIPA specifies "persons" may be the subject of the warrant, the ISA requires "property so specified". I recommended that submissions should be presented to the Home Secretary in such a manner as to make this difference clear for thematic applications.
Home Office	Equipment Interference	I asked the Home Office to ensure that the Equipment Interference Code is properly referenced in MI5 submissions and Home Office letters to the Home Secretary
Home Office	Equipment Interference	I recommended that once the Home Secretary has approved the EI handling arrangements. The Home Office should provide these to me as required by paragraphs 6.3 and 6.4 of the EI code of practice.
Home Office, FCO, and Northern Ireland Office	Property Warrants	I asked the Home Office to ensure that computers are identified in warrants as property to be interfered with and not referenced solely under the actions to be taken.
Northern Ireland Office	General	I suggested that the NIO should consider including a caveat on the warrant instrument to set out that the warrant is reliant on the details provided in the submission.
Northern Ireland Office	General	I recommended that the NIO should make sure that MI5 have clearly set out likely collateral intrusion and mitigations in each submission. The NIO should further ensure that it is clear how any information which is not of intelligence value will be handled.
Northern Ireland Office	General	I asked NIO to encourage MI5 to set out the precise relationship between the subject and the purpose of the warrant, such as the specific role of an individual within a terrorist group.

APPENDIX A

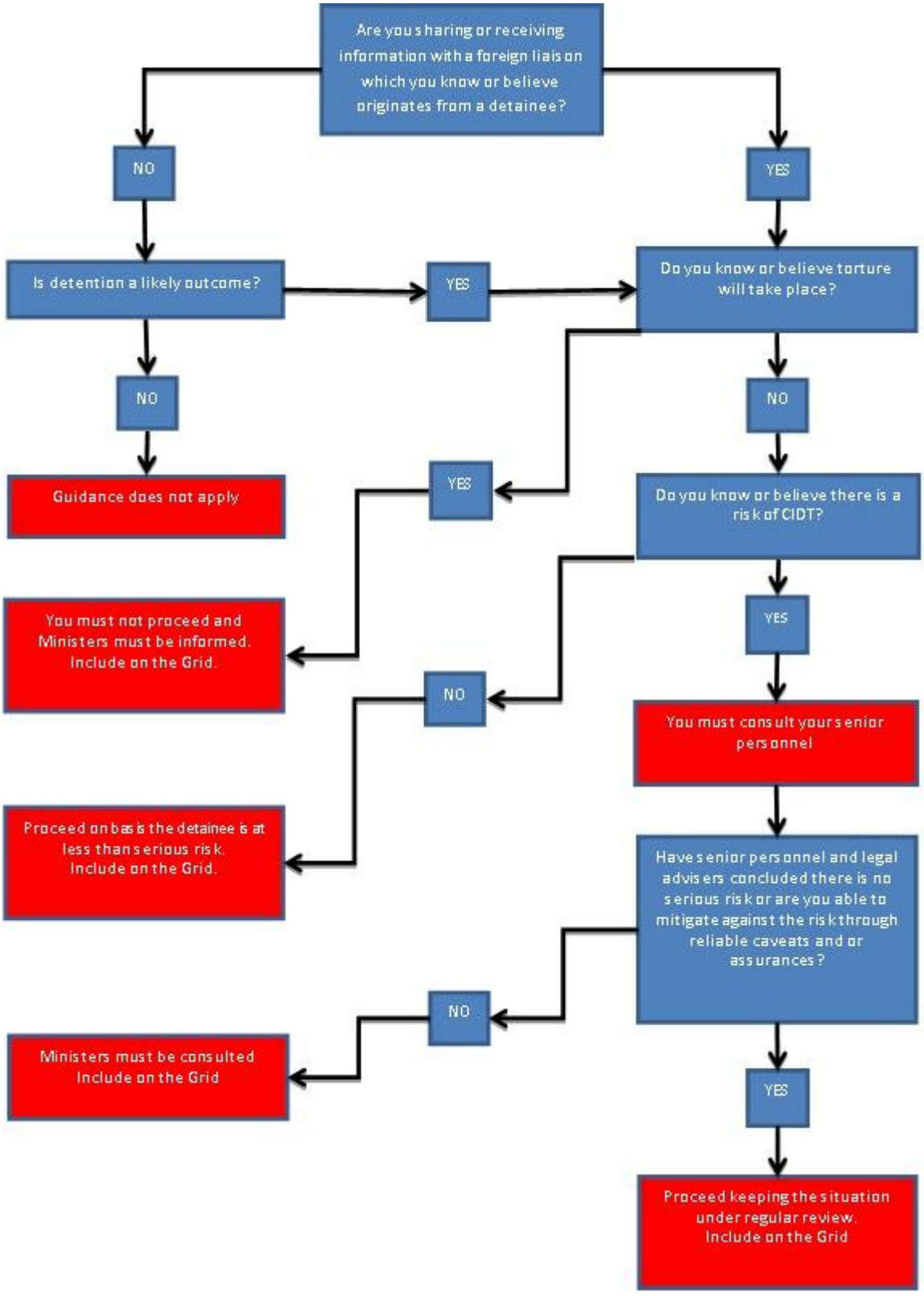
Expenditure

My office's total expenditure for the financial year 2016/17 was £426,049. The table below provides a breakdown of this expenditure.

Description	Total (£)
Staff costs	£341,285.11
Travel & Subsistence	£19,107.00
Legal fees	£29,615.33
IT	£19,608.00
Office Costs (including stationary and printing costs)	£16,434.46
Total	**£426,049.90**

APPENDIX B

Consolidated Guidance Process



ID CCS1217635040 12/17
ISBN 978-1-5286-0175-7