[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

cc [REDACTION] for info & return
EB 19/05/04

Home Office

Legal Adviser's Branch

806, 50 Queen Anne's Gate, London SW1H 9AT
Switchboard 0870 0001585 Fax 0171 273 3629 Direct Line [REDACTION]
E-mail [REDACTION]@homeoffice.gsi.gov.uk www.homeoffice.gov.uk

Sir Swinton Thomas
Interception of Communications
Commissioner
C/o Room 1022 Queen Anne's Gate

Our Ref
Your Ref
Date 14th May 2004

Dear Sir Swinton
The database

1. The purpose of this letter is to inform you of a Security Service proposal and to seek your views on our analysis of the appropriate legal framework, in particular with regard to the ECHR.

2. Please find attached as an annex to this letter an explanation of the Security Service proposal, codenamed ***the database*** project.

3. The implementation and operation of ***the database*** project involves two distinct stages. The first is the transfer of the data by the communications service providers (CSPs) to ***the database***; the second is the retrieval of specified data from the database by the Security Service.

Transfer to database

4. We intend that the first stage should be achieved by the Secretary of State giving a direction to the relevant CSPs under section 94(2) of the Telecommunications Act 1984 c.12). The Secretary of State may make such a direction only if he believes it necessary in the interests of national security. Further, he must believe that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct. We believe that the requirements of necessity and proportionality are met (the reasons for this are set out in the annex - we would be happy to provide further information if that would be helpful). As permitted by section 94(4), we would not intend the direction to be laid before both Houses of Parliament on the basis that disclosure of the direction would be against the interests of national security.

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

5. We do not think that the transfer of the data engages either Article 1 of Protocol No.1 or Article 8 of the ECHR (or any other right guaranteed by the ECHR).

6. The Article 1 of Protocol No.1 issue might be thought to arise because the effect of the direction will be to require the transfer of data belonging to the CSPs (Article 1 of Protocol No.1 expressly protects legal persons as well as natural persons). However, it is questionable whether the ownership of data constitutes a property right such as falls within the scope of Article 1 of Protocol No.1. Even if it does, we would argue that the section 94 direction does not interfere with the CSPs' right to peaceful enjoyment of the data - the direction only requires them to make a copy of the data, rather than handing it over, and the exercise will be cost-neutral for them - and therefore Article 1 of Protocol No.1 is not engaged.

7. Nor do we think that Article 8 is engaged by the transfer of data to ***the database*** and its storage there. Although the transfer and storage of data may in principle engage Article 8 (even if it is not accessed), the data in question must be personal data. In the case of ***the database***, the data will not include any information which on its own would enable a link to a particular individual to be established.

Retrieval of information from the database

8. The second stage [REDACTION] involves retrieval by the Security Service of specified data from the database. In some cases (depending on the information that it already holds or is able to obtain), the Security Service will at this point be able to link the data to a particular individual. Accordingly, we think that this is the first point at which the Service's conduct engages Article 8. In order to ensure that there is no infringement of Article 8, retrieval of the data from the database must meet the requirements of necessity, proportionality and being in accordance with the law.

9. In the case of *Malone v the United Kingdom* (1984) 7 EHRR 14, the European Court of Human Rights considered whether the practice of "metering" whereby the Post Office registered numbers dialled on a particular telephone line and the time and duration of each call could give rise to an infringement of Article 8. The information gathered through "metering" will be included amongst the information which will be held on ***the database*** (see annex). The Court held that the release of information to the police without the consent of the subscriber amounted to an interference with Article 8 (see paragraph 84 of the judgment). Presumably, this was because, once in the hands of the police, the information could be linked to particular individuals and thus became personal information.

10. We intend that the Security Service should apply Chapter II of Part I of the Regulation of Investigatory Powers 2000 (c.23) (RIPA) when accessing the data held on ***the database***, just as it would if it were accessing communications data in the possession of a CSP. Thus a designated person within the Security Service will grant an authorisation under section 22(3) of RIPA to other people within the

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

organisation to access the data if he believes that it is necessary on one of the grounds set out at section 22(2)(a) to (c) and he believes that accessing the data is proportionate to what is sought to be achieved. The authorisation will have to comply with section 23.

11. Section 22(3) provides that the authorisation is "to engage in any conduct to which this Chapter applies". Conduct to which the Chapter applies is defined in section 21 (1). Section 21 (1)(a) seems the relevant limb since the authorisation granted under section 22(3) will authorise the person in question to obtain data from ***the database*** (rather than authorising him to disclose it which would be covered by section 21(1)(b). It might be thought that it is somewhat awkward to fit the second stage [REDACTION] within section 21(1)(a) because the data is already owned by the Security Service but, subject to your views, we think it works (we explain below why we think it necessary to fit the second stage [REDACTION] within Chapter II). The two potential problems are as follows. Firstly, section 21(1)(a) applies to the obtaining of communications data., and it might be argued that the data held in ***the database*** is not being obtained because it is already in the possession of the Security Service. We think this is an unduly technical argument. Given that the data will be stored [REDACTION] and only accessed when it is needed, it seems natural to describe this as "obtaining" data. The second potential problem is that the conduct must be in relation to a telecommunication system. A telecommunication system is defined at section 2(1) of RIPA. It might be argued that the conduct involved in the second stage [REDACTION] is simply conduct for obtaining communications data, and the conduct has no relationship to the original telecommunication system. But, taken to its logical extreme, the same argument might apply to communications data held on a database owned by a CSP. We think a wide view must be taken of "in relation to" such that conduct in relation to something which derives from a telecommunication system for obtaining communications data is covered by section 21(1)(a).

12. The reason why we are concerned that the second stage [REDACTION] should be governed by Chapter II is that we think it necessary for Article 8 purposes. As explained above, accessing the data will amount to a prima facie infringement of Article 8. Although the Security Service could ensure that any individual decision to access was only taken if it was necessary and proportionate to do so, if Chapter II did not apply, we find it difficult to see how the "in accordance with the law" requirement would be met.

GCHQ

13. We understand that at your last warrantry review with GCHQ the ways in which GCHQ acquires its communications data were explained to you, including the fact that GCHQ does not rely on Chapter II of Part I of RIPA for accessing data acquired under a section 94 direction. This is clearly an approach that is different from that described above. However, we do not think that the two approaches are necessarily incompatible, principally because of the way in which GCHQ's present system and that which is proposed for ***the database*** differ.

[REDACTION]

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

14. Most communications data obtained by GCHQ is held in a single database. The majority of this data (approximately 90%) is acquired under the authority of "section 8(4)" interception warrants issued to GCHQ. The remaining 10% of data held in this database is acquired under a section 94 direction. The database does not differentiate between, or in any way flag up, the origins of the data with the result that anyone accessing the data will be unaware of the legal authority under which it has been obtained. To reconfigure the database to allow for such differentiation is not an option because of the technical difficulties and expense that this would entail.

15. However, the long term goal is for a database to be constructed which would allow data obtained under a section 94 direction to be accessed using Chapter II of Part I of RIPA (although the nature of the authorisations will not necessarily be identical to those used for ~~the database~~).

16. A copy of this letter goes to [REDACTION] (Home Office) [REDACTION] (Security Service) and [REDACTION] (GCHQ).

Yours sincerely,
[REDACTION]

[REDACTION]
Home Office Legal Adviser's Branch

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

ANNEX

The database is a project that would give the Security Service an enhanced capability to acquire and analyse communications data and to act on intelligence derived from that data.

Analysis of communications data is a vital investigative technique for the Security Service, particularly in its work to protect national security from the threat posed by international terrorism. **The majority of targets of Security Service investigations use phones**, and the Service acquires communications data from CSPs under Chapter II of Part I of RIPA.

Communications data can provide crucial intelligence about the behaviour and associations of targets [REDACTION]. This data is used to great success but the Security Service is constrained by the resources with which CSPs have to respond to disclosure requirements.

[REDACTION]

Under **the database project**, CSPs would transfer to a Security Service database [REDACTION] **traffic data and service use information** [REDACTION]. The data transferred would always be data already held by the CSPs for, for example, billing purposes and would always be anonymous. The data would be transferred **on a regular basis**. The Security Service would retain the data for six months. Initially **the database project** would involve only selected CSPs although the concept could be expanded [REDACTION].

The database would provide a database of communications data to which the Security Service would have direct access [REDACTION].

Technical safeguards would ensure that data could be retrieved from ***in the database*** only in response to a lawful RIPA authorisation for disclosure meeting the criteria of a specific search. [REDACTION] The vast majority of data held ***in the database*** would never fall within the parameters of a search and never be drawn from the database or viewed by an analyst. To the extent that data was drawn from the database, in many instances it would never be linked to an identified individual. Where a link were made to an identified individual, this would be done using information already held by the Service or subsequently obtained by the Service, for example, by obtaining subscriber information from a CSP using a Notice under RIPA.

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

Copies to DO
16/08/04
[REDACTION]

copied to [REDACTION] on
23/6/04
[REDACTION]
noted
[REDACTION]

cc [REDACTION]

From the Interception of Communications Commissioner:
The Rt. Hon. Sir Swinton Thomas
c/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

[REDACTION]
Home Office
Legal Adviser's Branch
Room 806
50 Queen Anne's Gate
London SW1H 9AT

Our ref: IPS/04 I/1/1

Date: 8 June 2004

Dear [REDACTION],

The database

Thank you for your letter of the 14th May. ***The database*** scheme raises interesting and quite difficult issues. However, I am confident that if there are any problems, they can be overcome.

My reservations relate to the first stage, the transfer to the database. It is proposed that the Secretary of State should give a direction to the CSPs under Section 94(2) of the Telecommunications Act 1984. So far, so good. But I think that since the coming into force of Chapter II of Part I of RIPA this legislation is engaged in such a direction when, as here, communications data are being acquired. It is said that in giving a direction under Section 94(2) the Secretary of State must be satisfied that what is sought to be achieved is proportionate. I am not clear as to where this comes from. It is certainly not in Section 94(2) itself. It may be simply that this is now regarded as a general underlying legal requirement of the acquisition of communications data since the coming into force of Chapter II. If so I am doubtful if that argument would succeed if it was challenged, unless the requirements of Chapter II are also complied with. I do not doubt that the requirements of necessity and proportionality are in fact complied with.

I would hesitate to express an opinion as to whether the ownership of data constitutes a property right. I do not think that this matters. It should be noted that the body of Article 1 of Protocol Number 1 refers to "the peaceful enjoyment of his possessions".

[REDACTION]

{NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD. DOUBLE-UNDERLINED AND ITALICS}

[REDACTION]

I agree that it is doubtful whether the proposed Section 94 direction interferes with the CSPs' right of peaceful enjoyment. In any event, providing the legal requirements of the legislation are complied with the reservations in the Protocol:

(a) No-one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law .....
(b) The preceding provision shall not, however, in any way impair the right of the State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest .....

provide ample protection to the Agencies and the CSPs.

I agree that Article 8 is not engaged in the transfer of data to ***the database*** for the reasons set out in your letter.

The problem which troubles me at the moment is that it seems to me that if Section 21 of Chapter II is engaged in the transfer to the database, then its provisions must be followed and the various requirements of Chapter II complied with. If this is right, and I am happy to be persuaded that it is not, this should not cause any great difficulty, although I accept that it is rather cumbersome when allied to the subsequent retrieval of the data from the database.

Retrieval of information *from the database*
I agree that Article 8 is now engaged and so must meet the requirements of necessity, proportionality, and being in accordance with the law. However clearly that can readily be achieved. I also agree that the appropriate way to achieve this is by the service of a Section 22(3) authorisation. Although it may, as I have said above, appear to be cumbersome and rather strange to go through the same, or at least a similar exercise twice, there is a logic about it, because the first stage is an acquisition of communications data obtained by notice, and the second is a disclosure obtained by an authorisation. I agree with what you say in the second half of paragraph 11 of your letter that, although at first sight it may be awkward to fit the second stage into Section 21(1)(a) it is in fact logical to do so, and is certainly necessary to fulfil the spirit of the legislation.

GCHQ
I have no difficulty with the data obtained and disclosed under a "Section 8(4) authority". However, I think that in relation to the remaining 10% the same problem may arise as that outlined above.

I will, of course, as always, be happy to discuss these issues with you and others if you wish to do so.

Yours sincerely,
Swinton Thomas

Sir Swinton Thomas

[REDACTION]

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

Copied to [REDACTION]
on 5/8/04

copied to DO
16/08/04
[REDACTION]

[REDACTION]

Noted
[REDACTION]
306/04

Home Office

Legal Adviser's Branch

806, 50 Queen Anne's Gate, London SW1H 9AT
Switchboard 0870 0001585 Fax 0171 273 3629 Direct Line [REDACTION]
E-mail [REDACTION]@homeoffice.gsi.gov.uk www.homeoffice.gov.uk

The Rt. Hon. Sir Swinton Thomas
Interception of Communications
Commissioner
C/o Room 1022
50 Queen Anne's Gate
London
SW1h 9AT

Our Ref
Your Ref
Date 22nd June 2004

Dear Sir Swinton

The database

1. Thank you very much for your letter of 8th June. This letter relates to the reservations that you have about the first stage [REDACTION] namely the transfer to the database

2. You say that if section 21 of Chapter II is engaged in the transfer to the database, then its provisions must be followed and the various requirements of Chapter II complied with. Although we agree that Chapter II could be used in relation to the transfer to the database, we do not think that that means it must be used. The purpose of Chapter II is to make lawful the acquisition and disclosure of communications data which would otherwise be unlawful. But if a direction had been made under section 94 of the Telecommunications Act 1984 (the 1984 Act), the acquisition of the [REDACTION] data would already be lawful (to the extent necessary to deal with any Article 1 of Protocol No.1 ECHR issue) and there would therefore be no need to use Chapter II[1]. In our view, the transfer to the database could be made lawful either by the issue of notices under Chapter II or by a direction under section 94 of the 1984 Act.

[1] You question where the requirement for proportionality in section 94 of the 1984 Act comes from. The answer is section 94(2A) which was inserted into the 1984 Act by paragraph 70(4) of Schedule 17 to the Communications Act 2003 (c.21).

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

The only practical difference between the two sets of provisions is that, if Chapter II were used, a new notice would need to be issued every month in accordance with the renewal provisions of section 23, involving a fresh consideration of the necessity and proportionality issues. This would not be the case under section 94. However, if the section 94 route were used, the Security Service would undertake regularly to review the necessity and proportionality of the direction with a view to cancelling it if these tests were no longer met.

3. It seems to us that the issue of whether to use Chapter II or a section 94 direction is essentially a matter of policy/presentation. In favour of using a section 94 direction are the following two factors.

4. Firstly, under section 94, the direction would be given by the Home Secretary. Under Chapter II, the notice could be issued at a fairly low level (in accordance with the Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003/3172)). Even if the notice were in practice issued at a much higher level, it would always be issued by an official rather than a politician (even if its issue were in fact approved by a politician). Arguably, a decision of this significance ought to be taken by a politician who is directly accountable to Parliament, rather than by an official.

5. Secondly, although there is nothing to stop Chapter II being used for transfers of data of the type envisaged by ***the database***, it has not in practice been used in this way to date. If the Security Service could use Chapter II in this way, then in principle so could all the other public authorities that have access to communications data if they could comply with the necessity and proportionality tests. We understand that some communications service providers are concerned that law enforcement authorities might try to set up their own version of ***the database***. Their perception is that, if Chapter II were used for ***the database***, it would make it more likely that law enforcement authorities would attempt to do something similar using their powers under Chapter II.

6. We would be happy to discuss these issues with you if you think that would be helpful.

7. A copy of this letter goes to [REDACTION] (Home Office), [REDACTION] (Security Service) and [REDACTION] (GCHQ).

Yours sincerely,
[REDACTION]

[REDACTION]
Home Office Legal Adviser's Branch

[REDACTION]

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

Interception of Communications Commissioner
The Rt Hon. Sir Swinton Thomas
C/O Room 1022
50 Queen Anne's Gate
London
SW1H 9AT
Telephone: [REDACTION]

[REDACTION]
Home Office Legal Adviser's Branch
Room 806
50 Queen Anne's Gate
London
SW1H 9AT

Date: 6th July 2004

Dear [REDACTION],

Thank you for your letter of the 22nd June. In particular, thank you for drawing my attention to Paragraph 70(4) of Schedule 17 of the Communications Act 2003. One of the problems of working in the outposts of the Empire is that one tends not to be informed of changes in the law, and has to rely on bumping into them by chance- as here!

On the issue of transferring data to the database this raises an interesting but, in the end, perhaps not over-important point. I agree that the provisions of both the Telecommunications Act 1984, and Chapter II of Part I of RIPA 2000, make the acquisition of communications data lawful. The question that arises is whether on the enactment of Chapter II, it became mandatory to follow the procedures set out in Chapter II in all cases of acquisition of data under any enactment, or whether the procedure applied only to data acquired pursuant to RIPA When I wrote to you on the 8th June I was inclined to the former view, but on re-consideration and in the light of your letter, I have revised that view, and can see that there is a strong case for arguing that the procedure should only apply in Chapter II cases. I am also impressed by the considerable and, if possible to be avoided, inconvenience in following the Chapter II procedure in ***the database*** proposals.

In these circumstances, I am content that you should proceed in the way that is suggested. I have assumed that this is in line with the views of the appropriate advisers within the Agencies concerned.

Yours sincerely,
Swinton Thomas

Sir Swinton Thomas

[REDACTION]

[NOTE: REDACTIONS ARE INDICATED AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS]

[REDACTION]

From the Interception of Communications Commissioner:
The Rt. Hon. Sir Swinton Thomas
C/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

[REDACTION]
Home Office
Legal Adviser's Branch
Room 806
50 Queen Anne's Gate
London, SW1H 9AT

July 2004

Dear [REDACTION]

The Database

This letter follows my letter of 6th July 2004.

When I visited the Security Service on 6th July, I was told that there is a suggestion being floated that bulk transfers of communications data might be obtained by Law Enforcement Agencies by means of a RIPA Notice only without the intervention of Section 94 of the Telecommunications Act, 1984.

Needless to say I have no settled view about this at the moment, but I think that I would be concerned about this being done without Ministerial intervention, and if there is any fixed proposal to this effect, I would be grateful if I could be consulted about it.

Yours sincerely,
Swinton Thomas

Swinton Thomas

[REDACTION]

[redacted]

GCHQ
Hubble Road
Cheltenham
GL51 OEX

[redacted]
Title LA2

Tel: 01242 221491 Ext: [redacted]
Brent: 01242 540088
Fax: 01242 709053
GTN: 1366 Ext: [redacted]
E-mail:

Sir Swinton Thomas
Interception Commissioner
Home Office
50 Queen Anne's Gate
London SW1H 9AT

GCHQ Reference: LA2/0534/6/3/19
Your Reference:

Date: 18TH October 2004

Dear Sir Swinton,

COMMUNICATIONS DATA – ACQUISITION AND DISCLOSURE

1. Following your visit to GCHQ in July 2004 and our discussion in London on 14th October 2004, this letter discusses the GCHQ procedures for handling communications data and seeks to confirm your view of their fitness for purpose.

2. Communications data is an increasingly important tool in GCHQ, especially in the fight against global terrorism and serious crime. About 250 staff are involved in its analysis and about 40% of End Product Reports are derived directly or indirectly from the analysis of communications data.

3. The communications data is stored in GCHQ databases. Huge volumes of data are acquired (about 40 million bits of data per day). There are two databases at GCHQ holding communications data acquired in 'bulk' – known as [redacted] Ideally all the material would be held on a single database, but the data is configured differently by the CSPs and resource constraints in GCHQ have meant that it is not feasible, at this point in time, to re-configure and hold all the data in a single database.

4. The [redacted] database holds computer-to-computer [redacted] communications data all of which originates from sources authorised by the RIPA 8(4) warrants. The [redacted] database contains communications data relating to telephony. About 90% of the data stored on the [redacted] database originates from sources authorised by the RIPA 8(4) external warrants and about 10% from section 94 directions.

5. The data held on the [redacted] database is not separated by reference to the legal instrument under which it was obtained for the following reasons:

- To date, GCHQ has relied on legal advice previously tendered (coupled with the requirements of the process described at para 9 below) that such separation, in legal terms, is unnecessary;

[redacted]

[redacted]

- In the interests of security and commercial confidentiality, GCHQ prefers to keep all the telephony material together in one database (rather than separate it) to disguise its source, as the origins of some of the material is extremely sensitive;

- The combining of all telephony-related communications data in a single database makes analysis of such data much quicker and more reliable; this is particularly so with pattern analysis which relies on exploiting large quantities of data.

6. The origin of the material is not consistently flagged, so an analyst cannot tell whether a particular bit of communications data originates from a warrant or a direction.

