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

ARRANGEMENTS FOR THE ACQUISITION OF BULK COMMUNICATIONS DATA PURSUANT TO DIRECTIONS UNDER SECTION 94 OF THE TELECOMUNICATIONS ACT 1984 AND ACCESS THERETO PURSUANT TO AUTHORISATIONS UNDER SECTION 22 OF RIPA

Contents

1.0	Introduction	p.1
2.0	What information these Arrangements cover	pp.2-3
3.0	The law	pp.3-6
4.0	Safeguards and oversight	pp.6-17
4.1	Authorisation of Acquisition	pp.6-7
4.2	Acquisition	pp. 7-8
4.3	Authorisation of access/use	pp.8-13
4.4	Authorisation of disclosure	pp.13-14
4.5	Data retention, review and deletion	pp.14-16
4.6	Oversight	pp.16-17

1. Introduction

1.1 These Handling Arrangements are made under section 2(2)(a) of the **Security Service Act 1989** (**"the SSA 1989"**). They come into force on 4th November 2015.

1.2 The Arrangements apply to the **Security Service (MI5)** with respect to its acquisition of bulk communications data (**"BCD"**) pursuant to directions issued by the Secretary of State under section 94 of the Telecommunications Act 1984, its access to such data under Part 1 Chapter II of the Regulation of Investigatory Powers Act 2000 (section 22), and its subsequent use and disclosure of such data.

1.3 The rules set out in these Arrangements are mandatory and are required to be followed by staff in MI5. References in these Arrangements to 'staff' are to staff in MI5 unless specified otherwise. Failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal and prosecution.

1.4 Since 2005 successive Home Secretaries have issued directions, under **section 94** of the **Telecommunications Act 1984 ("the Section 94 Directions")**, requiring certain providers of public electronic communications networks ("communications network providers" or "CNPs") to provide MI5 with bulk communications data in the interests of national security. Successive Home Secretaries have agreed that they would keep these arrangements under review at six-monthly intervals.

2. What information these Arrangements cover

2.1 The communications data provided by the CNPs under the Section 94 Directions is limited to "**Traffic Data**" and "**Service Use Information**" [*see paragraph 3.11 and 3.12 below for definitions of "Traffic Data" and "Service Use Information"*].

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

2.2. The data provided does not contain communication content or Subscriber Information [*see paragraph 3.13 below for definition*].

[REDACTION]

3. The law

Security Service Act 1989

3.1 The SSA 1989 provides that the functions of the Security Service are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime.

3.2 **Section 2(2)(a)** of the SSA 1989 imposes a duty on the Director-General of the Security Service to ensure that there are arrangements for securing (i) that no information is obtained by MI5 except so far as necessary for the proper discharge of its functions; and (ii) that no information is disclosed except so far as is necessary for those functions and purposes or for the additional limited purposes set out in section 2(2)(a) – namely, for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings).

3.3 The SSA 1989 accordingly imposes specific statutory limits on the information that the Security Service can obtain, and on the information that it can disclose. These statutory limits do not simply apply to the obtaining and disclosing of information from or to other persons in the United Kingdom: they apply equally to obtaining and disclosing information from or to persons abroad.

Counter-Terrorism Act 2008 ("the CTA")

3.4 **Section 19** of the **CTA** further confirms that information obtained by the Services in connection with the exercise of any of its functions may be used by the Service in connection with the exercise of any of its other functions. For example, information that is obtained by MI5 for national security purposes can subsequently be used by MI5 to support the activities of the police in the prevention and detection of serious crime.

Human Rights Act 1998 ("the HRA")

3.5 The Security Service is a public authority for the purposes of the HRA. When obtaining, using, retaining and disclosing bulk communications data, MI5 must therefore (among other things) ensure that any interference with privacy is justified in accordance with **Article 8(2)** of the **European Convention on Human Rights ("ECHR")**. In practice, this means that any interference with privacy must be both necessary for the performance of a statutory function of the Security Service and proportionate to the achievement of that objective.

Data Protection Act 1998 ("the DPA")

3.6 To the extent that any bulk communications data held may enable MI5, following access to such data pursuant to authorisation under section 22 of the RIPA, to identify a living individual when such communications data is considered in conjunction with other information in the possession of MI5, such data will fall within

the definition of "*personal data*" in **section 1(1)** of the DPA. To that extent, MI5 may properly be regarded as the data controller in relation to the bulk communications data and to that extent, when processing any such personal data, must ensure that it complies with the DPA, save insofar as exemption under section 28 of the DPA is required for the purpose of safeguarding national security.