7. Communications data is currently retained for [redacted].

8. The mechanics of facilitating access by GCHQ staff to communications data obtained by GCHQ in reliance on either its RIPA section 8(4) warrant or the section 94 directions issued to it are the same and were demonstrated to you on your recent visit to Cheltenham but, for ease of reference, are reproduced below:

9. The databases are searchable. To access the communications data databases the analyst is required to log on and an audit log is automatically created. The log records who accessed the database, the date, time on and time off. It also records the JIC requirement underpinning the request (national security, EWB and/or serious crime), a [redacted] number (which is a GCHQ system providing a higher level of granularity taken from the JIC R&P) and a specific justification. We consider that the provision of this information is sufficient to protect an individual's Article 8 rights (in that information may not be accessed unless it is for a proper purpose), and to ensure that GCHQ can respond appropriately should an individual complain to the Investigatory Powers Tribunal.

Legal analysis:

10. Communications data may be acquired under a number of different legal instruments:

- Section 8(4), or section 8(1) RIPA warrants. Section 5(6)(b) of RIPA provides that an interception warrant may authorise the obtaining of related communications data;

- Section 94 directions under the Telecommunications Act 1984 (as amended by the Communications Act 2003);

- Notices or authorisations given under sections 21 to 25 RIPA (Part 1, Chapter II).

[redacted]

(It is also the case that occasionally, e.g. immediately post 9/11, communications service providers voluntarily provide communications data to GCHQ for analysis.)

11. It has always been GCHQ's position that each of the three methods of acquisition listed above is equally valid in law and GCHQ presently relies upon all three types of legal instrument when acquiring communications data. This being so, we welcome the views that you express in your letter to [redacted] dated 6 July 2004.

12. We would contend (and from what you have said in your correspondence with [redacted] we believe that you concur) that the transfer of data to our databases pursuant to section 94 directions is in accordance with the law provided that the Secretary for State responsible for signing such directions is able to properly consider necessity and proportionality issues.

13. Turning now to the legal position relating to accessing the data obtained under the directions. GCHQ does not presently adopt the RIPA Part I Chapter II authorisation process to access data on its [redacted] databases. Hitherto, we have taken the view that s.94 (when coupled with the access procedures described in para 9 above) has operated in such a way so as to make the accessing of any data held on the database in accordance with the law. We are aware that you have previously expressed some reservations about this interpretation of the effect of s.94, and this brings us to the crux of this letter. Whilst we accept that it is *arguable* that s.94 is insufficiently precise so as to make the access of any data obtained pursuant to any directions issued under that section not in accordance with the law, GCHQ would favour the interpretation that it presently relies on, i.e. that s.94 operates to the effect that access to the data obtained under any direction is in accordance with the law (particularly when taken in conjunction with our current access procedures).

14. There are very real practical difficulties in GCHQ being required to obtain a RIPA Part I Chapter II authorisation in respect of accessing any data that it had obtained in reliance on section 94 directions. This is because it is not possible to identify which of the small percentage of the total communications data held on the [redacted] database has been acquired under section 94 directions. This being the case, if an authorisation was required to access any data held on [redacted] that was obtained pursuant to s.94 directions it would be necessary to obtain an authorisation in each and every case that communications data was accessed on this database – even if the data had been obtained in reliance on a RIPA section 8(4) warrant. At present, our staff make about 2,000 queries of the [redacted] database each week. In a proportion of these cases, the analyst will not have any information about the identity of the entity and may be undertaking target profiling work looking for calling patterns that are associated with known terrorist behaviour rather than a particular entity.

[redacted]

15. However, taking into account the fact that the Secretary of State would have made a judgement as to necessity and proportionality when issuing the directions authorising the acquisition of the data, we believe that the requirements that have to be fulfilled by GCHQ staff when communications data is accessed by them on the [redacted] database are such that the spirit of RIPA (insofar as the tests of justification, necessity and proportionality are met) is fully adhered to. In addition, an unintended consequence of requiring the RIPA process would be to create an inconsistency between the authorisation regime for communications data and that required for intercept selected under a RIPA 8(4) warrant. A higher level of protection would be provided for communications data than for such selected material. This seems odd given that taking action on communications data is agreed to be intrinsically less intrusive into privacy.

16. Given the contents of your 6 July letter to [redacted] and the comments you made when you last visited Cheltenham (when, if we understood you correctly, you seemed to suggest that adherence to the spirit of the legislation was an important factor when considering whether the necessary legal requirements for accessing the data held on the [redacted] database had been met), and those you made when we met in London on the 14th, are you content with the processes currently adopted by GCHQ for its staff to access communications data held on its [redacted] database and that such access is in accordance with the law? If you are not content with our current interpretation of s.94 and our practices/processes, then we would welcome the opportunity to discuss this with you further.

Yours ever,

[redacted]

pp [redacted]
Legal Adviser

CC: [redacted]

[redacted]

[redacted]

From the Interception of Communications Commissioner:
The Rt. Hon. Sir Swinton Thomas
c/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

[redacted]
Legal Adviser LA2
GCHQ
Hubble Road
Cheltenham
GL51 0EX

Your ref: LA2/0534/6/3/19

Our ref: IPS/04 1/1/1

Date: 17 November 2004

Dear [redacted]

COMMUNICATIONS DATA – ACQUISITION AND DISCLOSURE

Thank you for your letter of 18th October. I do not think that the problem of accessing communications data pursuant to a Section 94 direction is altogether easy or straightforward, and I have given it considerable thought.

When the Secretary of State makes a direction under Section 94(2) of the Telecommunications Act 1984 he must be satisfied that the requirements of necessity and proportionality are satisfied in relation to the acquisition of the data. When the data is accessed then, as is recognised, an individual's Article 8 rights are engaged. Whilst it is properly arguable that the Secretary of State impliedly authorises the accessing of the data when he gives the Section 94 direction, it would be very difficult to argue that he has considered the issues of necessity and proportionality in relation to the particular individual whose data is being retrieved. Thus, GCHQ must be able to show that the individual's rights are properly protected in that the data is being retrieved for a proper purpose and is proportionate and that the decision to retrieve it has been taken at an appropriate level. You tell me that these requirements are covered by the JIC requirement underpinning the request coupled with the record kept of the nature of the requirement in relation to each retrieval. I note that GCHQ takes the view that these safeguards would ensure that they could satisfy the Investigatory Powers Tribunal in the event of a complaint.

I have, therefore, reached the conclusion, not without some difficulty, that the present system for retrieval of data pursuant to a Section 94 direction is lawful. As you say, adhering to the spirit of the legislation is an important consideration, and I am also impressed by the fact that when armed with a Section 94 direction which clearly envisages both acquisition and retrieval, the requirement of a RIPA Section 22(3) authorisation would cause real difficulties which could not have been

[redacted]

[redacted]

envisaged by Parliament when RIPA was enacted. I am, therefore, content that you should proceed as proposed.

Yours sincerely,

Swinton Thomas.

Sir Swinton Thomas

[redacted]

[redacted]

GCHQ
Hubble Road
Cheltenham
GL51 0EX

[redacted]
Title LA2

Tel: 01242 221491 Ext: [redacted]
Brent: 01242 540088
Fax: 01242 709053
GTN: 1366 Ext: [redacted]
E-mail:

The Rt Hon Sir Swinton Thomas
Interception Commissioner
c/o Room 1022
50 Queen Anne's Gate
London SW1H 9AT

GCHQ Reference: LA2/0655/6/3/19
Your Reference: IPS/04 1/1/1

Date: 2nd December 2004

Dear Sir Swinton,

Re: Communications Data – Acquisition and Disclosure

Thank you for your letter of 17th November 2004. GCHQ very much welcomes the conclusion that you express in this letter.

For the sake of completeness I thought it appropriate to comment on part of your letter. You say,

"Whilst it is properly arguable that the Secretary of State impliedly authorises the accessing of data when he gives the Section 94 direction, it would be very difficult to argue that he has considered the issues of necessity and proportionality in relation to the particular individual where data is being retrieved".

Of course, whilst no particular individual whose data may be accessed is identified either in the Section 94 directions themselves or in the accompanying submission, the submission does itself contain a clear statement as to the manner in which any data obtained under the directions will be handled. The relevant extract from one of the submissions is as follows,

"Within GCHQ data will be handled in accordance with section 4 of the Intelligence Services Act 1994, and with additional safeguards designed to comply with the Human Rights Act 1998. These safeguards were included in the GCHQ Compliance Documentation ...."

This undertaking, combined with the limited purposes for which GCHQ can gather and use material and the adherence to the JIC requirements when requesting the data, we believe, allows GCHQ to demonstrate that an individuals rights are being properly protected. In addition, this extract, when coupled with the remainder of the submission, allows the Secretary of State to

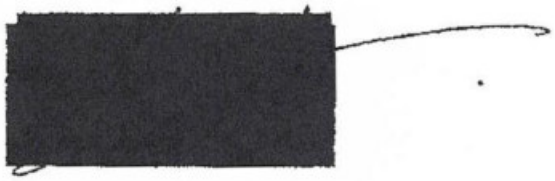
[redacted]

[redacted]

satisfy himself that GCHQ will obtain and subsequently handle the data in a justified and proportionate manner, notwithstanding that the individuals whose data may be accessed are not identified either in the directions themselves or in the accompanying submission.

GCHQ is not looking to re-open this issue, but I just thought it worthwhile to state our view as clearly as possible.

Yours sincerely,



[redacted]
Legal Adviser

Home Office

2 Marsham Street, London SW1P 4DF
www.homeoffice.gov.uk

The Director General
The Security Service

March 2015

Acquisition of Communications Data: operationally independent authorisation

Thank you for your letter of 19 March 2015 and the useful conversation we had on 26 March 2015.

I can confirm that I am content for your current single point of contact (SPoC) system to continue, though I am aware that this is an area that David Anderson, QC, is considering as part of his Investigatory Powers Review.

However, it is important that the operational independence of the Designated Person (DP) is strengthened across public authorities, to ensure a robust position regarding legal challenges to the UK's current model of communications data acquisition. While I understand the unique position of your service, I believe that the provisions of the new Acquisition and Disclosure of Communications Data Code of Practice regarding DPs should certainly apply to MI5 with respect to applications for communications data of those known to have professional duties of privilege or confidentiality, such as lawyers and journalists. I would like this change to be in place no later than 20 April 2015.

Of course, in urgent situations even for such cases, the code allows for authorisation by someone not independent of the operation.

In the case of the applications where the subject of interest is not a member of a sensitive profession, I am content that MI5 continue for the time being to operate under the national security exemption in the code regarding operational independence, provided the Interception of Communications Commissioner is informed as set out in the code of practice. The Commissioner may choose to publish details of this exemption in his annual report. This exemption must be kept under review, and I would like you to give careful consideration as to how you might be able to achieve operational independence of authorisation and provide a detailed breakdown of the costs and issues that would be involved. This should feed into your engagement in the work following up the Anderson review and the development of legislation to replace DRIPA.

These requirements are not a reflection of the sterling work that members of the service carry out day in day out to protect this country, nor the use by MI5 of communications data. Rather, they stem from the need to ensure that those very people you are protecting are reassured that the powers vested in your service, and other public authorities, are carried out with all due deliberation and that operational requirements do not trump considerations of necessity and proportionality

I am copying this letter to the Interception of Communications Commissioner.

The Rt Hon Theresa May MP

REDACTION

Home Office

2 Marsham Street London SW1P 4DF
www.homeoffice.gov.uk

Andrew Parker
Director General
The Security Service

June 2015

Acquisition of Communications Data: operationally independent authorisation

Thank you for your letter of 21 April 2015, regarding the operational independence of the designated person when authorising requests for communications data relating to those in sensitive professions, such as journalists and lawyers

I understand that MI5 has now managed to implement operational independence of designated person for communications data requests of those in sensitive professions and I welcome this

In my earlier letter, I indicated that, while I was happy for the time being for no corresponding change to be made where the subject of interest is not a member of a sensitive profession (subject to the Interception of Communications Commissioner), I wanted you to give consideration as to how you would achieve operational independence of authorisation in such cases. You will be aware that David Anderson has recommended operational independence in all cases so this work takes on a greater imperative and I would be grateful for an update on progress, as you suggested

The Rt Hon Theresa May MP

Cover Note re documents provided in response to Request 7 (namely IOCCO inspection reports for period 2011-2015)

NOTE:

All of the redactions to these documents, save for the redaction to the December 2015 report at page 19, 3rd column, 2nd row, are redactions made on the grounds of relevance.

[redacted]

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

Inspections under Chapter II of Part I of the Regulation of Investigatory Powers Act (RIPA) by the Interception of Communications Commissioner's Office (IOCCO)

Name of Public Authority	The Security Service (MI5)
Date/s of inspection	15th – 17th December 2014
Inspector/s	[redacted]

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner, Sir Anthony May. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objectives of the inspection were to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

Staffing:

Senior Responsible Officer (SRO)	[redacted]
SPoC Managers	[redacted]
Accredited Officers (AOs) (Indicate if full time, part time)	[redacted]
Other staff met during the inspection	[redacted]

[redacted]

[redacted]		[redacted]	
[redacted]	[redacted]		
DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved.	Partly	The DPs have an awareness of the investigations for which they approve communications data requests and to date this has been	[redacted]

although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons. Where a DP is directly involved in the investigation or operation their involvement and their justification for undertaking the role of DP must be explicit in their recorded considerations. (Para 3.11 CoP). A revised draft CoP was released for public consultation in December 2014 by the Home Office. The draft amends and strengthens this area of the process and requires DPs to be independent of the investigation. These changes stem from the recent European Court of Justice judgement which declared the Data Retention Directive invalid. The proposed new requirements are contained in Para's 3.11 to 3.15 of the revised consultation CoP .	[redacted]	justified on security grounds. There is no evidence of DPs complying with Para 3.11 of the CoP (indeed as mentioned in a preceding baseline many are not recording considerations at all when approving applications). The inspectors outlined the anticipated changes to the CoP (see adjacent baseline) which are likely to strengthen this area of the process and require DPs to be independent of the investigation. **It is recommended that MI5 reviews this area of the process and implements measures, in anticipation of the revised CoP coming into force, to ensure compliance (See Para's 3.11 to 3.15 of the revised CoP).**	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

See http://www.gov.uk/government/consultations/communications-data-codes-of-practice-acquisition-disclosure-and-retention

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

Inspections under Chapter 2 of Part I of the Regulation of Investigatory Powers Act (RIPA) by the Interception of Communications Commissioner's Office (IOCCO)

Name of Public Authority	The Security Service (MI5)
Date/s of Inspection	7th – 10th December 2015
Inspector/s	[redacted]

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Chapter 2 of Part I of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objective of the inspection is to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Chapter 2 of Part I of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

[redacted]

		[redacted]	
DPs must be independent from operations and investigations when granting authorisations or giving notices related to those operations (Paragraph 3.12 CoP).	No	MI5 have implemented a process whereby independent DPs consider applications that relate to individuals in professions or occupations with duties of confidence or privilege attached. All other applications (i.e. the majority) are forwarded to the applicant's line manager for approval. The line managers are not independent from the operations or investigations for which they are granting authorisations or giving notices. Our previous inspection recommended that the Security Service should review the independence of its DPs. This was in anticipation of changes being made to the CoP (enhanced safeguards for the independence of DPs). The CoP was duly amended to take account of the Digital Rights Ireland European Court of Justice (ECJ) ruling and the revised CoP came into force on 25th March 2015. One of the exceptions for independence in the CoP (Para 3.13) refers to ongoing operations or investigations immediately impacting on national security issues where the public authority is not able to call upon a DP who is independent. We do not consider that this exception applies to the routine applications submitted by the Security Service as in these cases there is no immediacy and the public authority has enough DPs of the prescribed ranks to be able to call upon DPs who are independent. [redacted]% of the communications data requests submitted by the Security Service in the inspection period were graded as 3 (the lowest priority level) in the National Priority Grading System (NPGS) and are therefore regarded as routine. The IOCCO inspectors were made aware of correspondence between the DG and the Home Secretary dated 19th March, 27th March, 21st April and 3rd June 2015.	

		In the 27th March letter the Home Secretary stated that she was "content that MI5 continue for the time being to operate under the national security exemption in the Code regarding operational independence provided the Interception of Communications Commissioner is informed as set out in the code of practice." The Home Secretary asked MI5 to keep the exemption under review and to give careful consideration as to how they might be able to achieve operational independence of authorisation (and to provide a detailed breakdown of the costs and issues that would be involved). MI5 responded on 21st April to confirm they had implemented measures to ensure independence for individuals in professions or occupations with duties of confidence or privilege. The Home Secretary emphasised in her response dated 3rd June that achieving operational independence in all other cases was imperative. We regard the recommendation relating to the independence of DPs that was made during the last inspection to be outstanding, and that the recommendation has become even more critical since the changes to the CoP in March 2015. **The Security Service must devise a strategy and implement procedures to ensure that DPs are independent from operations and investigations when granting authorisations or giving notices related to those operations in order to comply with Paragraph 3.12 of the CoP.**	
[redacted]	**No**	[redacted]	

[redacted]

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

Inspections under Chapter II of Part I of the Regulation of Investigatory Powers Act (RIPA) by the Interception of Communications Commissioner's Office (IOCCO)

Name of Public Authority	The Security Service (MI5)
Date/s of Inspection	25 – 27 November 2013
Inspector/s	Joanna Cavan and [redacted]

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner, Sir Paul Kennedy. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objectives of the inspection were to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

Staffing:

Senior Responsible Officer (SRO)	[redacted]
SPoC Managers	[redacted]
Accredited Officers (AOs) (indicate if full time, part time)	[redacted]
Other staff met during the inspection	[redacted]

[redacted]

[redacted]		
[redacted]		
DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons. Where a DP is directly involved in the investigation or operation their involvement and their justification for undertaking the role of DP must be explicit in their recorded considerations. (Para 3.11 CoP)	Yes	For security reasons the DPs generally have an awareness of the investigations for which they approve communications data requests
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		

[redacted]

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

Inspections under Chapter II of Part I of the Regulation of Investigatory Powers Act (RIPA) by the Interception of Communications Commissioner's Office (IOCCO)

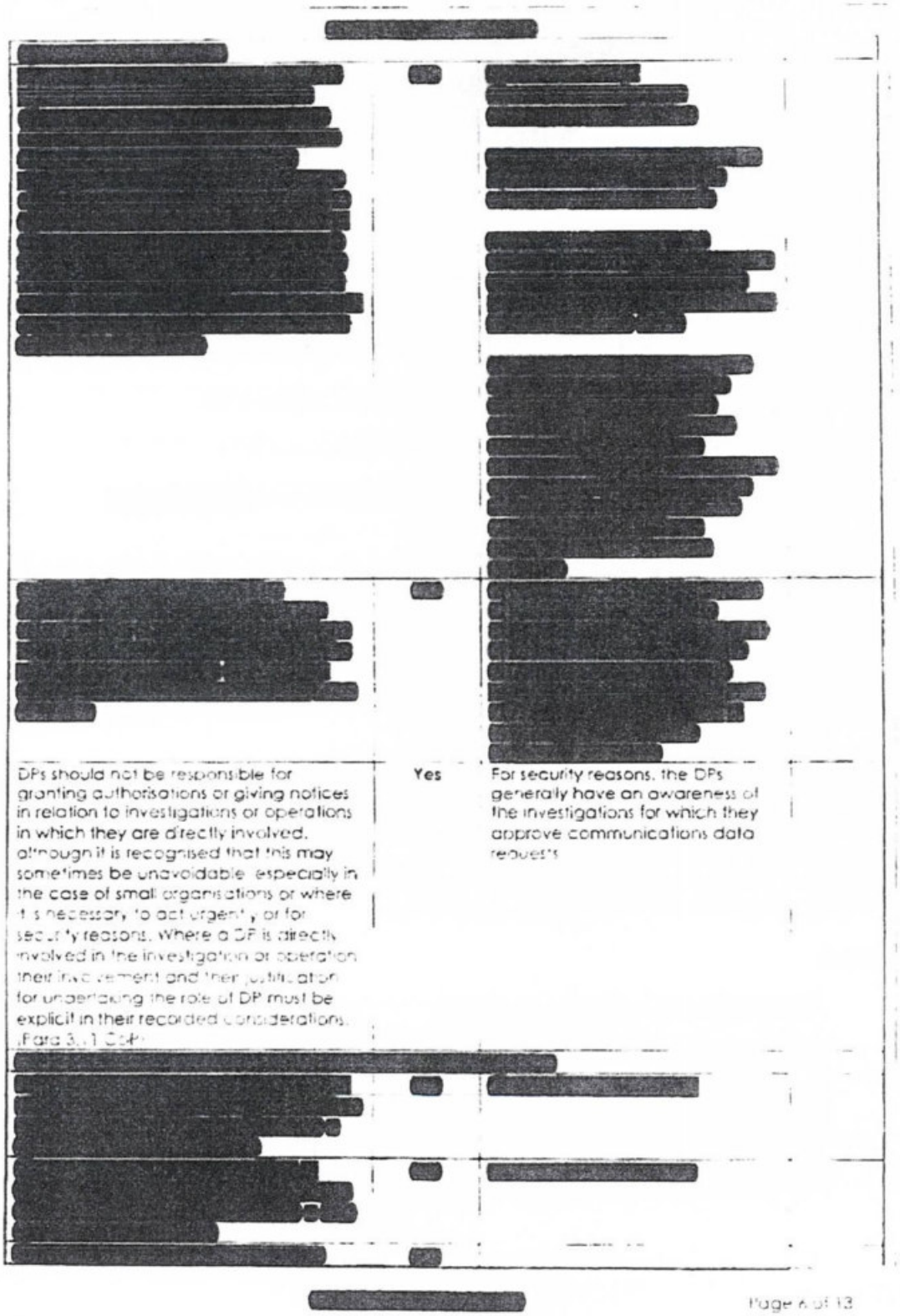
Name of Public Authority	The Security Service (MI5)
Date/s of Inspection	19 - 21 December 2012
Inspector/s	Joanna Cavan and [redacted]

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner, Sir Paul Kennedy. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objectives of the inspection were to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

Staffing:

Senior Responsible Officer (SRO)	[redacted]
SPoC Manager	[redacted]
Accredited Officers (AOs) (indicate if full time, part time)	[redacted]
Other staff met during the inspection	[redacted]



DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons. Where a DP is directly involved in the investigation or operation their involvement and their justification for undertaking the role of DP must be explicit in their recorded considerations. (Para 3.17 COP)	Yes	For security reasons, the DPs generally have an awareness of the investigations for which they approve communications data requests

[redacted]

INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE

Inspections under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA) by the Interception of Communications Commissioner's Office (IOCCO)

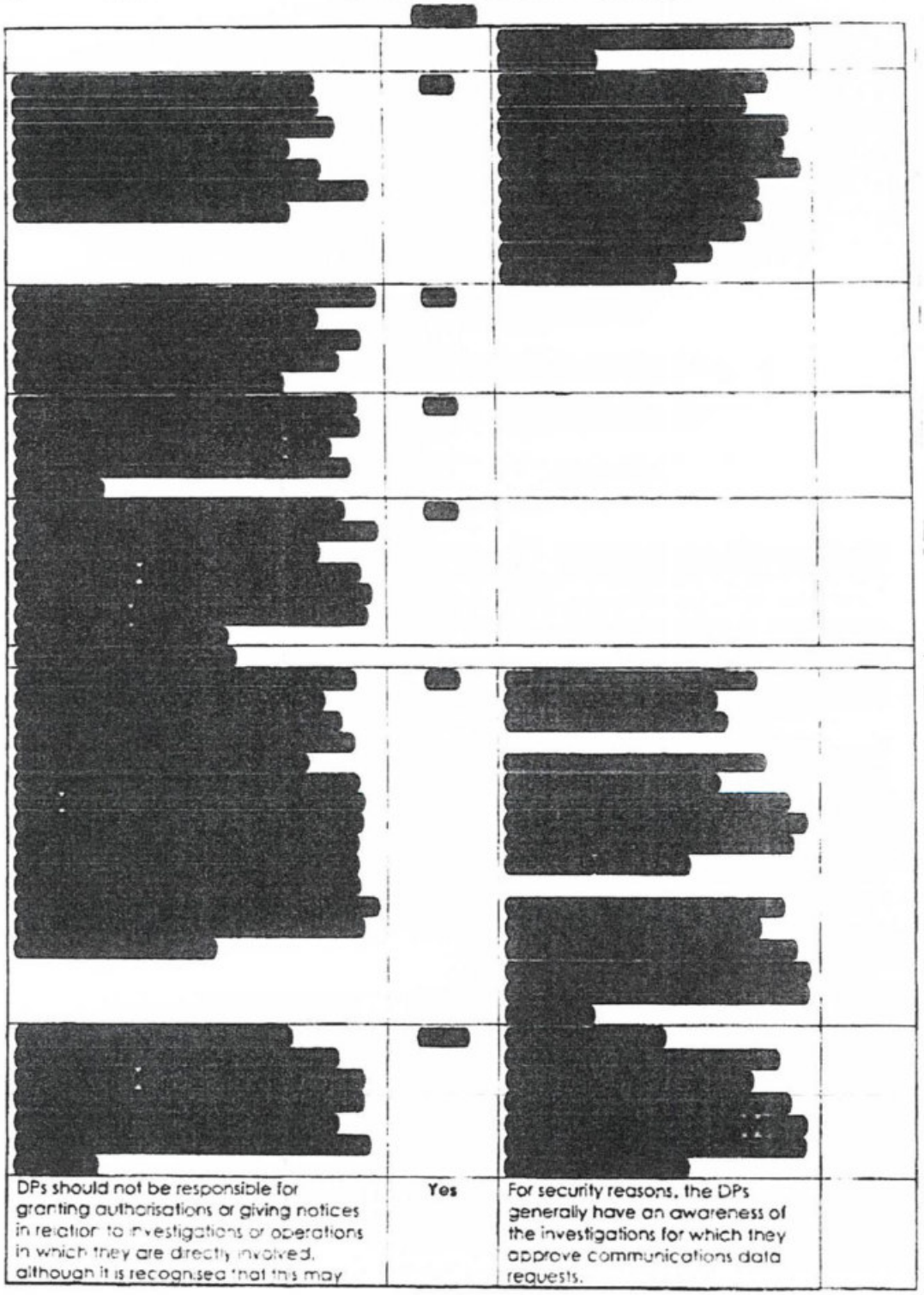
Name of Public Authority	The Security Service (MI5)
Date/s of Inspection	28 – 30 November 2011
Inspector/s	Joanna Cavan and [redacted]

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner, Sir Paul Kennedy. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objectives of the inspection were to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

[redacted]

[redacted]



DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may	Yes	For security reasons, the DPs generally have an awareness of the investigations for which they approve communications data requests.

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE

Andrew Parker

Director General

Rt Hon Theresa May MP

Home Secretary

19 March 2015

[Dear Home Secretary]

INDEPENDENT AUTHORISATION OF COMMUNICATIONS DATA

I understand that there is continuing discussion about making changes to our current internal processes for authorisation of access to communications data. [REDACTION] met with James Brokenshire last week and I wanted to follow this up by putting my concerns in writing.

2. We fully accept that we will need to look carefully at how the authorisations regime operates in a number of areas, including communications data, when David Anderson reports in a few weeks' time. Indeed we welcome the opportunity to strengthen the legislative framework and make it more transparent through the planned legislation in the next Parliament. However, we have been at pains to ensure that these issues are considered in the round, looking at the relative levels of intrusion and safeguards that accompany each capability, and the overall impact on our business of any changes

3. My chief concern is that apparently small changes made to the way we do our business, and particularly to how we authorise and oversee it, can - if they are not considered in the round and managed carefully - cause significant disruption, reduce our effectiveness, and introduce inconsistencies that will have the opposite effect to what is intended.

4 The current suggestion is that we should reorganise our internal structures to ensure that those signing off requests for access to CD (of which, as you know, there are ***more than 100,000*** a year) are more independent from the investigation Implementing this change would be a significant step: it would add additional bureaucracy to investigators' jobs, and would increase the processing time for requests because those taking the decisions would not be familiar with the relevant investigative context. We assess that as a result there would at least be some reduction in the timely progression of both leads and investigations at a time where, as you are aware, we are working hard to increase our assurance levels against an increasingly complex and challenging threat picture.

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE

5 We feel that there are significant risks for MI5 (and for the coherence of HMG's approach to the Anderson and ISC reviews more generally) if we take a position on this issue in isolation now, without considering the broader picture or fully understanding the operational impacts This is particularly so when these arrangements may well need to be changed again or reversed in a matter of months. Furthermore, there does not appear to be a pressing litigation or reputational requirement to commit to make these changes now and we can therefore see no obvious gain in doing so.

6. I would be happy to discuss this issue further if that would be helpful.

7. Copies of this letter to go to James Brokenshire, Charles Farr and Paul Lincoln.

[signed]

Andrew Parker

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE

Andrew Parker
Director General

Rt Hon Theresa May MP
Home Secretary

21 April 2015

[Dear Home Secretary]

INDEPENDENT AUTHORISATION OF COMMUNICATIONS DATA: SENSITIVE PROFESSIONS

Your letter of 27 March asked us to strengthen the independence of authorisation for communications data (CD) applications relating to individuals known to have professional duties of confidence or privilege. You are aware that doing so requires a shift in our business model and adaptations to IT systems and for this reason we are taking a phased approach to implementation. We are making good progress, but will not hit your deadline.

2. I can confirm that yesterday we circulated official guidance to investigative sections stipulating that all CD applications for individuals **known** to fall within the category of a sensitive profession must now be authorised by a Group Leader independent from the responsible investigative team, but within the same business area. This is being implemented with immediate effect and will also be incorporated in our training of investigators. [REDACTION]. We are also working rapidly towards a technical solution to incorporate these changes into our IT systems, which will provide further assurance and also enable us to capture the necessary statistics on requests of this type for the Interception Commissioner. We expect this to be rolled out by the end of May.

3. We are mindful of the importance of ensuring that these principles also apply to those applications where we **retrospectively** establish that the subject is a member of a sensitive profession. [REDACTION] We are developing thinking on how best to approach this and hope to have additional guidance for investigators by the end of May In the interim, investigators have been advised to highlight any such cases to our legal advisers for immediate review We will, of course, engage the Interception Commissioner on these new arrangements to ensure he is content.

[REDACTION]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE

4. I hope this progress is reassuring We will provide a further update at the end of May. I would, of course, be happy to discuss further in the interim should you wish.

5. I am copying this letter to the Interception of Communications Commissioner.

[signed]

Andrew Parker

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE

Andrew Parker Director General

Rt Hon Theresa May MP

Home Secretary 30 June 2015

[Dear Home Secretary]

INDEPENDENT AUTHORISATION FOR CD REQUESTS

Thank you for your letter of 3 June relating to operational independence for Communications Data requests.

2. As you are aware, we have now implemented a system for independent authorisation of CD requests for members of sensitive professions. Effecting this change required both [REDACTION] system and business process work and has an opportunity cost on the time of senior investigative managers who will operate as independents. We cannot yet estimate the exact impact, but our instinct is that the number of requests will be small and manageable. We will be monitoring this closely. We have also looked more closely at how to minimise the risk that we discover a CD check has been made for a person in a sensitive profession after the event. We think this is best handled by [REDACTION]. I have commissioned some work and will provide an update in early September.

3. Implementing operationally independent authorisation for all of our CD requests would be a substantially greater ask. We estimate that the additional burden would necessitate a minimum of [REDACTION] additional people allocated to the task.

4. [REDACTION]. The DP cadre in MI5 are key operational managers with a range of functions. Given current operational pressures, re-allocating their time for independent authorisation work would have a significant impact [REDACTION]. Taken together with the additional system and process changes which would be necessary and the uncertainty of the shape of the Investigatory Powers Act, we think there are significant risks from implementing independence for all CD authorisations at this point.

5. Given the amount of business change we are likely to need to implement as a result of new legislation, it would be my preference to implement further changes as part of that wider business change programme.

6. [REDACTION - LPP]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE

[REDACTION - LPP]

[signed]

Andrew Parker

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE

Andrew Parker
Director General

Rt Hon Theresa May MP
Home Secretary

18 December 2015

[Dear Home Secretary]

INDEPENDENT AUTHORISATION OF ACCESS TO COMUNICATIONS DATA

I wanted to return to the issue of MI5's position in relation to independent authorisation of access to Communications Data (CD) in order to ensure we are clear on how the requirements in the Investigatory Powers Bill will apply to MI5 in the future.

When we discussed this issue previously, I committed to implementing independent authorisation - within MI5 - for CD requests relating to members of sensitive professions, and as you know we have now done that. I recognise that there may be further debate in parliament in this area over the coming months, but I continue to have strong reservations about agreeing now to more widespread changes for targeted CD requests, either by introducing independent authorisation within MI5 [REDACTION].

2. As we have discussed, MI5's use of CD is significantly different from the use of CD by law enforcement, and the wider range of authorities who are able to access it. As you know, in MI5 investigators use CD in a very high proportion of the cases they work on. As with all our work, these cases will have already passed a national security threshold, including through the rigorous processes of leads triage and prioritisation that we conduct on a day-to-day basis. Consideration of necessity and proportionality is already at the heart of all of that decision making.

3. The context is different from the use of CD by law enforcement and others, who deal with a far wider range of cases, in most of which, CD is not a relevant and proportionate tool to use. This is of course not to say that MI5 investigators should avoid having to make proper, and recorded consideration of the necessity and proportionality of their access to this data, but the fact that these are highly trained, security cleared officers, working on the most serious of national security threats must be relevant in calibrating the additional safeguards required to ensure proper use of the data. I set out these arguments in the recent ISC evidence session on the Bill.

4. Another important pragmatic issue is that of volume As you know, we submitted a total of ***more than 100,000*** individual requests for CD in 2014, through 40,000 applications. If we were to switch to an arrangement where each of these has to be authorised by someone within MI5 who is

[REDACTION]

SECURITYSERVICE

unfamiliar with the case, and who has to be sufficiently briefed to be able to make a considered decision, we would be adding a non-trivial amount of administrative burden into our system, at the same time as we work to increase assurance levels against a very high tempo of threat, and as we seek to develop more streamlined ways of working The DP cadre in MI5 are key operational managers with a range of functions, and reallocating their time for independent authorisation would undoubtedly have an impact on this finite resource, diverting effort away from pursuing frontline investigations, without any clear benefit in terms of additional legal protection or improvements in the quality of decision making.

6. [REDACTION]

7. Your officials have asked us to consider whether there are certain CD cases to which we could consider applying independent authorisation. We have considered this, and there is no obvious logic we could apply, beyond the changes we have already made in relation to sensitive professions. Our main priority would be to protect security around the most sensitive cases. [REDACTION]. Widening access to these would, in my opinion, introduce significant operational risk by extending the knowledge of our most sensitive operations beyond those with a legitimate requirement to know the details. If on the other hand, we were to restrict independent authorisation to our [REDACTION] business, there would need to be several layers of guidance for the circumstances under which independent authorisation was required, with immediate threats to life for instance being exempt for example Given the complexity, potential for delays and compliance risk this would bring, my view remains that the national security exemption in the IP Bill should apply to all of MI5 requests for CD other than in relation to sensitive professions.

8. [REDACTION]

9. [REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

[REDACTION]

10. I fully understand that this issue may come under scrutiny during the passage of the IP Bill, and would of course be happy to discuss this further at any point. Currently however, it does not seem that the benefits of any concessions in this area outweigh the impact this would have on our business.

[signed]

Andrew Parker

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

[REDACTION]
Deputy Director -Interception and Digital Intelligence

Jo Cavan

09 March 2015

Head of IOCCO

DearJo

INSPECTION BY THE INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE (IOCCO) UNDER CHAPTER II OF PART I OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA)- SECURITY SERVICE RESPONSE TO RECOMMENDATIONS

I write further to your report of 9th February. In your report you asked for feedback on progress made against your recommendations.

[REDACTION]

2. [REDACTION]
3. [REDACTION]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

[REDACTION]

SECURITYSERVICE

4. [REDACTION]
5. [REDACTION]

Recommendation 3: Role of the DP

6. Your inspectors observed that the DP's within the Service are not independent of investigations and recommended that MI5 review this area of the process and implement measures, in anticipation of the revised CoP coming into force.

7. The Service considers its current process - which has been agreed by your office and the Home Office for several years- to be in accordance with the revised CoP, which allows for public authorities which have ongoing operations or investigations immediately impacting on national security issues to not need to call upon a designated person who is independent from their operations and investigations (para 3.13 of the revised CoP). We would also be content for you to state that the Service's DPs are not independent from operations and investigations in your report. We anticipate that issues of authorisation and oversight will be considered as part of future legislative proposals being put forward in the next parliament.

[REDACTION]

8. [REDACTION]

9. [REDACTION]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

SECURITYSERVICE

[REDACTION]

10. [REDACTION]
11. [REDACTION]

[REDACTION]

12. [REDACTION]
13. [REDACTION]

14. Should you have any further questions about this response, please do not hesitate to contact me.

[REDACTION]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

INTERCEPTION OF COMMUNICATION COMMISSIONER'S OFFICE

[REDACTION]
Deputy Director
Interception and Digital Intelligence

7th May 2015

Dear
[REDACTION]

Thank you for your letter dated 9th March 2015 returning the schedule of recommendations that was issued following the inspection of the MI5 Single Point of Contact (SPoC) in December 2015.

Rec 1 - [REDACTION]

Rec 2- [REDACTION]

Rec 3 – I note that MI5 considers its current process to be in accordance with Paragraph 3.13 of the revised Code of Practice (CoP) which requires:

"'in circumstances where a public authority is not able to call upon the services of a designated person who is independent from the investigation or operation, the Senior Responsible Officer must inform the Interception of Communications Commissioner of the circumstances and reasons." It further states that these circumstances may include *"'public authorities which have ongoing operations or investigations immediately impacting on national security issues and are therefore not able to call upon a designated person who is independent from their operations and investigations." [emphasis added].*

We would be grateful therefore to receive details of the circumstances and reasons as to why you are not able to call upon independent designated persons.

[REDACTION]
Interception of Communications Commissioner's Office (IOCCO)
Telephone: 020 7035 1200 Email: Info@iocco.gsi.gov.uk
our Website www.iocco-uk.info Follow us on Twitter @iocco_oversight

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

For your information we have been copied into a letter from the Home Secretary to Andrew Parker dated 2nd March and the response from Andrew Parker dated 21st April. However we have not had sight of Andrew Parker's original letter of 19th March which the Home Secretary refers to in her letter of 27th March. It might be that this letter contains the necessary information.

Rec 4 - [REDACTION]

Rec 5 - [REDACTION]

Rec 6 – Thank you for outlining that you are currently refreshing your guidance on errors. I note that this work is expected to be completed by the end of June.

I look forward to receiving a further update on the progress made against the recommendations by 11th May 2015.

Yours sincerely,

Joanna Cavan
Head of IOCCO

[REDACTION]

SECURITYSERVICE

Our ref: [REDACTION]

Your ref:

Jo Cavan
IOCCO

Date: 27 May 2015

Dear Jo,

Thank you for your letter of 7 May in response to mine of 9 March. We discussed some of the issues raised in our meeting on 20 May.

2. *Recommendation 2.* [REDACTION]

3. *Recommendation 3.* Andrew Parker's letter to the Home Secretary of 19 March is attached. As you can see, we are open to changes in our approach to Independent DPs, but we are anxious to do this in the context of the broader Anderson recommendations. Given the centrality of our cadre of DPs to the broad range of our CT investigations we are wary of introducing business change on CD authorisation processes now which will demand further business change in a year or so. [REDACTION]. We need also to think more broadly about what the overall impact of independent DPs will be and articulate the impact on assurance levels. Put simply, we think that the complexity of [REDACTION] investigations means that an independent with no knowledge of a case will need to spend at least [REDACTION] per application on understanding what the case is about before they can properly consider the issues that a DP needs to turn his/her mind to. For a cadre of less than [REDACTION] staff with a significant range of other investigative duties this will be a big impact on their working day, given the volume of CD requests we make. We are therefore working towards a different approach to independents and are looking
at options now: but to minimise the impact on assurance levels we think we can only take this step in the context of the Anderson recommendations. We will brief you on progress at the next Commissioner inspection.

4. *Recommendation 4.* [REDACTION]

5. *Recommendation 5.* [REDACTION]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

Yours Sincerely

[REDACTION]

[REDACTION]

[redacted]

[redacted]

Government Communications Headquarters

Room No [redacted]
Priors Road Cheltenham GL52 5AJ
Telephone Cheltenham [redacted]
GTN Number
Cheltenham [redacted]

E Wilson Esq
Secretary to the IOCA Commissioner
Room 732A
50 Queen Anne's Gate
London SW1H 9AT

Your reference

GCHQ reference
A/3284/9000/3, 9002/2
Date
20 November 1998

Dear Mr Wilson,

RETENTION OF IOCA MATERIAL

Thank you for setting up our meeting with Lord Nolan on 4 November. We found the discussion most useful. I attach as promised a paper summarising the issues; I should be grateful if you could give it to Lord Nolan. Please let me know if he requires any further information. We will of course be able to discuss further, if Lord Nolan wishes, when he visits us on 16 December.