Telecommunications Act 1984

3.7 **Section 94** of the **Telecommunications Act 1984** (as amended by the Communications Act 2003) provides that the Secretary of State may give to CNPs "*such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*" The Secretary of State shall not give a direction unless he believes that the conduct required by the direction is '*proportionate to what is sought to be achieved by that conduct.*'

3.8 As indicated in paragraph 1.4 above, successive Home Secretaries have reviewed and approved Section 94 Directions to certain CNPs to provide MI5 with bulk communications data in the interests of national security.

3.9 **Section 94(4)** provides that the Secretary of State must lay a copy of every direction before each House of Parliament "*unless he is of the opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom.*" The Home Secretary is of the view that disclosure of these MI5 Section 94 Directions would be against the interests of national security, and so they have not been published, nor has the fact of their existence until 4 November 2015.

Regulation of Investigatory Powers Act 2000 ('RIPA') - Part I Chapter II

3.10 The legal framework governing the acquisition or obtaining of communications data, including obtaining access to such data, **is contained in Part I Chapter II** of **RIPA.** This regime is designed to ensure that any interference with an individual's human rights under Article 8 of the ECHR is justified as necessary and proportionate and in accordance with the law.

3.11 **Section 21(4)** of **RIPA** defines '*communications data*' as meaning any of the following:

- **Traffic Data** – this is data that is or has been comprised in or attached to a communication for the purpose of its transmission [*section 21(4)(a)*];
- **Service Use Information** – this is the data relating to the use made by a person of a communications service [*section 21(4)(b)*];
- **Subscriber Information** – this relates to information held or obtained by a communication server provider about persons to whom the communication server provider provides or has provided communications services [*section 21(4)(c)*].

3.12 **Section 21(6)** defines '*traffic data*' for these purposes, in relation to any communication, as meaning:

- any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;

- any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted;
- any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting (in whole or in part) the transmission of any communication; and
- any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

3.13 **Section 22** of **RIPA** provides that an authorisation for obtaining any communications data may be granted by a 'designated person' in the relevant public authority if he believes that it is **necessary** on (amongst others) the following grounds and is **proportionate** (section 22(2)(a)-(c)) -

- in the interests of national security;
- for the purpose of preventing or detecting crime [or of preventing disorder];
- in the interests of the economic well-being of the United Kingdom.

3.14 **Section 25(3)** of **RIPA** provides that the Secretary of State may by order impose restrictions on the authorisations that may be granted by any individual holding an office, rank or position with a specified public authority and on the circumstances in which or the purposes for which such authorisations may be given by such individuals. The relevant order for these purposes is the **Regulation of Investigatory Powers (Communications Data) Order 2010 (S.I. 2010/480)**. This states that an officer with "General Duties 3" i.e. a ***Grade 3***, within MI5 may authorise the obtaining of communications data for the purposes specified in paragraph 3.14 above.

3.15 A designated person at ***Grade 3*** level will grant an authorisation under **section 22(3)** of **RIPA** for other officers to access BCD if they believe that it is necessary on one of the specified grounds and that accessing the data is proportionate to what is sought to be achieved.

3.16 The form and duration of authorisations is provided for in **section 23** of **RIPA**. An authorisation under **section 22(3)** must be in writing or, if not in writing, in a manner that produces a record of it having been granted.

3.17 Under **section 23(4)(a)** of RIPA, a ***Grade 3*** is capable of authorising data to be obtained prospectively for a maximum period of one calendar month only, i.e. one calendar month beginning with the date on which the authorisation is granted. This means that authorisations for the acquisition of data that will or may be generated in the future are restricted to a period of no more than one calendar month from the date on which the authorisation was granted.

3.18 Authorisations in respect of **historic** data are not restricted in the same way and are capable of authorising the obtaining [REDACTION] or analysis of up to 365 days' of BCD product (if necessary and proportionate to do so).

4. Safeguards and Oversight

4.0.1 The acquisition, use, retention and disclosure of BCD requires clear justification, accompanied by detailed and comprehensive safeguards against misuse and must be subject to rigorous oversight.