A specific issue concerns GCHQ's compliance with the Commissioner's determination of August 1997 on "Retention on Serious Crime Grounds of Material Derived from Intercepted Communications". In compliance with the determination, GCHQ has introduced different procedures (copied to you on 1 December 1997) for the handling of material intercepted where its acquisition and retention is necessary to prevent or detect serious crime. The sufficiency of those new procedures, which attempt to take account of the nature of the material received under warrants complying with section 3(2), is not addressed in the attached paper. As the Commissioner is aware, virtually all interception by GCHQ in the serious crime field is undertaken under the authority of such warrants. We will need to discuss separately with Lord Nolan the progress of our first annual review of such material, perhaps when he visits here on 16 December.

Yours sincerely,

[redacted]

A84

Copies to DO DL LA LA1
AZ to see on file

Copied 29/7/99 (CGU) to [redacted] ISA Comms. Sec.

15/6/2016
Scanned & saved

[redacted]

[redacted]

Attachment to A/3284/9000/3

RETENTION OF IOCA MATERIAL

Issue

1. Important GCHQ operations are authorised by warrants and certificates complying with section 3(2) of the Interception of Communications Act 1985 (IOCA). As a result of technical developments the product of these operations is now handled in new ways; further change is contemplated. GCHQ seeks the Commissioner's confirmation that current practice is in line with section 6 of IOCA, and his views on our proposals for the future.

2. Subject to the Commissioner's views, GCHQ proposes to resubmit to the Secretary of State amended "safeguards documents" that which will allow him to conclude that the requirements of section 6(2) and (3) are satisfied. These documents will cater specifically for the use of databases to store intercepted material.

Background

Established practice

3. Warrants complying with section 3(2) ("3(2) warrants") authorise interception of external communications; they are accompanied by a certificate that sets out what intercepted material may be examined. By section 6(1)(b) the Secretary of State is required to ensure that intercepted material outside the terms of the certificate is not read, looked at or listened to. In practice GCHQ has worked as follows to meet these requirements:

a. Because of resource limitations, only part (between 1% and 20%) of the communications specified on the warrant can be intercepted at any one time.

b. The intercepted material is scanned automatically (usually by reference to telephone numbers or keywords) at the point of interception. This selection process is designed to implement the certificate, and only telephone numbers or keywords designed to select messages within one of the categories specified in the certificate are used in the process.

c. Only the selected material (between 0.5% and 15% of the intercept – but only around 0.1% of the warranted communications) is available for examination at GCHQ. We believe that the small proportion available for examination reflects the success of our efforts to exclude irrelevant material and so minimise intrusions into the privacy of the public.

d. The selected material is sent to the analysis and reporting area originally requesting the collection, and looked at or listened to within a few days of arrival. If it is of clear intelligence interest, it is transcribed and (if appropriate) reported; if not, it is quickly discarded and cannot be returned to.

[redacted]

[redacted]

4. This has the disadvantage that GCHQ has to decide whether to use selected material at once, and the decision has to be taken by the person who asked for the material to be selected. But in the real world such inflexibility acts against GCHQ fulfilling its functions under the Intelligence Services Act 1994 (ISA), and prevents the production of valuable intelligence. In the areas of terrorism, proliferation and serious crime, leads typically emerge at unpredictable intervals; in order to make most effective use of GCHQ's collection systems, it is necessary to be able to follow up these leads in earlier as well as later intercept. In all these areas GCHQ aims to provide long-term strategic intelligence. The individuals and groups involved in a particular incident or crime today are in many cases likely to be involved themselves in others in the future, and also to communicate with different individuals and groups who also are or will be legitimate targets.

Current practice

5. GCHQ has for some while fed selected material emanating from 3(2) warrants (that is, the material described in paragraph 3c above) into databases, from where it is retrieved by analysts as set out in paragraph 3d. However the material is not then discarded, and can be returned to. This obviously permits analysts – not only those in the area which originally requested selection of the material - to retrieve material from them at later dates. This achieves many of the aims of paragraph 4. Indeed some material will, because of GCHQ's limited resources, not be examined at all at the initial stage, but will still be available for later retrieval. Unless a message is retrieved by a subsequent query, it will remain in electrical form, unseen and unread after its initial examination (if any), until the time comes for it to be deleted (see paragraph 6d below). The same databases also contain material that has been intercepted outside the scope of IOCA.

6. The following safeguards are being applied. For practical reasons, they are applied equally to IOCA and non-IOCA material – that is, a highest common factor is applied.

a. Only GCHQ staff with a legitimate need can access the database.

b. All queries asked of the database must have an identifiable and specific intention, which is necessary for one or more of the purposes set out in section 2(2) of IOCA.

c. Each query is recorded permanently in an audit trail with the date and the identity of the analyst responsible. A random sample of the audit trail is periodically checked by a line manager, with the intention of ensuring that use of the intercepted material is limited to that necessary for the purposes specified in section 2(2) of IOCA, deterring improper use and detecting any such use that may occur.

d. If a query is designed to elicit information about a UK person (for example if it uses a UK telecommunications address[1], a person's name, or other details that identify an individual, as a basis for the request), special permission has to be obtained in advance. Similar rules apply to other categories of persons regarded as sensitive. In the case of a UK person, the permission can only be given by a member of GCHQ Directorate,

1 This is to be distinguished from initial selection by reference to a UK telecommunications address, for which an 'overlapping' warrant is required.

[redacted]

[redacted]

applying the same test that would be applied by the Secretary of State to the issue of an IOCA warrant.

e. All material in the database is deleted [redacted] after it is intercepted, whether or not it has been looked at. Additionally all material obtained under warrant for the purpose of preventing or detecting serious crime will be reviewed after at most [redacted] and deleted unless there is specific and justifiable cause to retain the material for a longer period.

7. GCHQ believes that such safeguards are sufficient for the purposes of IOCA section 6. The limit of [redacted] for retention is the same as currently agreed by the Secretary of State. Much more of the selected material will however be retained for the whole [redacted] rather than being discarded after a few days. But little of that material will actually be examined during its longer retention. For that to happen it will have not only to be selected in the first place, but also be retrieved from the database in response to a query. The query (as well as the initial selection) will have to be necessary to meet one or more of the purposes set out in section 2(2) of IOCA, in that they are necessary in the interests of national security etc. Once a query has been made, any further copying or disclosure of the material retrieved will be in accordance with the existing arrangements, just as if the material had been examined on first being intercepted.

Future developments

8. In some special cases it will be necessary for GCHQ to feed certain categories of material into a database as a whole, without selection. For example, GCHQ can use [redacted] to identify the movements – if necessary some while before the date of the search – of those suspected of espionage or terrorism. Since it cannot be known in advance who the suspects will be, or when or where they may travel, no initial selection is possible.

9. To date GCHQ has obtained this kind of material from non-IOCA sources only. But in future it may become available under 3(2) warrants. The selection of each category will have to be justified in terms of the relevant certificate (modified if necessary). All the safeguards listed in paragraph 6 will apply. In addition GCHQ recognises the particularly sensitive nature of the material, and so access to this unselected material will be limited to a very small number of GCHQ analysts (no more than ten), who will submit queries on behalf of the remainder of GCHQ or (when appropriate) other agencies. Such queries, obviously, will be asked only for the purposes specified in section 2(2) IOCA, and any dissemination of the results will be in accordance with arrangements made to comply with section 6.

---

2 A small amount of material – for example cipher that cannot yet be read – is exceptionally retained for longer periods. For practical reasons such retention is in separate databases with limited access. The copy in the main databases is always deleted after [redacted]

[redacted]

Gist to accompany document ref 20 November 1998, GCHQ ref A/3284/9000/3 9002/2

Paragraph 8, gist to read: *'travel or financial messages'*

Double underline indicates gisting

Release of Raw Sigint Data to Industry

GCHQ is increasingly working with OGs and industry partners to maximise its impact in critical operational arenas.

A key factor in the development of new Sigint systems and capabilities enabling GCHQ to stay ahead of technological developments is the process of sharing sets of raw Sigint data with commercial partners and suppliers contracted to develop new systems and capabilities for GCHQ.

Mission Policy is responsible for authorising the release of raw Sigint Data to Industry partners. Additionally, limited Delegated Release authority has been granted to specific individuals in *the research team* in recognition of the business requirement for frequent releases of routine sets of raw Sigint data to industry partners, as part of *the research team's* Mission to keep the organisation agile.

Processes for Releasing Raw Sigint Data to Industry Partners

Requestors should fill in the request form, providing as much detail as possible and applying special consideration to:

- Data transfer - Security requirements state that all data leaving the building must be encrypted.
- Data storage - GCHQ data must be stored on databases/systems that are suitably accredited for the data that you wish to release.
- Proportionality - Assess whether the requirement could be fulfilled with less data.
- Access/clearances - Access to GCHQ data must be limited wherever possible to DV and STRAP cleared personnel, with a need-to-know.

Raw intercept is provided only for the stated purposes on the data release request form. Any proposal to share the data outside of these parameters must be referred back to GCHQ.

Once completed, request forms should be emailed to:
Non- *research team* requests – *relevant policy team*

Research team requests – *relevant named GCHQ POCs*

Double underline indicates gisting

REQUEST TO RELEASE RAW DATA

NAME and TEAM OF REQUESTOR:

DATE OF REQUEST: __/__/__

POLICY RESPONSE REQUESTED BY: __/__/__

	Who do you want to release the data to?		
For Language Processing	BSS	SIS	JLAC
Bulk Raw Sigint data	*Foreign partner*	*Foreign partner*	INDUSTRY
Other (Please give further details)			

477

N.B. Bulk data sharing with SIS/BSS is handled by the SIA Inter Agency data sharing process, there is a separate request form for this [REDACTED]

ON COMPLETION, THIS FORM SHOULD BE EMAILED to:

Your local delegated release authority for Language processing or *research team* requests

Relevant team for foreign partner requests

Relevant policy team named POCs for everything else

SUMMARY			
What data do you want to release? (Please include type of data e g. [REDACTED] etc.) Please include *identifier numbers and notations.*			
Will this be a one-off or ongoing requirement?			
Please provide context details on the Operation/Target/Project			
Why do you want to send the data? (Please provide clear business benefit, and include *requirement* number and statutory purpose NS/SC/EWB where relevant)	National Security	Serious Crime	Economic Well-Being
Is there any precedent for this request? (If so, please provide details)			
OPERATIONAL DATA			
How much data is needed to complete the task?			
Is the data selected or non-selected?			
What is the Protective Marking of the data?			
Is the data owned by GCHQ? (If the data is not owned by GCHQ please identify the owner, and include *identifier numbers and notations.* here possible. If owned by a collaborating agency, please state which agency.)			

478

SUMMARY	
Will the identity of SIGINT targets be apparent in the data?	
Will the means by which GCHQ has acquired the data be apparent to the recipient?	
Has the data been processed by *the relevant GCHQ team? ?* If yes, please include formal release approval (email) from the *relevant GCHQ team? ?* . (you can check here **[REDACTED]**	
Is the data from *special source co*llection? If If yes, please include formal release approval (email) from the *relevant GCHQ team? ?* . (you can check here **[REDACTED]**	
Language Processing releases ONLY: Why can't the data be processed by GCHQ or *foreign partner* linguists?	
If the content is of value, will it be reported (and if so by whom)?	

479

RECIPIENTS' DETAILS	
Who will the data be provided to? (Please provide organisation, name and job title.)	
How many additional people will require access to the intercept?	
Please provide the level of clearance and indoctrination (SC, DV, STRAP etc.) for all recipients mentioned above.	
(***Special source collection*** **data only)** Please include details of any [REDACTED] briefings required/received	
What is their employment status within their organisation (employee, contractor etc.)?	
Where will the data be processed?	
How will the data be sent to that location? (Please include details of secure transfer method to be used)	
Where and how will the data be stored? (Please include details of system accreditation levels and additional security measures in place to protect the data)	
How long will the data need to be kept to complete the task?	
Will the data be destroyed or returned to GCHQ? (Please include details of destruction processes in place if not being returned)	

480

ANY OTHER CONSIDERATIONS?

ADDITIONAL DETAILS: (FOR APPROVERS USE ONLY)

AUTHORISED BY: (NAME AND DATE TO BE COMPLETED BY POLICY/DELEGATED RELEASE AUTHORITY) PLEASE INCLUDE ANY ADDITIONAL CAVEATS/CONDITIONS FOR APPROVAL IN YOUR RESPONSE The approver should save the form with the approval / rejection decision to the *electronic filing system* in this folder (for language requests): [REDACTED] relevant folder)

481

Double underline indicates gisting

Main corporate BPD tool Learning Guide

Table of Contents

1. Introduction

This provides a guide to using the *main corporate BPD tool* for running queries and handling results. You may refer to individual sections for reference as required or read the whole document for a full understanding of the tool.

The material is available on the *internal webpages*, in this document, and in addition in an enhanced interactive version available on *the e-learning tool*.

You may also refer to the Troubleshooting page for further help resolving specific known issues.

2. Running Queries

A. Selector Query

[REDACTED]

B.

- Click the **Selector Query** tab to start a query for a single selector
- Enter the selector you'd like to query data sources for (the 'query term') and choose the type, e.g. [REDACTED].
- Your search will attempt to find an exact match [REDACTED] [REDACTED]

- Enter a *requirement* number, JIC and HRA justification for your query. For further information, see the Compliance Guide
- Click the **Search** button to enter your query.
- On the 'Select Data Sources' page, you must choose which data sources you would like to query against. Initially, all available data sources are selected which contain data matching the type you've entered. You can deselect data sources to exclude them from your search.
- If you do not see a data source available which you expect to be able to search, check that you've entered the type appropriate for the data source. Otherwise you may need to be assigned to a particular group in order to get access and you should discuss this with your local *point of contact*.
- Click the **Start Query** to begin searching. Alternatively you can click **Edit Query** if you need to go back to change your query term or type.
- [REDACTED]

- Your new query will be added to the top of your Results list. Once this has completed you can View the Results.

C. Bulk Query

- [REDACTED]
- Click the **Bulk Query** tab to start a query for a list of selectors
- Enter a list of selectors that you'd like to query data sources for (the 'query terms') and choose the type, e.g. [REDACTED]. All the selectors in the query must be of the same type, so you'll need to create a separate query for selectors of separate types.
- Enter a justification and select the data sources, just the same as the selector query, to start searching. Each of the selectors in your list will be appear as a *separate* query at the top of the list of results. As these complete you can open each individually to View the Results.

[REDACTED]

D. Text Query

[REDACTED]

- Click the **Text Query** tab to start a query words or characters to find in textual data - names or addresses.
- Enter the words that you'd like to query data sources for (the 'query term') and choose the type, e.g.[REDACTED]
- Your query will attempt to find all of the words you have entered in the data source but [REDACTED].
- [REDACTED]
- Enter a justification and select the data sources, just the same as the selector query, to start searching.

E. [REDACTED] Queries

[REDACTED]

- [REDACTED]
- These queries [REDACTED] may take much longer to run

3. *Viewing Results*

A. Data Sources

- The *main corporate BPD tool* queries multiple datasets from a variety of sources. Datasets are constantly changing and often don't have much in common - it's not really helpful to think of it as '*main corporate BPD tool* data', because each dataset is different.
- To find out about the different datasets, click on the 'datasources' tab, or click on the name of the dataset from your results screen.
- You will only be able to see datasets you have access to. Some datasets also have access restricted at column level.
- See also 'Reporting Results', below.

B. Results Summary

[REDACTED]

- The Results summary list is displayed after creating a new query or can be found from the **Results** tab. This lists your *current and previous queries* and shows if they are complete or still pending.
- Once complete, a query will show the number of results and hovering over this number will give a breakdown of data sources in the results. **Double-click** on the query to open and see the results.
- You can click on the column headings to sort the table. By default, the most recent queries are shown at the top.
- [REDACTED]
- The following **alerts** may be shown in the *Info* column:
  - ! indicates that your result have a hit in an important data source, which you must review. Hover-over or open the results for more information.
  - indicates that another user has also run the same query. Hover-over for the details of who and when.

- Initially *all* of your queries are displayed. Select an alternative view from the drop-down to show only certain queries.
  - *Bulk* queries are the individual query terms run as part of a bulk search.
  - *Empty* queries are those with no results.
  - *Complete* queries are those which have completed processing.
  - *Expired* queries are those more than two weeks old, for which the results have been purged from the system. You can re-run the query if you have an ongoing justification.
  - *Failed* queries have not been able to complete a search successfully due to a technical issue and there may or may not be results. You should review the Troubleshooting page and raise a support call if this continues to occur.
  - *Defeated* queries have returned an excessive number of results or have been added to the defeat list for some other reason. Hover over the status for more information.
  - [REDACTED]

- **Defeats** are designed to ensure the quality of results returned by excluding selectors that are known to not be meaningful or return large numbers of irrelevant results. They also help ensure timely and performant results by avoiding long-running queries on the system.
  - For example, known cloned IMEIs and bad or invalid data found recurring in sources can be added to the defeat list to avoid returning large numbers of results when querying for these values or hitting on results that would chain through them.
  - If a query results in more than 500 results from any one data source then the query will be automatically defeated and the query term will be added to the defeat list by the system.

- If you think your query should not be defeated then you should review the Troubleshooting page and consult your local *point of contact* for further advice.

[REDACTED]

- Once you no longer need to retain the results of a query you can remove the query from your list by selecting it and clicking the **Delete** button. You can also use the right-click menu.

[REDACTED]

- You can select multiple query results by holding the **CTRL** (to select a series of rows) or **SHIFT** (to select a range of rows) button and selecting a series of rows, or by clicking **Select All**, and then delete all in one go.

C. Result Detail

- When you open the results for a query you'll see the full detail of the results in a subwindow broken down by data source.
- [REDACTED]
- The summary at the top of the page gives the number of results in each data source. Scroll down or click the data source name to jump straight to a particular data source.
- The matching field in each result is highlighted in green, whilst [REDACTED] results will be highlighted in yellow.
- Other fields that are searchable are links and clicking them will seed a new Selector Query.
- Fields containing the *target knowledge base unique identifier* or links to other systems will click-through to launch in a new window.
- Hover over the data source name, or click for a popup providing further information about the content of the data source and instructions for handling the data.
- Hover over the column headings for further information on the content of the column, including the specific protective marking of a column:

    - *Where a set of results contains a data source with one or more columns specifically protected by knowledge compartments or nationality caveat, the classification banner on the data source will include this and show the combined protective marking. The coloured triangle on individual columns indicates those column are protected with the same marking as the banner; but in this case other columns will show a black square indicating that the column is not protected by the same knowledge compartments or caveat, and the hover-over and handling instructions will provide further detail.*

D. [REDACTED]

[REDACTED]

E. Viewing [REDACTED] Results

[REDACTED]

- The data sources in the *main corporate BPD tool* are fused together by the shared *field types* which link corresponding selectors in different sources.
- [REDACTED]

F. Providing Authorisations

[REDACTED]

- When you open the results for a query you may see that some of your results are hidden and are prompted for an authorisation. This indicates that your search returned results from one or more datasets which contain communication content or are otherwise sensitive.
- The results from these datasets will be hidden, along with [REDACTED], and the warning messages in grey boxes indicate which sources contain the hidden results as well as the matching terms (including [REDACTED]). Click the data source names to view the descriptions and identify whether the dataset contains content, or *data of a financial or travel nature*.

- You are expected to take reasonable steps to determine whether you need an authorisation to view the results.
  - A RIPA s.16(3) authorisation (if your target is in the UK) and your results include communication content.
  - A COPA if your target is sensitive in COPA terms and your results contain communication content, *data of a financial or travel nature*.

[REDACTED]

- You may need to use tools such as *the locational tool* to determine whether the selector indicates that the target is in the UK.
- In order to view results that are hidden then you must provide a reference number for the authorisation or indicate, with a reason, why none is required, and click **Apply**. For example, *Target not believed to be in the UK or otherwise sensitive*. This information is recorded for audit purposes.
- If your results contain dated communication content [REDACTED]. If your authorisation does not permit retrospective querying of this content then you must enter the valid dates of the authorisation in order to view only the matching records. You will be notified if there are remaining hidden results that are outside this date range.
- If you are authorised to view some but not all of the sources containing results then you must run a new query choosing only the relevant sources.
- Where you have some results that chain through 'hidden' sources you will first authorise the results that match directly and then if any of those seeded chained results that are also in hidden sources then a second authorisation is required to reveal those chained results.

G. Viewing Multiple Results

[REDACTED]

- The detailed results sets open in a moveable window within your browser window and if you need to view and compare two or more result sets at a time then you can do so.
- If you have one result set open and want to compare to a second you can just double-click a second query in the result summary list to open a second window.
- Or you can select two queries from the result summary list holding the CTRL or SHIFT buttons whilst selecting and open them both at once, by clicking Open from the bottom of the screen, or Open Selected on the right-click menu.
- To see both results windows at once you may need to spread these across two monitors. To do this you must first expand your Firefox/Internet Explorer window across the two monitors, by restoring the window (if it was maximised) using the  button and then resizing the browser window using the  button to extend across your monitors. Then you can move the result windows, using the black bars, between monitors.

[REDACTED]

H. Bookmarking Results

[READCTED]

- To save bookmarks for result sets, press **CTRL-D** whilst you have the results open. This will create a bookmark which will return you to *main corporate BPD tool* and open the result set at a later date, provided it has not expired or been deleted.
    - In *Firefox*, you can also click the button in the address bar. The bookmark will be created in the *Recently Bookmarked* folder on your *Bookmarks* menu.
    - In *Internet Explorer*, you can also click **Favourites > Add Favourite** and the bookmark will be created in the selected folder.

4. Exporting Results

A. Exporting to Excel

[REDACTED]

- To export your results to Excel, select the query and either click the **Export** button, or the **Export Selected** option from the right-click menu.
- In Firefox, you may need to accept the popup warning the first time you do this. Click the **Options** button on the yellow bar at the top of the window and choose to *Allow popups...* (as shown). On this occasion you may need to click the **Export** button again.
- The *Opening...* window will appear and you can choose to Open or Save. Opening will launch Excel.
- [REDACTED]

- Your results are arranged into separate tabs (worksheets), with a separate tab for each data source. The first tab shows a summary of results, and you must choose one of the other tabs to see the detailed results (as shown).
  [REDACTED]

B. Write-back to the *target knowledge base* using *the relevant tool*

[REDACTED]

- You can write-back new selectors that you find in your *main corporate BPD tool* results into the *target knowledge base* using the *relevant tool*. This allows you to create new selectors individually or in bulk to reduce the repetitive steps, and passes metadata from the *main corporate BPD tool* data sources and your query HRA in order to automate much of the process of populating the *target knowledge base* record.
- Click the *relevant* button at the top-right of the result window to start the 'picker'. Then click the cell of each of the selectors that you would like to write-back and it will be highlighted purple.
  [REDACTED]
- In order to associate the new selectors to an existing target, you should click the corresponding *unique identifier* in a *target knowledge base* result. Otherwise, the selectors will be associated to a new target. You can click *the relevant* field to pass it as the name of the new target.
- Only columns that can be used as selectors in *target knowledge base* will be pickable. These are [REDACTED], and are highlighted as you hover over them. Any TEL_NUMBERS will be defaulted to the *target knowledge base* MS-ISDN type - if your selector is a PSTN, you should change the type in *the relevant tool*.
- Click the **Continue to *the relevant tool*** link to launch the *relevant* tool. In Firefox, you may need to accept the popup warning the first time you do this. Click the **Options** button on the yellow bar at the top of the window and choose to *Allow popups...* (as shown). On this occasion you may need to click the **Continue to *the relevant tool*** button again.
- For more information on using *the relevant tool* to complete the write-back to *target knowledge base*, see the Getting started with *the relevant tool* guide and the *internal webpages*, which provides an eLearning package.

[REDACTED]

5. *Reporting Results*

A. Handling Instructions

[REDACTED]

- Before including any results in *intelligence reporting* you must check the **Handling Instructions** which are displayed by clicking on the name of the data source in your results. You can also find these by clicking on the **Data Sources** tab at the top.
- This will detail whether and how you can report the results you have found. You may need to consult the data owner for permission.
- If not otherwise specified, then details of the *main corporate BPD tool* results used in *intelligence reporting* should be recorded in *the reporting tool* in *the relevant tab*. This should describe how the material was found in *main corporate BPD tool.*

Double underlining indicates gisting

BPD Travel data tool Tutorial

1. Introduction

This is a training tutorial for the travel analysis tool, the *BPD travel data tool*. It can be used in unison with online training videos, or as a standalone training document. It will outline how you can use the *BPD travel data tool* to perform travel analysis on targets. Each section is self-contained and uses a scenario to explain how you can perform specific activity in the tool.

The *BPD travel data tool* is GCHQs Travel Analysis tool that uses various different feeds of information to build a picture of the travel of individuals. Underlying data sources include [REDACTED]. More details around the tradecraft of Travel Analysis can be found in the *relevant* training course.

2. Contents

3. [REDACTED] Search

This topic will show you how to complete a search for a target [REDACTED]. For this Scenario, let us suppose that we have intelligence that indicates our target 'Mohammed Al-Khani' may have travelled [REDACTED]. We want to use the *BPD travel data tool* to locate this travel record, and find out more details.

[REDACTED]	[REDACTED]
Choose a name for the search *[REDACTED]*	At this point we can give our search a name – 'Al-Khani's [REDACTED]. Although this is not mandatory it will allow us to find this query later on, particularly if we go on to create a number of other queries.

500

In the HRA field, click the plus button to create a new HRA Justification. ***[REDACTED]***	Using the *relevant tool* HRA pickers we can quickly select a recently used HRA justification, JIC Priority and *requirement* Number. As this is a *relevant tool* component my last 3 HRA's are shared across all *relevant tool* applications. For this query I will choose to create a new HRA justification.
Enter target's name in 'Any Name' Field. ***[REDACTED]***	The *BPD travel data tool* allows us to search for names [REDACTED]. By using the [REDACTED] fields we can explicitly ask the *BPD travel data tool* to search for [REDACTED]. [REDACTED].

151

[REDACTED] **[REDACTED]**	The *BPD travel data tool* supports [REDACTED]. [REDACTED]

527

[REDACTED] **[REDACTED]**	[REDACTED]
View the [REDACTED] field *[REDACTED]*	[REDACTED]
[REDACTED] **[REDACTED]**	[REDACTED] Once the query is completed, pressing view will navigate to the results page.

4. Interpreting Results

The previous topic showed how to create a simple query for the travel of a [REDACTED] individual. This next topic will show you how to interpret and manipulate the results.

Inspect the Various Different Message Types **[REDACTED]**	The first thing we should note about the results screen is the various types of different results which have been returned, including [REDACTED].
Click on the headings to sort fields **[REDACTED]**	By clicking on any of the headings labelled with a hand icon we can sort the results. If there are a small number of results this may be sufficient to spot the information.

504

Using the menu on left, filter the results using the available fields **[REDACTED]**	Alternatively the *BPD travel data tool* allows **filtering** by expanding the side bar on the left of the screen Each of the heading details a particular field, and when expanded this section shows all values for that field which are present in the results set. These can be used as a filter to remove results which are not required. [REDACTED]
View the flags field within the results table **[REDACTED]**	The flags to the right of the screen provide an indication of what additional information is included in the travel record, these could indicate, [REDACTED] For our current search it looks like there might be a number of [REDACTED].
Click on the Actions button and then 'Expand Row' to show the detail for an individual row. **[REDACTED]**	Clicking on the Action button at the end of individual rows, or anywhere on the row, will expand and show the detail for that row. The *BPD travel data tool* records which rows have been expanded and viewed by different individuals, and this is indicated by the eye icons on every row. Because we have just opened this row, a blue icon has appeared. If we had viewed this row by mistake it would be possible to remove the viewing by clicking on the actions button and selecting 'remove viewing'. With the row expanded we can see details of the selectors highlighted in the icons.

	The *BPD travel data tool* has integration with *an analysis tool* which means all [REDACTED] information that relate to the travel can be 'clipped' and sent to casebook. Similarly it is possible clip individual fields such as [REDACTED], or use these as seeds for a new Travel Query.
Export technical data **[REDACTED]**	It is also possible to export the whole result set, using the Actions button on the top right of the screen. From our starting point of 'search for travel from [REDACTED]' we have discovered a [REDACTED] that we can use for targeting in the future. We may wish to include this in an *intelligence* report at this point, and will need to export the suitable *technical data* information. To do this we first need to select the travel records which we are going to include in the report. These can be individually selected from the tick-boxes to the left of each item. Then using the Action menu on the top of the screen we can display the *technical data* information for the individually selected row(s), which we can use to copy and paste into *the intelligence reporting repository*.

5. [REDACTED] Search

In the previous Topic we were able to discover [REDACTED]. This scenario will show how we can search for [REDACTED].

Navigate to the Dashboard and select '[REDACTED] Search' ***[REDACTED]***	Starting from the dashboard we will choose a new [REDACTED] Search.
Enter Search Name, Details and HRA Justification ***[REDACTED]***	As we are using the same HRA justification we recently used to search for Muhammad Al-Khani we can select that from the list 'Recently Used HRA justifications'. We can now enter the [REDACTED]. [REDACTED] We therefore click 'view' to navigate directly to the results.
Expand a row to view details [REDACTED]	The results show the [REDACTED] record which reveals the [REDACTED] for our target.

6. [REDACTED] Search

This topic will show how the [REDACTED] Search can be used as a 'keyword' search. [REDACTED]. The *BPD travel data tool* allows us to create a search that will look for a match across all fields.
In this scenario we are interested in the travel of [REDACTED]

Return to the Dashboard and click [REDACTED] [REDACTED]	Starting from the dashboard we will choose a new [REDACTED] Search.
[REDACTED]	*Give search a name – Saudi Travel – and then enter::* • *HRA* • *[REDACTED]* We can enter our [REDACTED] [REDACTED]
View search results ***[REDACTED]***	After we have submitted the search we can see that the *BPD travel data tool* has returned 377 results, including several that include [REDACTED] – highlighted in Yellow. For the purposes of this scenario we wish to focus on travel between [REDACTED]
Expand the first two records. [REDACTED]	Looking through the detail of the record, we can see that they encompass [REDACTED].

7. Saving, Active Queries and Bookmarking

The previous topics looked at ways of creating queries and interpreting results. This topic focuses on saving queries for future reference and therefore marking them as active.

In this scenario, we want to set up an active query that will continue to look for travel data for Mohammed Al-Khani each time we log into the *BPD travel data tool*. We have already created a search which looks for Mohammed Al-Khani's [REDACTED]. We now need to save the query and mark it as active.

Navigate to the Dashboard and select [REDACTED]	Starting from the dashboard we will choose a new [REDACTED] Search.
Give the Search a name [REDACTED]	Enter a title for the search, 'Mohammed Al-Khani - 3rd Feb 2015' in the text box to the left of the pencil and then click Save.
Enter Classification [REDACTED]	After clicking Save we will be asked to enter a classification to cover the sensitivity of the query terms. Enter the classification as [REDACTED] and click OK. The application will confirm when the query has been saved successfully.

505

Return to Dashboard and view Stored Searches [REDACTED]	If you navigate to the Dashboard tab we will see our query is available in the Stored Searches widget. You can order searches by selecting the drop down menu in the top right corner of the Stored Searches widget. Click on the 'Stored Searches' title to view the searches in more detail.
Edit or delete stored searches [REDACTED]	Clicking on the 'Stored Searches' title allows you to view and manage your stored searches. This shows a complete list of all your personally stored searches. The Dustbin icon on the right hand side of each saved search, allows us to delete that search. If we wanted to rename or edit a saved search, clicking on the Pencil icon on the right hand side of the search takes us to the Search view. We can retype the search name and save to update the name of the stored search.
Mark search as active [REDACTED]	An Active Search enables us to monitor a saved search for new results using our original search criteria. We can make a search active in one of two ways; from within a saved screen by clicking on the active button... ... or from the Saved Searches page. Next to the option to delete a saved search is a clock icon which toggles on/off the 'Active' search.
Navigate to the dashboard and view Active Searches [REDACTED]	Once a search is marked as active it will now show in the Active Searches widget. The *BPD travel data tool* will check the query for new results when you press the refresh icon at the top of the section, or the icon next to an individual search.

	If there are any new results since the last time we viewed the results of the query, then clicking on the orange pill will navigate to those results. Alternatively clicking on the Magnifying Glass icon will navigate to all results for that query.
Navigate to View Results page to Bookmark results ***[REDACTED]***	Bookmarking allows important query results to be flagged, making it easier to return to them at a later date. Let us suppose there are some travel events which have been flagged in Al-Khani's latest travel results which we need to remember to look at in more detail. We can bookmark an item using the Actions button next to our results. We can see a Bookmark flag and we can see when we bookmarked the item by hovering over the flag. This is important because Bookmarked items are only retained for one month before the bookmark, and the HRA justification expires.
Navigate to the dashboard and view Bookmarked Items [REDACTED]	You can view all bookmarked items on the Dashboard. Click on the Magnifying Glass icon on the right hand side of an item to navigate directly to those results. Alternatively you can click on the 'Bookmarked Items' title to navigate to the Bookmarks page.
Group by HRA Justification [REDACTED]	It is possible to group all bookmarks by the HRA justification under which they were searched for. Select 'HRA Justification' from the drop down list to group bookmarks by HRA Justification. By clicking on the icon next to the HRA justification we can navigate to see all results collected under this justification
Remove bookmark from results page [REDACTED]	Bookmarks can be removed from the results page using the actions button or...

115

	... from the dashboard by clicking on the dustbin icon

8. [REDACTED] Search

The topic will show how to complete a [REDACTED] Search. For this scenario we have reason to believe that [REDACTED]

[REDACTED]	Our first step is to use the '[REDACTED] Search' Template to create a query [REDACTED]. Once we have completed our query we can press the 'count' button.
[REDACTED]	Just like the [REDACTED] Search also has an intermediate step we can use to limit our total results. Before we are taken to the results page, we can view [REDACTED].
[REDACTED]	[REDACTED].
[REDACTED]	Using the menu on the left we can filter the results. [REDACTED]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE
MI5

[REDACTION]
Deputy Director General

Relevant team/BPD/Policy

Sir Mark Waller
Intelligence Services Commissioner

29 October 2014

[Dear Sir Mark]

BULK PERSONAL DATA – CHANGE OF MI5 POLICY ON REVIEWS

I would like to advise you of our intention to change the way we conduct reviews of bulk personal data. Currently, all such datasets are reviewed on paper every six months, and our internal Bulk Data Review Panel reviews each dataset as least once every two years. We intend to move to a flexible, risk-based approach which will enable us to apply different review periods to different datasets based on a clear set of criteria.

2. In summary, we will use our assessments of the levels of (i) intrusion and (ii) sensitivity (or corporate risk) associated with a dataset to determine the review period:

HIGH Intrusion and/or HIGH Corporate Risk:	Every 6 months
MEDIUM Intrusion and/or MEDIUM Corporate Risk	Every 12 months
LOW Intrusion and/or LOW Corporate Risk:	Every 2 years

3. We intend to give our Panel discretion to vary these review periods if it judges appropriate. The extent of 'use' is likely to be a key factor (e.g., lack of use will mean more frequent reviews).

4. I am confident that the changes will enable us to apply a more effective and proportionate review process, with attention focussed on the most intrusive and sensitive datasets, whilst reducing the burden of paperwork in relation to lower intrusion and lower risk datasets. As you know, GCHQ already uses flexible review periods (6 and 12 months), and SIS decided in 2013 to adopt flexible review periods (between 12 and 42 months). Whilst review timescales and criteria are not yet fully aligned across the SIA, this change will bring MI5 closer to the approaches used by the other two agencies.

[REDACTION]

SECURITY SERVICE
MI5

5. At every inspection visit, we will continue to provide you with a full list of all bulk datasets that were extant at any point during the review period, and invite you to inspect any of the datasets held. All review paperwork from the preceding meeting will also be made available. Further details of our new process are provided at Annex, and I would welcome the opportunity to discuss our new arrangements during your inspection in December.

6. Copies of this letter go to [REDACTION] and Sir Paul Kennedy.

[signed]

[REDACTION]

NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

[REDACTION]

SECURITYSERVICE
MI5

Annex

MI5 Reviews of Bulk Personal Data – Flexible Review Periods

1. Review periods for MI5 BPD will be determined by:

   i. ***Intrusion*** - the level of intrusion associated with the database

   ii. ***Corporate Risk*** – the level of corporate risk associated with the dataset

   iii. ***Usage*** – low levels of usage means that D/SIRO and BDRP can require datasets to be reviewed more frequently.

   iv. ***Theme*** – as determined in advance by the BDRP

2. The assessments of **intrusion** and **corporate risk** will be the primary determinants of the review period applied to a dataset. The periodicity proposed is:

High Intrusion and/or **High Corporate Risk**	-	**6 months**
Medium Intrusion and/or **Medium Corporate Risk**	-	**12 Months**
Low Intrusion and/or **Low Corporate Risk**	-	**2 years**

3. Where assessments of intrusion and corporate risk differ, the higher level of assessment will determine the review period (e.g. 'medium' intrusion and 'low' corporate risk would result in a review period of 12 months, not 2 years). Based on current holdings, the number of datasets falling into each review period is as follows:

	Risk	Intrusion	Total
6 months	[REDACTION] High	[REDACTION] High	[REDACTION] High
12 months	[REDACTION] Medium	[REDACTION] Medium	[REDACTION] Medium
2 years	[REDACTION] Low	-	[REDACTION] Low
			[REDACTION]

4. In relation to **usage**, datasets meeting the following criteria will also be referred to the BDRP for discussion:

[REDACTION]

515

SECURITYSERVICE
MI5

- Any datasets with **no demonstrable usage during a review period**, or where there are issues or concerns around usage; a lack of usage may require the dataset to be **placed on 6 monthly review thereafter;**
- Any datasets **held by MI5 but not ingested** within 6 months to be submitted to the next Panel;
- Any datasets referred to the panel for any reason by the **business, *legal advisers, the relevant team*, or Panel members** during the process of authorisation, review, sharing or transfer;
- Any dataset **approved for deletion** by the BDRP but **not deleted within 6 months**;

5. The BDRP will also review datasets on the basis of **themes** [REDACTION] where datasets falling under a chosen theme are reviewed together. This will enhance consistency and enable strategic issues to be explored by the Panel. Each meeting of the Panel will decide what theme will be addressed at the next panel, so that business and compliance teams can prepare the appropriate paperwork.

6. The D/SIRO and BDRP may choose to **vary the review period** by exception (e.g. to require a dataset to be reviewed in six months rather than two years, if there is a lack of usage). The review period may be increased (e.g. from 1 year to 2), or reduced (e.g. 2 years to 6 months). Whenever a review period is varied, the reason must be recorded.

7. **BDRP meetings** - will continue to be held every six months, ahead of Intelligence Services (IS) Commissioner visits. All datasets submitted for review on paper will be submitted to the BDRP.

8. **Intelligence Services (IS) Commissioner** - The IS Commissioner will continue to be provided with a full list of all bulk datasets held, and invited to inspect any of the datasets held. All review paperwork from the preceding meeting will also be made available.

[REDACTED]
3 January 2014

SUMMARY FILE NOTE: VISIT OF SIR ANTHONY MAY, INTERCEPTION OF COMMUNICATIONS COMMISSIONER, 8-9 OCTOBER 2013

[REDACTED name of dataset]

35. Following a discussion of this dataset, Sir Anthony suggested that it might be appropriate to include the small number of non-targeted bulk personal datasets obtained from interception in the listing put forward to Sir Mark Waller for inspection, so that Sir Mark is aware of their existence and nature.

> **Action 3:** GCHQ to include those bulk personal datasets obtained through interception on the list for Sir Mark Waller's consideration and to explain that this is at Sir Anthony's request. (Action completed)

[REDACTED]

[REDACTED]

4 October 2012

Summary Filenote: Visit of Sir Paul Kennedy, Interception Commissioner, 3 October 2012

[REDACTED]

4. The Commissioner was invited to inspect GCHQ's holding of a highly sensitive and closely held dataset [REDACTED – name of dataset], as part of his non-statutory role in overseeing bulk personal datasets acquired under RIPA authorisation. D/D Mission Policy explained how the acquisition and retention of bulk personal datasets is internally reviewed by a panel of policy seniors. The [REDACTED – name of dataset] dataset is relatively new and has yet to be presented to the panel but will be considered at the next meeting of the panel in November. [REDACTED] The Commissioner commented: "Obviously does help you to [REDACTED]... I can see why it's valuable."

[REDACTED]

[REDACTED]
30 May 2013

SUMMARY FILENOTE: VISIT OF SIR ANTHONY MAY, INTERCEPTION OF COMMUNICATIONS COMMISSIONER, 15 MAY 2013

Key points

[REDACTED]

- He remains to be convinced of the necessity of our retention of communications data for up to [REDACTED] and financial data for even longer.
- He is interested in determining whether there is potential for rationalisation of retention policies across the agencies.