4.0.2 These Arrangements accordingly provide specific published guidance to staff in MI5 with respect to the acquisition/obtaining of BCD and access to it and use, retention and disclosure to persons outside MI5 where this is necessary for the proper discharge of the relevant Service's statutory functions. Staff must ensure that no BCD is accessed/used, retained or disclosed **except in accordance with section 2(2)(a) of SSA, section 94** of the **Telecommunications Act 1984**, **Part 1 Chapter II of RIPA** and **these Arrangements.**

4.1 Authorisation of Acquisition – Stage 1

4.1.1 When considering the justification for acquiring a dataset comprising BCD pursuant to a Section 94 Direction, MI5 will undertake extensive preparatory work in order to consider the necessity and proportionality of the acquisition and the level of intrusion involved. Where MI5's Director General is satisfied that such acquisition is justified, the issue of a section 94 Direction by the Home Secretary will be requested for the purpose of acquiring the BCD in question.

4.1.2 The DG of OSCT at the Home Office will then commission a submission (informed by MI5's preparatory work) so as to enable the Home Secretary to consider:

- whether the acquisition and retention of the BCD provided for by the Direction is necessary in the interests of national security or relations with the government of a country or territory outside the UK;
- whether the acquisition and retention of the BCD would be proportionate to what is sought to be achieved;
- whether such information could be acquired elsewhere through less intrusive means;
- the level of collateral intrusion caused by acquiring and utilising the requested BCD;
- any reputational and political risks of Directing the CNP to provide the requested BCD;
- the financial implications for HM Treasury of Directing the CNP to provide the BCD;
- Any relevant ethical issues.

4.1.3 This submission must also outline any national security argument as to why the Home Secretary cannot lay the Direction before each House of Parliament in accordance with 94(4) of the Act.

When seeking authorisation of a new set of BCD, MI5 must consider and articulate the following for the Home Office/Secretary of State to consider:

- **The reasons why is it necessary to acquire and retain the data.**
- **The proportionality of acquiring and retaining the data. In particular, whether there is a less intrusive method of obtaining the data and a less obtrusive way of obtaining the same intelligence benefit.**
- **The level of collateral intrusion, in MI5 holding, accessing and utilising the proposed dataset.**
- **The associated reputational and political risks.**
- **The financial implications.**

4.2 Acquisition – Service of Section 94 Direction

4.2.1 Should the Home Secretary agree to serve the Direction, it will be served on a CNP by the Home Office, which will enable MI5 to receive the requested dataset.

[REDACTION]

4.3.4 Applicants are required to include the following necessity and proportionality considerations:

(i) **Necessity**

In order to meet the 'necessity' requirement the Applicant must consider why obtaining the data is 'really needed' in support of national security. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.

(ii) **Proportionality - General**

In order to meet the 'proportionality' requirement the Applicant must balance the level of interference with the individual's right to privacy against the expected value of the intelligence to be derived from the data. The Applicant must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion.

(iii) **Proportionality - Collateral Intrusion**

As mentioned above, collateral intrusion forms part of the proportionality argument. The Applicant must seek to identify any collateral intrusion to individuals outside of the line of enquiry, factoring in the impact of the time period of data specified and any identified mitigations. Collateral intrusion should always be considered and described if it is identified. However, it may be that none can be identified. When this is the case, then an Applicant is required to state this.

4.3.5 ***Once the applicant has submitted a request it will be considered by taking into account:***

- The justification provided by the Applicant is sufficient to satisfy the DP that obtaining the requested data is both necessary and proportionate;

- The individual mentioned in the justification is identical with the one for which the data is being obtained, that is that the justification has not been "copied and pasted" from another application;

- The intrusion into privacy that will result from the request has been addressed where necessary and where identified, measures to mitigate collateral intrusion have been outlined;

- The time period of data requested is proportionate and that the reasoning for requesting the time period listed is explained in the justification.

4.3.6 ***Any application for communications data is required to be refused if there is not a convincing case for both necessity and proportionality of the request. When an application is rejected the reasons are noted.***

[REDACTION]

Sensitive Professions

4.3.8 All applications must state whether the Applicant believes that the data returned will relate to a sensitive profession. **For sensitive professions, see also 4.3.20 below.** If an application is related to a sensitive profession, then the applicant must send the application to an 'independent' DP [REDACTION] for sign-off.