Details

1. This was the first formal inspection visit by Sir Anthony May since taking up post as Interception of Communications Commissioner in January 2013, although he had visited GCHQ for familiarisation briefings in January [REDACTED]. The Commissioner was accompanied by Jo Cavan, Chief Inspector of IOCCO, acting in the role of Private Secretary.

[REDACTED]

Bulk personal dataset obtained under RIPA authorisation

3. The briefings began with examination of the [REDACTED – name of dataset] dataset. The Commissioner was provided with background on the Hannigan Review and the reasons behind GCHQ's request that he provide oversight of non-targeted bulk personal datasets obtained under RIPA authorisation. The financial data that forms the [REDACTED - name of dataset] dataset is collected *overseas* under the authorisation of GCHQ's [REDACTED] 8(4) warrant. The Commissioner queried how, if the collection takes place *overseas*, it fits in with his jurisdiction. D/D LA provided an explanation.

4. It was explained to the Commissioner that financial data can be retained, subject to regular review, for up to five years, which is longer than the standard data retention period. The reasons for this policy were explained. The Commissioner expressed interest in the storage and retention of bulk personal data and would like to come back to the long retention period for financial data.

Action 2: Further discussion of data retention policies to be included in Commissioner's next visit or inspection - Hd/Warrantry and Oversight

[REDACTED]

Deletion/destruction briefing

25. The Commissioner has shown a particular interest in deletion and destruction in GCHQ and across at least the SIA. He requested a briefing on what destruction meant in a technical sense within GCHQ. He explained that if the data is truly deleted or rendered inaccessible that would provide him with assurance, but if it is not, it may be a subject of concern. Hd/Compliance went through GCHQ's operational data retention policy, noting that there are special measures to delete data collected in error. The Commissioner commented that he has seen different variations across the agencies and is wondering whether there is a case for rationalisation. He queried the rationale behind GCHQ's policy for [REDACTED] retention for selected content and [REDACTED] for communications data. It was explained that this policy was developed following a review carried out several years ago. It was assessed that communications data has been proven to remain useful for more than [REDACTED], particularly in the context of target discovery through 'pattern of life' analysis. The Commissioner challenged this by saying that GCHQ uses the term "useful" but the statute says "necessary". In other (LEA) agencies the cut-off point tends to be when the operation has come to an end. The Commissioner was told that GCHQ does the same in relation to Serious Crime cases. D/D LA presented a CT scenario where we need to build up a picture over a long period and therefore need to retain data for a longer time; he also made the case that communications data is inherently less intrusive. The Commissioner agreed the last point but commented that the degree of intrusion does not have much relevance to necessity.

26. The Commissioner asked whether all the communications data was selected (it is not) and checked whether we keep the entirety of all the communications data that comes into the building for up to [REDACTED]. It was confirmed that this is indeed the policy but often storage limitations mean that the data is deleted before the maximum [REDACTED] retention point is reached.

27. The case was put that the longer retention period is critical to our target development/target discovery work, with the 7/7 investigation quoted as an example. The Commissioner suggested that after a period of time we are unlikely to search the data without a prompt such as a terrorist attack. He was told that examination of communications data was also invaluable in determining whether or not to put targets on cover to collect the content of their communications. The Commissioner did not appear to be wholly persuaded.

28. *The relevant official* provided a briefing on GCHQ's disk storage and disk management process, describing how the deletion process first makes the data inaccessible by removing the location reference that would allow the system user to find the data and then eventually overwrites the data. She explained that data recovery is not trivial, it takes time and skill, and the recovery process requires the system to be offline, so we would know if it was being done without proper authorisation. She also touched on disk destruction, explaining that we wipe disks using electromagnetic charges when they come to the end of their life. The Commissioner said that he was reassured by what he had heard.

[REDACTED]

[REDACTED]

16 June 2014

SUMMARY FILE NOTE: VISIT OF SIR ANTHONY MAY, INTERCEPTION OF COMMUNICATIONS COMMISSIONER, 22-23 APRIL 2014

[REDACTED]

Dataset session

20. The Commissioner had been provided with the paperwork on three datasets obtained via interception under RIPA Part I Chapter I – [REDACTED – name of datasets]. He was given short explanations of the nature and value of these datasets, with which he appeared content. He queried whether, given the Intelligence Services Commissioner's oversight of the majority of GCHQ's non-targeted bulk personal datasets, the small number of datasets obtained via interception might be transferred to him. It was explained that Sir Mark was asked to provide oversight on a non-statutory basis only for those datasets obtained via means other than interception because this was perceived as a gap in oversight following the Hannigan review, responsibility for datasets obtained via interception already falling within the oversight responsibilities of the Interception Commissioner. The Commissioner accepted that he should continue to provide this oversight.

[REDACTED]

Filenote of Intelligence Services Commissioner's inspection of GCHQ – 11-12 November 2014
[REDACTED]

Day 1 (primarily CNE, also s94)

[REDACTED]

3. [REDACTED]

(Actions/recommendations relating to s94 oversight were overtaken by events, as oversight has moved to the IOCC.)

Day 2 (Consolidated Guidance, Bulk Personal Datasets and RIPA Part II authorisations)

[REDACTED]

Action taken following an incident concerning misuse of intercepted data

[REDACTED]

9. Sir Mark queried how many [REDACTED] ('triggers' which prompt investigation of potential misuse) have arisen when no misuse had actually taken place. A figure of 100s of [REDACTED] per day when no misuse had actually occurred had been mentioned during the briefing on protective monitoring provided during the May inspection. Some of these can be discounted very quickly, others take longer to investigate, but no serious misuse had ever been detected by these measures. Sir Mark requested a brief description of the trigger mechanisms and an illustration of what the triggers are ('metrics') in order to illustrate the investigation process; he did not feel that it mattered what operational data this related to. Sir Mark was concerned that he had said in his annual report that staff cannot act independently, but the [REDACTED – name of dataset] case demonstrated that this was not true. It did not matter if no misuse was detected; Sir Mark still wanted this information.

[REDACTED]

[REDACTED]

INSPECTION OF NON-TARGETED BULK PERSONAL DATA BY SIR PETER GIBSON, INTELLIGENCE SERVICES COMMISSIONER, 6 DECEMBER 2010

Introduction

1. This was an initial inspection of GCHQ's holdings of bulk personal data, intended to inform Sir Peter's report to the Prime Minister on the Agencies' use and holdings of such data and to allow him to provide guidance on the format of any future inspection of this type. Sir Peter was keen to establish a common set of principles underpinning the Agencies' use of bulk personal data. He was accompanied by Sir Mark Waller, who is soon to take over the post of Intelligence Services Commissioner.

2. DGO noted that the non-targeted bulk personal data that formed the subject of the inspection was a niche part of GCHQ's business and untypical of the majority of GCHQ's foreign intelligence activity. However, data analysis was a core function of GCHQ (unlike sister agencies where the function might be concentrated in a specialist area away from the core investigative functions). GCHQ was consciously moving towards access to non-targeted bulk personal datasets by a wider group of analysts, although smart security would be built into the model and would maintain and enhance the proportionality of this access. DGO noted that GCHQ did not wish to retain large quantities of non-targeted bulk personal data: this would be undesirable on grounds of proportionality and cost.

3. *The relevant official* briefly noted the legal principles underpinning GCHQ's acquisition of such data. Section 4 of ISA allows GCHQ to acquire data in support of its statutory functions. GCHQ policy is that the safeguards set out in section 15 RIPA should govern the handling of any operational data, even if that data has not been acquired under RIPA itself. GCHQ may also rely on Section 19 of the Counter-Terrorism Act 2008 to acquire data, even where there is an obligation of confidence, so long as that data is necessary for the proper exercise of one of GCHQ's functions. If GCHQ receives data from a sister agency or a commercial partner, we would take it on trust that the original acquisition of that data had been lawful.

GCHQ's Procedures with regard to Non-Targeted Bulk Personal Data

4. *The relevant official* described GCHQ's response to the "Hannigan review" of non-targeted bulk personal data. Although GCHQ had not had a formal review process for such holdings prior to the review, we had now developed one. We had also instituted a new Data Acquisition Authorisation form (from 4 November 2010), and updated the relevant sections of the Compliance Guide available on our Intranet. (The updated sections, part of the pre-reading supplied by GCHQ, were again made available.) For each dataset acquired from now on, a Data Requester (*relevant senior official*) would make an application on the DAA form, citing a Responsible Owner (of no specific grade but the person best-placed to take responsibility for the dataset), and the application would be either approved or rejected by the *relevant senior official*. The Authorising Officer has the power to grant temporary approval pending fuller assessment or fuller use of the dataset. It is also his responsibility to determine whether the dataset in question constitutes non-targeted bulk personal data. Sir Peter noted that the critical point of judgement was before the Agency ingested newly acquired data into a database, or made it available for analysts to use. Sir Mark enquired how GCHQ reviewed the retention of its bulk personal data: we stated that we made use of a retention review panel, which meets every six months and is chaired by *a relevant senior official*. The review panel will order the deletion of a dataset where it is no longer needed. Sir Mark noted a potential area of difference between GCHQ and the other Agencies who might decide to retain data against a potential future need.

[REDACTED]

5. Sir Peter had been initially concerned that the Agencies might not be using a common form to record their acquisition of bulk personal data. We noted that the GCHQ form had been informed by others' best practice; however, it did contain different features important to our business, including space to record *foreign partner* sensitivities.

6. *The relevant official* noted the compliance process built into all operational systems (including repositories holding communications data) which obliges those interrogating bulk data to enter an authorised purpose, a *requirement* number and a short HRA justification. (An example screenshot of *the relevant system* was viewed.) Although the sampling and audit of these justifications was well-established, bulk personal datasets were not yet routinely included, and the sampling methodology was not well-suited to detecting anomalies. We had therefore asked the IT Services and Accounting and Audit team to help monitor the use of such datasets. *The relevant official* from IT Services then gave a short presentation on auditing of access to bulk personal datasets, with some illustrated examples of the processes and techniques being developed. Sir Peter was satisfied with the rigour of the audit processes; he also found it interesting to note our usual procedure of requiring analysts to record an HRA justification before acquiring any access to bulk data.

[REDACTED]

7. *The relevant official* gave a demonstration of *the main corporate BPD tool* followed. It was clear that the analyst was not able to scroll through datasets at will, but that data was only returned in response to a specific query. Sir Mark asked about the difference between *the main corporate BPD tool* and SIS's *main corporate BPD tool* database: *the main corporate BPD tool* had more users in total, but there was additional compartmented security at the level of datasets [REDACTED]. [REDACTED]

8. The Retention Review Panel had held its initial meeting in September 2010, and the datasets considered by the panel at that meeting had formed the "menu" of datasets offered to Sir Peter ([REDACTED] of 8 November 2010), of which he had selected the following four non-targeted bulk personal datasets for his inspection.

Inspection of Datasets

9. [REDACTED]

Conclusions

13. On the conclusion of the inspection, Sir Peter gave some preliminary feedback as follows. The principles governing inspections of non-targeted bulk personal data were the same as those governing the usual Commissioner inspections of authorisations. He believed that the Agencies should draw the Commissioner's attention to anything he may need to know and any issue that had been difficult or particularly interesting. The Commissioner should be free to select those datasets that he wished particularly to examine (the "choice letter" had been very adequate and there seemed no advantage to having any more information than had already been presented). Sir Mark thought it would be valuable to see how the audit process was working; for example, to see figures of how often an irregularity was spotted and any "case studies" that resulted.

Section 94 of the Telecommunications Act 1984

14. In addition, Sir Peter had agreed to review a dataset obtained by GCHQ under section 94 of the Telecommunications Act 1984. *The relevant official* explained that GCHQ aimed to reduce the number of data holdings that were not under judicial oversight, and envisaged that all data holdings might eventually come under a Code of Practice and statutory oversight arrangements. We believed that oversight of s.94 data should fall outside the Interception of Communications role, although we were happy to be advised. Sir Peter suggested that it was for GCHQ to set out the track on which such an oversight arrangement might be put in place; Sir Mark agreed that he would in principle be happy to oversee such data in the future.

15. *The relevant official* noted that under s.94 of the Telecommunications Act 1984 the SoS may give a Direction to a CSP to disclose anything held by that CSP, if it is required in the interests of national security. The Communications Act 2003 modified this power to give directions by introducing a test of necessity and proportionality. GCHQ has a number of such Directions, which allow us more flexibility than Notices under Part I Chapter II of RIPA (these notices only last for one month). Sir Peter had selected [REDACTED – Name of dataset] from the [REDACTED] "choice letter" and the relevant submission and instrument (signed in 2001) were made available for the Commissioner to examine.

16. *The relevant official* explained how such Directions were served only as part of a cooperative relationship with a CSP. *The relevant official* then gave an illustration of the benefits of [REDACTED] data, which currently contributes to 7% of GCHQ reporting based on [REDACTED] material. This briefing was well-received by both Sir Peter and Sir Mark.

Filenote for [REDACTED]

11 May 2011

VISIT OF SIR MARK WALLER, INTELLIGENCE SERVICES COMMISSIONER, 29 MARCH 2011

[Redacted]

Inspection of s.94 Directions and Bulk Personal Data

10. *The relevant official* provided some context around the Telecommunications Act 1984, with which Sir Mark was not familiar, rehearsing that s.94 allows the Secretary of State to issue Directions to CSPs in the interests of national security, and that changes made as a result of the Communications Act 2003 specified that any Directions issued must have regard to necessity and proportionality. The data GCHQ receives under s.94 Directions is that which CSPs are willing to provide, but there is no other mechanism by which we can support that provision with a form of legal authorisation. SMW asked whether other public bodies made use of s.94 - the answer was yes (e.g. Security Service).

11. SMW had selected the s.94 Direction served on [REDACTED – Name of CSP] for inspection (GCHQ has requested oversight of the s.94 Directions; it is not a statutory duty). *The relevant official* provided a briefing on the two datasets provided: [REDACTED – Name of dataset]. *The relevant official* noted that it was very unusual for GCHQ to have domestic datasets; [REDACTED]. Any searches of the data were logged and auditable. SMW was satisfied with the case for acquiring and retaining the data, commenting that most people would assume such data was available to security and intelligence agencies; [REDACTED].

12. SMW had requested to inspect the following non-targeted bulk personal datasets: [REDACTED – Name of dataset]. He was satisfied that the datasets were necessary. He asked some specific questions with regard to storage of the data: could we take datasets out of *the main corporate BPD tool* once they are in it? (yes); how did we know whether data had been useful? (analysts fill in the *technical data screen* on reports). We mentioned that GCHQ's review panel had approved 2 *financial* datasets on the basis that they should be re-reviewed after one month and deleted if not proved to be useful.

13. SMW noted that it would be extremely useful to inform his future report if GCHQ could provide (a) a summary of how GCHQ makes use of, manages and reviews non-targeted bulk personal data, and (b) how we audit usage and what safeguards are in place to ensure proportionate and managed access.
Action: GCHQ to write to SMW with this information on non-targeted bulk personal data

14. *The relevant official* provided an update briefing, as SMW had requested, on IT security audit procedures for access to non-targeted bulk personal data. One process had identified some staff who had set queries to run when they had left the building but there was nothing untoward about that. Another process had detected an analyst who had run a self-referential query; this incident had been investigated and resolved. SMW continued to be impressed by the HRA query log, and the fact that there was no re-editing opportunity after any HRA query had been run.

15. Overall SMW commented that his day had been, "very interesting and very good".

[REDACTED]

1 November 2011

VISIT OF SIR MARK WALLER, INTELLIGENCE SERVICES COMISSIONER: 17-18 OCTOBER 2011

[REDACTED]

Examination of s.94 Direction and Non-targeted Bulk Personal Data

11. The statutory part of the inspection being complete, Sir Mark looked at the s.94 Direction in respect of [REDACTED – name of CSP]. *The relevant official* described how samples of rich communications data had been obtained. SMW was interested in where the data was stored: being telephony communications data this was stored in *the relevant tool* along with a larger portion of CDRs obtained from RIPA 8(4) collection. SMW was interested in how access to this data was controlled (HRA justification), and how audits were performed and potential misuse might be found. There was some discussion of how far it might be reasonable to provide a report to SMW on this aspect when the majority of the communications data subject to these controls would be acquired in the course of warranted interception and therefore under Sir Paul's remit. Although SMW had agreed to oversee the s.94 data in response to GCHQ's request rather than any other driver, his interest was at least as much in monitoring of potential misuse as in the justification for acquiring the data. The questions in which he was interested were "what is the control system for access to operational data?", "are you checking for misuse?", "what is the process by which you check?", and "how have you responded to any incidents of misuse?"
Action: *The relevant official* to consider what would be a reasonable response to SMW's wish to have an annual report on audit of operational data (with particular regard to SMW's role on s.94 Directions).

12. SMW examined the [REDACTED – Name of dataset] dataset. The fact that it had led to 26 intelligence reports over the last year (although it was an ageing dataset) left him in no doubt as to its value. He asked whether we deleted datasets that the review panel did not judge worthy of retention (yes) and was pleased to hear that most of GCHQ's operational data is subject to a default data retention period of [REDACTED]. SMW also examined [REDACTED – Name of dataset]: he was left in no doubt of the CI requirements in the relevant location, but asked why there was no data in relation to British nationals [REDACTED]. SMW was again interested to know how we monitored potential misuse (though he noted that the risk of misuse was lower for a dataset that did not contain data relating to British nationals).

[REDACTED]

[REDACTED]
20 January 2012

Summary Filenote: Visit of Sir Paul Kennedy, Interception Commissioner, 13 December 2011

[REDACTED]

11. *The relevant official* provided some context to the role that Sir Paul had kindly agreed to fulfil on **Non-Targeted Bulk Personal Data.** The 2010 review initiated by Robert Hannigan had examined the acquisition and handling of this sort of data, much of which was not obtained under any form of legal authorisation. The Intelligence Services Commissioner had assumed a non-statutory role in overseeing nearly all the relevant datasets, but for the few (currently [REDACTED]) GCHQ datasets that were obtained under RIPA authorisation, Sir Paul had agreed to examine them. *The relevant official* also explained the role of the GCHQ Retention Review Panel. On this occasion Sir Paul had chosen to examine [REDACTED – Name of dataset] and he scrutinised the form completed by the panel after their review of this dataset. He was content that a justification had been properly made out for the retention of the dataset.

[REDACTED]

[REDACTED]

11 May 2012

Filenote for Visit of Intelligence Services Commissioner, 19-20 March 2012

[REDACTED]

Other topics including non-statutory inspection

11. [REDACTED] He was content with the three bulk personal datasets he had selected. He was also content with the Section 94 Direction, although would like to have seen a more explicit assertion that GCHQ would only search the data for its lawful purposes, in addition to the words on proportionality that appear in the 'Legal Issues' section.

12. *The relevant official* briefed that he was preparing a first draft of the report on GCHQ's practices of auditing access to operational data. He stressed that most of GCHQ's data holdings did not qualify as 'bulk personal data' according to the terms of the Prime Minister's letter to the Commissioner, and that data which did fall within the definition would not usually have been acquired by GCHQ itself but by an OGD or another Agency. However, GCHQ's operational data was usually treated in such a way that queries had to be supported by an HRA justification, and the logs of these queries were audited. The Commissioner received a briefing from the IT *services* team on how audit searches were continually developing, and how numerous false positives had been identified and discounted. He received clarification that the team had found no instances of deliberate misuse. [REDACTED] The formal report on auditing is to be sent to him in due course.
Action: *The relevant official* **to send report on auditing of operational data.**

[REDACTED]

[REDACTED]
9 July 2012

Summary Filenote: Visit of Sir Paul Kennedy, Interception Commissioner, 17 April 2012

[REDACTED]

7. The Commissioner inspected paperwork associated with a **non-targeted bulk personal dataset** acquired under the authority of an interception warrant. This dataset, [REDACTED – Name of dataset], contained financial data. The Commissioner noted that the dataset potentially had an application to Serious Crime as well as to Counter-Terrorism. He clarified how *the main corporate BPD tool* would run queries across multiple datasets and that results would only be obtained in the event of a match. He commented that holding data at all had implications for Human Rights, but this issue was not acute until the point of query. The Commissioner also checked that the retention period of [REDACTED] could be justified and was satisfied to hear that financial data was [REDACTED] and could continue to be useful for such a period. He noted that GCHQ, given its mission, did not hold much data in respect of UK citizens.

[REDACTED]

[REDACTED]

2 January 2013

Filenote of Inspection Visit by the Intelligence Services Commissioner, Sir Mark Waller, 4-5 December 2012

[REDACTED]

Direction under s.94 of the Telecommunications Act [REDACTED – name of access] – non-statutory

23. The Commissioner pointed out that the application for the direction was on the basis of a one month pilot but we were still getting access to the data some years on. It was explained that there is no legal requirement to renew such a direction and indeed there was no provision for doing so in the Act. GCHQ will however resubmit for a direction if a company changes its name. We also undertake to review the requirement every 6 months and write to the company concerned to inform it that we continue to require the data.

24. The Commissioner appeared reassured that the data could only be queried if an HRA justification has been supplied by the querying analyst. He sought and was provided with clarification on the type of reporting that was derived from this data and he concluded the session by commenting that it had been "very interesting".

Non-targeted Bulk Personal datasets – non-statutory

25. [REDACTED – name of dataset] – The Commissioner queried what safeguards were in place to prevent analysts from querying against non-targets in an inappropriate way. He was provided with assurances in respect of the need for HRA justifications for every query. He had spotted that the [REDACTED – name of dataset] dataset, of which [REDACTED – name of dataset] is a part, was overdue for review. **Action 12:** *Mission Policy and Legalities team* to check that this dataset is on the agenda for the 14 December review panel. **Action complete.**

26. The Commissioner had not realised that he had inspected [REDACTED – name of dataset] previously (even though a list of previous choices had been included as an annex to the choice letter and his former PS had been alerted to this in advance of the visit). **Action 13:** *Mission Policy and Legalities team* to come up with a new method of alerting the Commissioner to previous selections in the choice letter for the next inspection.

27. [REDACTED – name of dataset] - The Commissioner had spotted the discrepancy between the date of the DAA authorising the acquisition of the data and the setting of a [REDACTED] retention period and the date of the data destruction. It was explained in the briefing that this was because there had been significant delays in getting the data into the building and therefore the [REDACTED] retention period

had not in fact been exceeded. The Commissioner suggested that it would have been useful to have had this highlighted in the table in the choice letter. **Action 14:** *Mission Policy and Legalities team* to consider what additional information might be added to the spreadsheet detailing these datasets for selection. This should as a minimum include highlighting those that the Commissioner has inspected before (and when), those that are new since the last inspection and those that have been deleted since the last inspection. It was suggested that some type of colour coding might be helpful.

28. [REDACTED – name of dataset] - The Commissioner questioned the absence of a DAA form and it was explained that this dataset had arrived in the building before the introduction of the DAA process but had appeared on the spreadsheet because it had been available during GCHQ's stocktake of its holdings of bulk personal data during the Hannigan Review. However, because the data had not been acquired via a DAA, the requirements to track its progress and report its destruction to Mission Policy were not followed. This had been addressed by the compilation of the form presented to the Commissioner for inspection, which would also form the corporate record of the history of the data in GCHQ. The Commissioner was assured that this should not happen with any datasets that have been subject to the DAA process.

Action 15: *Mission Policy and Legalities team* to go through the master list of non-targeted bulk personal datasets and identify if there are any further datasets that are not fully accounted for.

[REDACTED]

Audit session

34. The Commissioner described the Audit report that had been sent to him the week before as "very helpful". He confirmed that he does not need to see the individual documents produced by the *IT services* team. He remains keen that we stay alert to the possibility of abuse of access to data. He was interested in to what extent staff were aware of the potential consequences of any abuse. He was informed of the various guidance documents that are available to staff. During his next visit he would like to see copies of the following:

- Conduct and discipline documents relating to abuse of IT access or systems
- A copy of the Civil Service Code
- Compliance documentation relating to access to systems or data
- *System operating procedures* (a few samples will probably suffice).

Action 17: *Mission Policy and Legalities team*.

[REDACTED]

Table of Actions					
	Action	**Owner**	**Deadline**	**Completed**	**Para ref**
	[Redacted]				
12	Check that the [REDACTED – name of dataset] dataset is on the agenda for the 14 December review panel.	*Mission Policy and Legalities team*	14/12/12	04/12/12	25
	[Redacted]				
14	Consider what additional information might be added to the spreadsheet detailing the non-targeted bulk personal datasets for selection.	*Mission Policy and Legalities team*	Next choice letter		27
15	Go through the master list of non-targeted bulk personal datasets and identify if there are any further datasets that are not fully accounted for.	*Mission Policy and Legalities team*	Next choice letter		28
	[Redacted]				
17	Provide copies of the following for Commissioner's next visit: • Conduct and discipline documents relating to abuse of IT access or systems • A copy of the Civil Service Code • Compliance documentation relating to access to systems or data • *System operating procedures* (a few samples will probably suffice)	*Mission Policy and Legalities team*	Next visit		34
	[Redacted]				

534

[REDACTED]

19 June 2013 filenote updated with status of actions as at 6 February 2014

Filenote of Inspection visit by the Intelligence Services Commissioner, Sir Mark Waller, 4-5 June 2013

[REDACTED]
The actions from this inspections are available in tabular form in Annex B.

Non-targeted bulk datasets

25. The Commissioner explained that in his inspection of these datasets he was looking to see if GCHQ is justified in holding the data, where the data is going to go, who has access to it and any potential for misuse. The Commissioner was taken through the three datasets he had selected, all three of which had been deleted. The Commissioner had no major queries in relation to the selected datasets and commented that we had shown ourselves to be handling data responsibly by deleting the [REDACTED – name of dataset] dataset when it became evident that it was not going to be loaded onto corporate systems. He queried briefly why the [REDACTED – name of dataset] data had been retained until January 2013 when the original plan was to delete it in October 2012, but he was satisfied with [REDACTED – name of operation] being cited as the reason for the longer retention.

Section 94 Direction

26. The Commissioner explained that he was particularly interested in the necessity and proportionality of GCHQ acquiring data under s.94 of the Telecommunications Act and he was interested in the possibility that the data we acquire under this authority includes information that is private. He asked that, when seeking a direction, the submission should include more specific information covering privacy safeguards and providing further evidence that the expected intelligence gains outweigh the level of intrusion.

Action 12a: *Ensure that future submissions seeking s.94 Directions cover the level of intrusion into privacy, risk of collateral intrusion and associated proportionality considerations and safeguards.*

Action 12b: *Update guidance to advise staff of the type and level of detail to include under these headings in submissions seeking new s.94 Directions.*

Access to systems: safeguards, policies, controls and guidance

27. Hd/Compliance took the Commissioner through a variety of documentation including the Civil Service Code, GCHQ's Behaviour and Conduct Policy, and Security Operating Procedures for *the corporate IT systems* to show him how staff

were alerted to their responsibilities in relation to access to operational data. Although he was happy with the guidance and documentation he had been shown, the Commissioner said that he wants to be presented with an audit report at each inspection setting out what the system auditors have found during their audits and the outcomes of any resultant investigations. He would also like a briefing from the Audit team included in the programme.

Action 13a: *Provide an IT Systems Audit report at each inspection.*

Action 13b: *Include a session on IT Systems Audit in each inspection programme.*

[REDACTED]

Annex B - ACTIONS FROM INTELLIGENCE SERVICES COMMISSIONER INSPECTION OF GCHQ, 4-5 JUNE 2013

No.	Action	Owner	Deadline	Status (RAG) and notes	Para
	[REDACTED]				
12a	Ensure that future submissions seeking s.94 Directions cover the level of intrusion into privacy, risk of collateral intrusion and associated proportionality considerations and safeguards.	*Mission Policy and Legalities team*	Next s.94 Direction	Complete. Extension of s.94 Direction in relation to [REDACTED - name of company] has a new heading to cover this requirement.	26
12b	Update guidance to advise staff on the type and level of detail to include under these headings in submissions seeking new s.94 Directions (e.g. filtering, discarding on non-intelligence related information etc).	*Mission Policy and Legalities team*	End July 2013	Complete.	26
	[REDACTED]				

S34

[REDACTED – name of database]

23 December 2013 filenote updated with status of actions as at 6 February 2014

File note of inspection visit by the Intelligence Services Commissioner, Sir Mark Waller, 10-11 December 2013

[REDACTED]
The actions from this inspections are available in tabular form in Annex B.

Key points

[REDACTED]

- Commissioner remains concerned about the potential for rogue activity on GCHQ systems resulting in intrusion into private data.

[REDACTED]

Operational update/lunchtime discussions

[REDACTED]

6. The Commissioner was briefed on the document that has been prepared for Sir Anthony setting out details of those computer systems which hold data that has been obtained by means of interception under Part I of RIPA. Sir Mark requested a counterpart document covering those systems which handle data obtained under the authorisations which fall under his oversight – ISA s.5, ISA s.7, CHIS, DSA, Directions under s.94 of the Telecommunications Act, and non-targeted bulk personal datasets not obtained by means of interception under RIPA Part I.

> **Action 1:** GCHQ to provide a document setting out relevant details of those systems which handle data obtained under ISA or otherwise fall under the IS Commissioner's oversight.

[REDACTED]

Section 94 Direction

39. The Commissioner inspected the s.94 direction issued in respect of [REDACTED – name of company]. D/D LA reminded him of the background to s.94 directions. As s.94 directions have no expiry date, it was explained that the requirement for the data was reviewed every six months and the company informed of the continuing requirement or a decision to discontinue the provision of the data, as appropriate. Some companies prefer to be informed verbally rather than in writing as they do not have storage facilities for highly classified documents.

40. Sir Mark requested that confirmation of the outcome of the latest review be included in the reading pack for selected s.94 directions. This should either be a copy of the letter sent to the company or a note of when the verbal confirmation of the continuing requirement was made to the company.

> **Action 11:** Add to checklist that latest confirmation of continuing requirement is to be included in the paperwork for selected s.94 directions.

> **Action 12:** Add to checklist that a copy of the letter to the Foreign Secretary confirming the outcome of the s.94 direction six-monthly review is to be included in the Commissioner's inspection reading pack.

Non-targeted bulk datasets

41. The Commissioner inspected the **[REDACTED – name of dataset]** and **[REDACTED – name of dataset]** datasets. He was satisfied with the business cases for obtaining both sets of data. He noted that there was an outstanding requirement for a strengthened business case for the retention of [REDACTED – name of dataset] to be put to the review panel by the end of October. He was assured that, as the business case had not yet been received, the dataset had been quarantined in *the main corporate BPD tool* and would not be made available again to analysts without the approval of the review panel.

42. At the request of Sir Anthony May, Sir Mark had been provided with information relating to the non-targeted bulk personal datasets obtained via interception, so that he was aware of these datasets which come under Sir Anthony's oversight. Sir Mark was asked if he required any further information on these datasets but he indicated that he was happy with what had already been provided.

[REDACTED]

Annex B - ACTIONS FROM INTELLIGENCE SERVICES COMMISSIONER INSPECTION OF GCHQ, 10-11 DECEMBER 2013

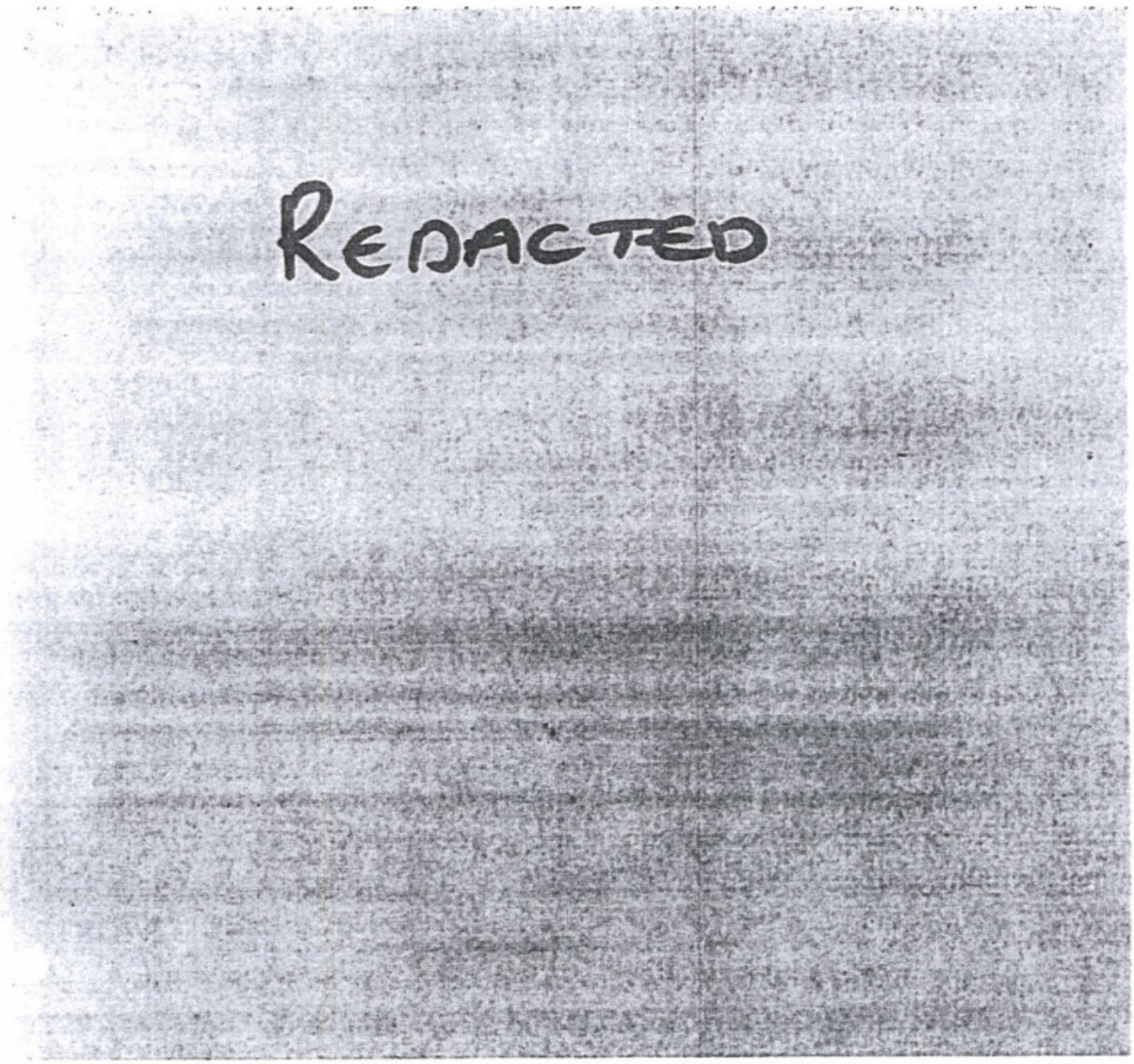
No.	Action	Owner	Deadline	Status (RAG) and notes	Para
	[REDACTED]				
	[REDACTED]				
11	Add to checklist that latest confirmation of continuing requirement is to be included in the paperwork for selected s.94 directions.	*The relevant official*	Future inspection visits	Action Complete - This requirement now appears in the inspection visit preparation checklist.	40
12	Add to checklist that a copy of the letter to the Foreign Secretary confirming the outcome of the s.94 direction six-monthly review is to be included in the Commissioner's inspection reading pack.	*The relevant official*	Future inspection visits	Action Complete - This requirement now appears in the inspection visit preparation checklist.	40
	[REDACTED]				

[redacted]

Intelligence Services Commissioner

SIA Inspection Report 2014

Organisation	Government Communications Headquarters
Dates	List: 6 May 2014 Inspection: 27 and 28 May 2014



[redacted]

Annex A: Bulk Personal Data

Oversight of bulk personal data is divided into the intelligence services' (1) holding of bulk personal data, and (2) use of bulk personal data.

Government Communications Headquarters

Bulk Personal Data	
Total number available for inspection	[redacted]
List broken down as	Non-Targeted Bulk Datasets • Commercial • Communications • Financial • ID • Travel The list sets out • a description of the dataset • the source of the dataset • when it was last reviewed by the Commissioner [redacted] datasets were new [redacted] had been deleted since the last inspection [redacted] had been reviewed previously (since 2001)
Selected	3

Section 94 Directions

There continues to be [redacted] s94 directions [redacted] of which have been reviewed previously. 1 was selected for Inspection which had not previously been reviewed.

The list set out

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

Bulk Personal Datasets General Discussion

Bulk personal data comprises only a small proportion of the operational data held by GCHQ and is sometimes held in databases alongside data from other sources. Access to these databases is restricted to individuals who have demonstrated an operational requirement to use that data.

The Commissioner looked in more detail at three specific data sets held and challenged GCHQ to justify their retention.

[redacted]

[redacted]

[redacted] is a commercial data set containing [redacted] as a standalone date set. GCHQ make it available to analysts who work on the [redacted] programme.

[redacted] is a communications data set containing publicly available subscriber data but GCHQ acquired a full copy covertly. This is available in [redacted] and [redacted] (which is an older database).

[redacted] is a financial data set containing financial data with very strict rules of access. It is not used very often but it is a supporting data set. It has probably come to the end of its useful life so will most likely be deleted soon.

Having:

1) reviewed the retention of these three data sets
2) considered GCHQ's internal review process to assess the acquisition, retention and deletion of data sets

the Commissioner was content that GCHQ's holding of personal bulk data sets was both necessary and proportionate.

Misuse of Data and Protective Monitoring	
Breaches	
Detail	Assessment
3 minor breaches	These did not relate to bulk personal data.
General Discussion	
The Commissioner was briefed on the safeguards in place within GCHQ to protect all operational data held and restrict access to it. Access to data is restricted to individuals that have demonstrated an operational requirement to use the data and their access can be corroborated through their unique logon ID. Prior to collecting data, the analysts must have a target record in place (in [redacted], the target knowledge base) which contains references to the PIC process and statutory purpose (eg national security). This target must contain an HRA justification demonstrating why the target is expected to lead to intelligence meeting a requirement outlined in the Mission Mandates. This HRA justification must be reviewed annually – without this annual review the record becomes dormant and no data can be collected. Once the target record is in place data may be collected but each request to access that date must be accompanied by an individual HRA justification entered into the	

[redacted]

[redacted]

system where the collected data is stored.

Training Staff

There are two levels of core legalities training. The first part consists of mandatory training for all staff, integrees and contractors with access to GCHQ's IT systems and provides a missions legality overview and the rules that everyone should know including:

- UK Legal Framework)
- Policy framework
- Oversight
- Ethics

This takes approximately one hour to complete and has a pass or fail test at the end.

The Commissioner suggested that the course ought to highlight that protection of privacy applies to everyone.

The second part is advanced training that is mandatory for staff in roles that give them access to operational data. Different modules are tailored for analyst reporters or for those staff working on capability development or access collection.

Vetting Staff

All staff in GCHQ must hold developed vetting clearance (including contractors). This is a rigorous process and the minimum standards are set out in the Cabinet Office led security policy framework. Unlike government, each intelligence service conducts its own vetting and having been cleared by this process a high level of trust can be assumed. Clearance does not pass from one organisation to another and is checked with the host organisation for any visitor.

Justification for Targeting

In order to run a query the analyst must complete a pop up screen containing three fields:

- the statutory purpose (eg national security)
- a reference link to the Priorities for Intelligence Collection (PIC) requirement
- free flow text to demonstrate the necessity and proportionality of the action – the "HRA justification".

Incident Management

[redacted]

[redacted]

GCHQ protects all operational data with increasingly sophisticated computer monitoring. This monitoring provides tip-offs for further investigation. There is a team of [redacted] people in the Incident Security Team involved in protective monitoring and subsequent investigation. The automated searches are very technical so the auditors also need to be technical so they can check query terms for example. About [redacted] arise each day but only a small amount of these require significant further investigation – most are false positives.

The Team audit access to data holdings. This will include:

- automated monitoring for issues such as short HRA justifications
- automated searches for key words or phrases such as celebrity names
- manual random monitoring
- targeted monitoring following reported concerns about unusual actions or behaviour which managers are required to look out for.

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

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

Bulk Personal data is only a proportion of all operational data. The three minor breaches recorded did not relate to Bulk Personal Data. It was important for the Commissioner to have the complete picture so as to be able to assess the effectiveness of the monitoring system. He would like to be able to publicise figures in his open report.

HRA Audit

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

The Commissioner commented that this monitoring system seemed a good system. It is not an absolute guarantee but nothing could be absolute. MI5 and SIS treat any inappropriate access of personal data as a major breach and recommended that GCHQ discuss with

[redacted]

[redacted]

colleagues across the SIA to ensure consistency in approach.

He asked about auditing of [redacted] and was informed that this was not done yet but GCHQ have plans to do so. [redacted] is monitored three times a year with approximately 3% of records being reviewed on each occasion, therefore 10% of records in each year. [redacted], which contains the product of RIPA and ISA activity, is audited twice yearly.

The Commissioner encouraged the auditing of [redacted] which he is keen to see done.

Compliance Guide

GCHQ have a compliance guide which was shown to the Commissioner in electronic form. This document provides the safeguards which apply to any personal data retained and it is approved by the Foreign Secretary. The Commissioner requested an opportunity to go through the guide in more detail in [redacted].