[REDACTION]

Additional safeguards governing access

4.3.19 The following **protective security measures** must be applied in relation to the use of or access to all communications data, whether derived from BCD obtained pursuant to the Section 94 Directions or from targeted communications data:

- Access to BCD must be strictly limited to those with an appropriate business requirement to use these data and managed by a strict authorisation process;
- Physical security to protect any premises where the information may be accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy;
- Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;
- A range of audit functions must be put in place: users should be made aware that their access to BCD will be monitored and that they must always be able to justify their activity on the systems;

- Appropriate disciplinary action will be taken in the event of inappropriate behaviour being identified;
- Users must be warned, through the use of User Agreements and Codes of Practice, about the consequences of any unjustified access to data, which can include dismissal and prosecution.

4.3.20 MI5 has also put in place the **following additional safeguards** governing access to all communications data, whether derived from BCD obtained pursuant to the Section 94 Directions or from targeted communications data:

- Where staff intend to access communications data relating to the communications of an individual known to be a member of a sensitive profession, i.e. one that handles privileged information or information that is otherwise confidential (medical doctors, lawyers, journalists, Members of Parliament, Ministers of religion), they must give **special consideration** to the necessity and proportionality justification for the interference with privacy that will be involved and must follow the procedure prescribed in 4.3.8 above.
- In addition, staff must take particular care when deciding whether to seek access to BCD and must consider whether there might be unintended consequences of such access to BCD and whether the public interest is best served by seeking such access;
- In all cases where staff intentionally seek to access and retain communications data relating to the communications of individuals known to be members of sensitive professions (as referred to above), they must record the fact that such communications data has been accessed and retained and must flag this to the Interception of Communications Commissioner at the next inspection;
- In the exceptional event that staff were to seek access to communications data specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand at Director level. Any communications data obtained and retained as a result of such access must be reported to the Interception of Communications Commissioner at the next inspection;
- In the exceptional event that staff were to abuse their access to communications data – for example, by seeking to access the communications data of an individual without a valid business need – MI5 is obliged to report the incident to the Interception of Communications Commissioner at the next inspection.

4.4 Authorisation of Disclosure

4.4.1 The disclosure of BCD is carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The disclosure of an entire BCD, or a subset, outside MI5 may only be authorised by the Home Secretary or a Senior Official[1] in the Home Office.

4.4.2 Disclosure of individual items of communications data to persons outside MI5 can only be made if the following conditions are met:

[1] Equivalent to a member of the Senior Civil Service.

- The objective of the disclosure falls within MI5's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
- It is necessary to disclose the information in question in order to achieve that objective;
- The disclosure is proportionate to the objective;
- Only as much of the information will be disclosed as is necessary to achieve that objective.

4.4.3 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the communications data is 'really needed' for the purpose of discharging a statutory function of that Agency. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, in cases where disclosure of BCD is contemplated, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole BCD.

4.4.4 The disclosure of the communications data must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of MI5's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved.

4.4.5 Before disclosing any communications data, staff must take reasonable steps to ensure that the intended recipient organisation has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled, or that they have received satisfactory assurances from the intended recipient organisation with respect to such arrangements.

4.4.6 These conditions must be met for all disclosure, including between the Intelligence Services. They apply equally to the disclosure of an entire BCD, a subset of the dataset, or an individual piece of data derived from the bulk communications dataset or from targeted communications data.

4.4.7 Where disclosure of **an entire BCD (or a subset)** is contemplated, (in addition to the requirement in 4.4.1 above) this is subject to prior internal authorisation procedures as well as to the requirements in 4.4.2-4.4.5 that apply to disclosure of individual pieces of data. Where these requirements are met, then (prior to submission to the Home Office/Home Secretary) the BCD is formally requested by the requesting agency from MI5 through an agreed sharing procedure using ***the appropriate form***. ***The data governance team*** is then responsible for submitting ***the appropriate form*** seeking the approval of MI5's Director General. ***The appropriate form*** outlines the business case submitted by the requesting agency, detailing the data requested, the necessity and proportionality case for disclosure of that data and the proposed data handling arrangements

4.4.8 . If the Director General is content, a submission will be prepared for the Home Office and/or Home Secretary. Disclosure of the whole BCD (or subset thereof) is only permitted when this has been authorised by the Home Secretary or a Senior Official at the Home Office. Once authorisation has been given, arrangements will be made for the data to be disclosed to the relevant acquiring agency.