Oversight

The majority of GCHQ's operational data is obtained from interception of international communications under authority of a RIPA 8(4) warrant. A smaller amount comes from RIPA 8(1) UK communications and CNE or other operations conducted under ISA with an even smaller portion collected under RIPA Part II authorisations. GCHQ offered to provide the figures but very few analysts have access to bulk personal data and many will go through their career without ever having had access. However, the protective monitoring covers all aspects of data held by GCHQ and GCHQ's record of security incidents concerning potential misuse of operational data do not capture the type of authorisation the data was acquired under.

The Commissioner believes that it would be helpful if he looked at misuse of data generally without limiting this to bulk personal non intercept data. This would collate in one place all aspects of misuse of GCHQ IT systems. However, he understood that clarity was required to determine if the Interception of Communications Commissioner already had an oversight responsibility in relation to intercept product to avoid duplicate reporting to the Prime Minister.

Recommendations
The Commissioner would like to see all cases of misuse of data or systems made available

[redacted]

[redacted]

to him since his last inspection with the case detail and outcome/assessment.

It was important for the Commissioner to have the complete picture so as to be able to assess the effectiveness of the monitoring system. He would like to be able to publicise figures in his open report.

The Commissioner requested an opportunity to go through the Compliance Guide in more detail in [redacted].

The Commissioner is keen to see [redacted] audited for the purpose of protective monitoring.

[redacted]

Table of gists for 'doc 15' SIA inspection report 2014

Page 3, line 5, replace with: 'the main corporate BPD tool' and 'its predecessor'

Page 6, line 2, replace with: 'the main corporate BPD tool'

Page 6, line 3, replace with: 'the target knowledge base'

Page 6, line 5, replace with: 'the relevant database'

Page 6, line 6, replace with: 'the main corporate BPD tool'

Page 6, line 10, replace with: 'GCHQ's London offices'

Page 7, line 6, replace with: 'GCHQ's London offices'

Page 7, line 7, replace with: 'the main corporate BPD tool'

548

[REDACTED – name of database]
24 November 2014

SUMMARY FILE NOTE: VISIT OF SIR PAUL KENNEDY, INTERCEPTION OF COMMUNICATIONS COMMISSIONER, 21-22 OCTOBER 2014

3. The Commissioner was pleased that implementation of the recommendation to reduce the retention period for communications data (Recommendation 5 from the October 2013 inspection) is almost complete. He asked us to consider on a regular basis whether the retention period could be reduced further. He asked for further details on how the cases for exceptional retention would work and it was explained that a written business case would need to be submitted to D/D *Mission Policy* who would make the decision on whether longer retention would be appropriate.

IOCCO Action 1: Jo and *IOCCO official* agreed to a request that IOCCO provide a paragraph that could be included in communications to analysts explaining the reasons behind the reduced retention period.

Recommendation 1: GCHQ to conduct a regular profiling exercise to test whether related communications data retention periods are justified.

[REDACTED]

[REDACTED – name of dataset] **Dataset**

21. The Commissioner was provided with a recap of how bulk personal data is handled and overseen within GCHQ. He was taken through the data acquisition and review process. *The relevant official* then provided a briefing on the history of the dataset, which was acquired as a continuous feed between 2011 and November 2013. [REDACTED] The Commissioner asked how the data is used and it was explained that this type of data can be very good for *meeting specific finance related intelligence requirements*. The Commissioner appeared content.

[REDACTED – name of dataset] **dataset**

22. The Commissioner was briefed on the use of this dataset, which is generated from interception obtained under [REDACTED – name of warrant] and associated subscriber checks, and how it is used to discriminate between targets and not-targets so that non-targets can be excluded from our investigations more promptly and thereby unnecessary intrusion into their privacy can be avoided. As some details are kept on parties not of intelligence interest, the Commissioner was interested in who can access the data. He was reassured when he was told that the file is password protected and only 10 named individuals within the *relevant* team have access.

GCHQ's Filenote of Intelligence Services Commissioner's inspection of GCHQ – 21-23 April 2015

[REDACTED]

20. The inspection then moved onto Bulk Personal Datasets. It was explained by *the relevant teams* that because of the complexity of the data the recently acquired [REDACTED – name of dataset] dataset was still being processed and had not yet been ingested into standard GCHQ analytical tools. The tight controls around access to the data were explained and it was anticipated that the data would only ever be accessible to a small number of analysts because of its sensitivity.

21. [REDACTED – name of dataset] was a dataset that had been acquired for a limited-time trial to investigate what value GCHQ might gain from the acquisition and analysis of internet economy data (in an attempt to replace some of what had been lost from GCHQ's RIPA 8(4) interception accesses due to the growth of ubiquitous encryption). [REDACTED]

[REDACTED]

36. The next session concerned the [REDACTED – name of dataset] Bulk Personal Dataset, which contains data 'scraped' from the internet and which was being stored in isolation from other operational data, with very limited access while GCHQ decides where to store it and how to set access limits in the longer term. This prompted Sir Mark to reflect dissatisfaction with any organisation that may acquire data but is then not able to exploit it in a timely manner. He was reassured that this is rarely the case for GCHQ, but the following action was agreed to offer him further reassurance on this topic in future.

> **Recommendation/action 11:** GCHQ to add several columns to the table of extant bulk personal datasets included in the choice letter covering: when each dataset was acquired, when it was ingested into corporate systems, and when it was last reviewed by the panel.

[REDACTED]

Filenote of Intelligence Services Commissioner's inspection of GCHQ – 21-23 October 2015

[REDACTED]

Day 2 afternoon (ISA Section 5 warrantry and Bulk Personal Datasets)

[REDACTED]

28. Due to scheduling difficulties, the next session covered the first of the selected BPDs: Non-targeted Bulk Personal Dataset: [REDACTED – name of dataset].

[REDACTED]

31. We then returned to BPDs:[REDACTED – name of dataset]. Sir Mark enquired about how limited user access was to this set of data. [REDACTED]

32. After a further period of reading time, Sir Mark moved onto the next BDP: Non-targeted Bulk Personal Dataset: [REDACTED – name of dataset], which contains [REDACTED] Having read the paper work provided, Sir Mark wanted to track back over the timeline, as there were gaps where the internal process and paperwork had not been properly completed. He expressed concern that there might be other examples and would like to be reassured that this was just a rouge example. The 2010 BPDAR was unsigned and he could see no evidence that this BPD had been brought to the BPD panel between 10/13 and 9/15. Since the briefer recently took on responsibility the [REDACTED – Name of Dataset] is now properly managed and deleted. *Relevant official* assured Sir Mark that new staffing would allow us to work through all BPD's to track if there were other cases. Sir Mark was content for any other cases to be brought to his attention at inspection, not as they occur or are discovered.

    Recommendation/Action 12: *Mission Policy and legalities team* to review all BPD paperwork to ensure no slip ups on documentation – and highlight any cases with slip ups on the BPD section of the choice letter for next inspection.

    Recommendation/Action 13: Sir Mark to receive minutes of BPD panel meetings (both latest and preceding minutes) with the Choice letter for each inspection.

33. Non-targeted Bulk Personal Dataset: [REDACTED – name of dataset] *is a biographical dataset*. Sir Mark was informed that this is now being removed from *the main corporate BPD tool* as the system is being decommissioned. The team have recently received permission to put this data onto *a relevant system*.

[REDACTED]

35. The final BPD inspected is one that was separately raised to Sir Mark to explain an error in our internal handling. [REDACTED - name of dataset][REDACTED]

36. Sir Mark commented that this was in a different category to other work we do and to other BPDs. Defence of employees was justifiable and it made use of a capability we possess. It was right to go through the BPDAR process but there was no question about it being the right thing for us to do, including sharing with our partners. This was a defensive not offensive activity. The internal process does need to be followed but he had no doubt that it was right to protect partners in this case. There should continue to be cross-agency education on what should be put onto public profiles.

37. The last session on Day 2 was an Update on errors and protective monitoring of operational systems. Protective Monitoring (PM) was covered first. *Sir Mark was provided with an update since his April inspection.* He commented that the new system was very good and that the new anomaly detection was exactly what one wants. Sir Mark was keen to see parallel sanctions across the SIA.

38. Sue Cobb asked why PM did not come under BPDs when it involved working with large amounts of personal staff-related data. Sir Mark stated that PM was clearly part of his remit under BPD. *The Deputy Director Mission Policy* commented that the situation may become clearer with the fuller scope of the new IPB. *Relevant official* would like a clear differentiation between operational BPD and our own PM in external communications, to avoid any misleading impressions.

39. Post inspection GCHQ clarified its understanding of the status of its Protective Monitoring data as follows:

> GCHQ does not regard Protective Monitoring data as BPD because it does not require or use Protective Monitoring data in the exercise of its functions under the ISA. Crucially, GCHQ does not use such data for an intelligence purpose. GCHQ uses the data to monitor the use by staff its of systems. GCHQ regards and treats such data as corporate data. It is of the same nature as data derived and used by any organisation that seeks to monitor the conduct and behaviour of its own staff for a legitimate organisational purpose (eg. to identify and prevent fraud or misconduct). The draft Investigatory Powers Bill clarifies this issue at clause 150(1).

[REDACTED]

[REDACTED]

[REDACTED]

553

[REDACTED]

Recommendations/Actions from October 2015 Inspection

Recommendation no. and summary	Details	Status
[Redacted]		
12: BPD paperwork	Compliance team to review all BPD paperwork to ensure no slip ups on documentation – and highlight any cases with slip ups on choice letter for next inspection.	Ongoing
13: BPD panel meeting minutes	Sir Mark to receive minutes of BPD panel meetings (both latest and preceding minutes) with the Choice letter for each inspection	Ongoing
[Redacted]		
15: Wording for BPDs in Annual report	*Relevant officials* to discuss final wording on BPDs and Protective monitoring with Sir Mark prior to the Annual Report being issued to prevent any public misunderstanding	Ongoing
[Redacted]		

[REDACTED]

554

[REDACTED – name of database]
13 May 2015

SUMMARY FILE NOTE OF INTERCEPTION INSPECTION BY THE INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE (IOCCO), 6 MAY 2015

[REDACTED]
Key points

- [REDACTED]
- **There are issues around the ownership of financial datasets and the failure to load many datasets onto systems where analysts can make use of them; these are to be addressed at the next Bulk Personal Data Retention Review (paras 7-11);**
- [REDACTED]
- **Also discussed:**
- [REDACTED]
    - **Oversight of s.94 Directions (para 62)**
- [REDACTED]

Introduction

1. IOCCO Chief Inspector Jo Cavan and Interception Inspector *IOCCO official*, conducted a formal inspection visit of GCHQ on 6 May 2015, on behalf of the Interception of Communications Commissioner, Sir Anthony May. [REDACTED]

[REDACTED]

Inspection element of the visit

[REDACTED – name of dataset] dataset

7. Although there was a briefing on the specific nature of the [REDACTED – name of dataset] dataset, this session developed into a wider discussion of GCHQ's acquisition and use of financial data and what happens when other agencies are provided with copies of the datasets. Jo Cavan was interested in what happens at retention reviews when data has been shared and whether data is deleted by all parties at the same time. Currently each agency makes retention decisions independently but this is likely to change as we move towards a model of a single holding of data with shared access from across the SIA, a feature of the *relevant* programme.
The Inspectors requested a more general briefing at the next inspection visit on the SIA trilateral approach to handling of bulk personal datasets. Jo Cavan plans to liaise with Sir Mark Waller, who oversees the vast majority of GCHQ's bulk personal datasets, to ensure a common approach between the two Commissioners.

GCHQ Action 1: Briefing on the SIA trilateral approach to handling of bulk personal datasets to be included in next inspection visit (or new Commissioner's familiarisation visit)

8. The discussion also covered the problems with the ownership of financial datasets which had been covered in the briefing notes. D/D *Mission Policy* explained that there had not been as much progress as expected with this issue and that the decision had been taken to suspend acquisition of financial datasets until this is fully resolved and GCHQ's longer-term strategy for the acquisition and use of financial data has been agreed.

GCHQ Action 2: An update on GCHQ's strategy for the acquisition and use of financial data to be provided to IOCCO, either at the next inspection visit or in writing.

[REDACTED – name of dataset] dataset

9. The Inspectors were briefed in the nature of the dataset *of this* target that make information of this type so valuable to analysts. [REDACTED] Jo Cavan questioned why this was handled as a bulk personal dataset. It was explained that a lot of filtering had been applied during the compilation of the dataset and therefore it was likely that most of the individuals listed would be subject to a reasonable degree of intrusion.

10. Jo also queried why the data had been collated in this way rather than being entered into *the target knowledge database*. Consideration had been given to this at the time of its compilation but it was decided that, because not all of the listed individuals are current targets, it was not proportionate to record their details in the target knowledge base. It was also not an efficient use of analysts' time to record all of the details individually when many of the selectors would not be targeted.

11. Jo asked who has access to the data and how it is used. This exposed a longstanding problem with uploading datasets into *the main corporate BPD tool* which has meant that GCHQ holds a number of datasets that cannot be accessed by analysts. This issue will be looked at again at the next review panel meeting.

GCHQ Action 3: BPD Review Panel to consider the problems with uploading BPD into *the main corporate BPD tool*.

[REDACTED]

Other issues

Oversight of s.94 Directions

62. There was some discussion of s.94 authorisations in the context of Sir Anthony's oversight. IOCCO is holding back from inspecting s.94 authorisations until more resources have been recruited but at this stage Jo is querying why the approached taken by GCHQ and MI5 are so different. D/D *Mission Policy* said that this was because the approaches were aligned to each agencies respective primary activities in relation to comms data – MI5 obtains the bulk of its CD via Part I Ch II requests whereas the vast bulk of GCHQ's communications data is obtained via 8(4) interception. Our approaches to acquisition and use of data obtained under s.94 merely reflect our different approaches to intelligence work.

[REDACTED]

From: [REDACTED name of sender]
Sent: 14 April 2015 18:21
To: [REDACTED –name of recipient]
Subject: Quick download on IOCCO Reading Day

Classification: [REDACTED]

[Redacted]

We will need to cover both datasets in the programme. Jo is somewhat baffled by the history of [REDACTED – name of dataset], the less than impressive paper trail and the issue of ownership of financial datasets. She was also interested to note that the data is shared with SIS and wanted to know whether they had access to our copy of the data or had a copy of their own. She also asked whether, in cases where partner have access to the data they have any input to the review process.

With [REDACTED – name of dataset] she didn't feel that the source and nature of the data was made particularly clear and would like to talk to the data owners. What does semi-targeted mean? Is the dataset of sufficient volume to qualify as as BPD. If it is all target-related info why is it not in the *target knowledge database*?

[Redacted]

[REDACTED – name of database]
4 November 2015

FILENOTE OF INSPECTION VISIT (READING DAY) BY THE INTERCEPTION OF COMMUNICATIONS COMMISSIONERS OFFICE (IOCCO) INSPECTORS, 3 NOVEMBER 2015

[REDACTED]

s.94 Review

11. With the arrival of the two new interception inspectors IOCCO is now in a position to conduct its planned review of the use by the intelligence agencies of directions under s.94 of the Telecommunications Act. *IOCCO official* has been tasked with conducting this review before the end of February so that his conclusions can be covered in the next six-month Commissioner report. As *the relevant official* is the resident expert on s.94 *IOCCO official* will arrange to speak to him in the next few weeks. I have asked to attend the session so that I can benefit from the knowledge harvest.

> **Action:** *the relevant official* to provide IOCCO with information in respect of the s.94 review.

Bulk personal datasets

12. As Jo has agreed with Sir Mark Waller that he should assume oversight of all Bulk Personal Datasets, the inspectors did not examine the paperwork associated with [REDACTED – name of datasets], although Jo said that they would continue to consider whether the s.15 safeguards were being applied more generally to BPDs collected under an interception warrant. I explained that there were some reservations about whether datasets derived from interception should be transferred to Sir Mark. As it was late in the day, Jo asked that these reservations be conveyed to her either by email or telephone when she was back in the office.

> **Action:** *the relevant official* to email/phone Jo to discuss oversight of BPD obtained via interception.

[REDACTED – name of database]
23 December 2015

SUMMARY FILE NOTE OF INTERCEPTION INSPECTION BY THE INTERCEPTION OF COMMUNICATIONS COMMISSIONER'S OFFICE (IOCCO), 26-27 NOVEMBER 2015

[REDACTED]
Key points

[REDACTED]

- **Inspectors now understand and appear to accept how and why GCHQ's use of s.94 directions differs from MI5's approach; IOCCO formal review of GCHQ's use of s.94 directions to be completed over the next 2 months; findings to be included in Annual Report (paras 21-31);**

[REDACTED]

Introduction

1. IOCCO Chief Inspector Jo Cavan and Interception Inspectors [REDACTED – IOCCO official names], conducted a formal inspection visit of GCHQ on 6 May 2015, on behalf of the Interception of Communications Commissioner, Sir Stanley Burnton. Although he has taken up office Jo felt that Sir Stanley would benefit from a familiarisation visit to GCHQ before taking part in one of our inspections. The Inspectors had previously selected [REDACTED] items for inspection (a combination of warrants, authorisations, end product reports based on privileged material and datasets, though, in the event the datasets were not examined). The paperwork associated with these selections had been examined earlier in the month during a combined reading day and familiarisation visit[1]. The inspectors requested further discussions on five of the warrants/authorisations they had examined and requested sessions on partner compliance and audit and an opportunity to sit with analysts to see how they conduct queries against data obtained via interception. As IOCCO is in the process of conducting a review of the use of s.94 directions a session on GCHQ's use of these authorisations and the data obtained under them was also included in the programme.

[REDACTED]

GCHQ use of s.94 Directions

21. *The relevant official* provided a background briefing on GCHQ's use of Directions issued under s.94 of the Telecommunications Act 1984.

22. GCHQ merges the s.94 data with CD obtained under our 8(4) warrants to enable analysts to query the full range of data. The analyst will not necessarily be

[1] A file note on the outcome of the reading day can be found at Reference A.

aware that they are interrogating s.94 data. The data is accessed via the same tools as RCD collected under 8(4), all of which require the provision of an HRA justification to access the data.

23. MI5 adopted a different model for its [REDACTED – name of dataset] data whereby the data is retained by the CSP and analysts submit RIPA Part I Chapter 2 CD requests to access the data. Sir Swinton Thomas was consulted about the differing approaches and he was content that both models were compliant with Article 8 of the ECHR.

24. Had GCHQ been forced to adopt the MI5 model, either all CD queries would have had to be authorised in a similar way or the data would have had to be skimmed off into another database, which would have reduced its analytic value significantly.

25. Jo said that she had, until the previous week, been unable to access the previous Commissioners' files but would look in them for any record of Sir Swinton's position on this. D/D *Legal Affairs* offered to provide a copy of our records of the correspondence on this.

Action 4: D/D *Legal Affairs* to provide IOCCO with copies of the correspondence with Sir Swinton Thomas on the subject of handling s.94 material.

26. The replacement capabilities on the IP Bill are focused on the acquisition of CD and this will be done under a bulk acquisition warrant (Part 6 of the Bill) This will address the current situation where directions cannot be cancelled or renewed. The s.94 Direction, sought by MI5 on behalf of all three agencies and known as the [REDACTED] is not seeking communications data but other types of support from the CSP in question. In the IP Bill this "rump" bit of s.94 is catered for separately in Part 9, and will be covered by a national security notice. Part 9 of the Bill does not currently come under any judicial oversight as the activities it covers do not impinge on Article 8.

27. The inspectors were provided with an overview of the new handling arrangements that were now in place for bulk personal data obtained under s.94 and from other sources, including the introduction of a new formal review board.

28. Jo Cavan spoke about some of the logistical issues she had faced in trying to pull together a full list of s.94 directions and appropriate POCs within the CSPs. She wants to check with [REDACTED – names of companies] to see if any have been served on them as they do not appear on the central record compiled so far. Jo was advised that there were commercial sensitivities around the provision of s.94 data by some of the CSPs, particularly the "non-standard" ones that would need to be taken into account during the IOCCO review.

29. Jo asked when Sir Mark Waller had been invited to oversee the s.94 directions – this happened in 2010 at the same time as he was asked to provide oversight of our handling of bulk datasets.

30. [REDACTED]

31. Jo said that her plan was to include a separate section in the Commissioner's report to cover the s.94 review. Once again, there are no plans for a closed or confidential annex to the report.

[REDACTED]

Audit

40. IOCCO had asked for a detailed session on GCHQ's audit processes within one of the recommendations from the May 2015 inspection and two hours had been set aside for this. The session opened with a short background presentation on the processes used to audit the necessity and proportionality of queries run against data in GCHQ systems. This set out what we look for, what good and poor necessity and proportionality statements look like, how we audit *foreign partner* activities and their overall compliance levels [REDACTED]

[REDACTED]