Disclosure of MI5 BCD must be:

- **Justified on the basis of the relevant statutory disclosure gateway;**
- **Assessed to be necessary and proportionate to the objective;**
- **Limited to only as much information as will achieve the objective;**
- **Agreed by DG and authorised by the Home Secretary or Senior Official (entire BCD or a subset).**

4.5 Data Retention, Review and Deletion

4.5.1 ***The data governance team*** is required to conduct a comprehensive review of the capability every 6 months on behalf of the **BCD Governance Group** (**BCDGG**), to ensure that retention and use remains necessary for the proper discharge by MI5 of its function of protecting national security under section 1 of the Security Service Act 1989 and is proportionate to the achievement of that objective. This review will include, but is not limited to:

- An assessment of the value and use of the dataset during the period under review and in a historical context;
- the operational and legal justification for continued retention, including its necessity and proportionality;
- The extent of use and specific examples to illustrate the benefits;
- The level of actual and collateral intrusion posed by retention and exploitation;
- The extent of corporate, legal, reputational or political risk;
- Whether such information could be acquired elsewhere through less intrusive means;
- Any relevant ethical issues;
- The adequacy of security arrangements.

4.5.2 If ***the data governance team*** is satisfied that the ongoing acquisition and retention of the BCD (and the associated level of intrusion) are justifiable under Article 8(2) of the ECHR, it will recommend accordingly when it reports on its review to the **BCDGG**, which is required to meet at least every 6 months to consider the data governance team's report.

4.5.3 The BCDGG consists of, but is not limited to, the following: ***senior MI5 officials, the Ethics Counsellor and the Legal Adviser.***

4.5.4 ***If the BCDGG agree with the recommendation, it is then sent to the Deputy Director General. If he agrees, he will then submit the recommendation to the Director General of the Office of Security and Counter Terrorism, for the consideration of the Home Secretary, who will decide whether the case is sufficiently strong for the capability to be retained.***

4.5.6 In addition, the chair of the BCDGG must keep MI5's Executive Board apprised of MI5's BCD holdings, by providing the Board with a note on the position as appropriate.

4.5.5 MI5 can only retain data where it is necessary and proportionate to do so, and if it is judged (at any time, but including in the course of the six-monthly review process described above) that it is no longer necessary and proportionate to retain BCD, it must be deleted or destroyed (see 4.5.8 below).

Deletion

4.5.6 Data is retained for 365 days, after which it must be deleted. Specific data that has been retrieved from BCD following the procedures outlined in section 4.3 will be retained in accordance with MI5's Information Management policy.

4.5.7 Should the review process find that there remains an ongoing case for acquiring and retaining BCD, a formal review will be submitted at intervals of no less than six months for consideration by the relevant Secretary of State.

4.5.8 In the event that MI5 or the Home Secretary no longer deem it to be necessary and proportionate to acquire and retain the BCD, the Home Secretary will cancel the relevant Section 94 Direction and instruct the CNP concerned to cease supply. MI5 must then task destruction of the BCD to the technical teams responsible for Retention and Deletion. Confirmation of completed deletion must be recorded with ***the data governance team.***

For the purposes of retention, review and deletion of BCD holdings, MI5 must:

- **Regularly (at least every six months) review holdings to ensure that retention and use remains necessary and proportionate for MI5 to carry out its statutory duty to protect National Security;**
- **Submit a request for any proposed continuation to the Home Secretary;**
- **Delete BCD holdings after any decision is made that it is no longer necessary or proportionate to hold the data and notify the Interception of Communications Commissioner accordingly.**

4.6 Oversight

Internal

4.6.1 The BCDGG Chair, who is a member of MI5's Executive Board, keeps the Board apprised of BCD holdings.

4.6.2 Use of IT systems is monitored by the audit team in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal process whereby the officer undertaking the activity is interviewed. The officer's line manager will be copied into the investigation and legal, policy and HR input is requested where appropriate. MI5 has an agreed error reporting policy with the Interception of Communications Commissioner and breaches in relation to

section 94 may be reportable according to this policy. Appropriate disciplinary action may be taken which in the most serious cases could lead to dismissal and/or prosecution under the Computer Misuse Act 1990, the Data Protection Act 1998, the Official Secrets Act 1989 and Misfeasance in Public Office depending on circumstances.

4.6.3 All reports on audit investigations are made available to the Interception of Communications Commissioner (see 4.6.8 below).

External

4.6.4 The **Interception of Communications Commissioner** has oversight of:

(a) the issue of Section 94 Directions by the Home Secretary enabling MI5 to acquire BCD;

(b) MI5's arrangements in respect of acquisition, storage, access to the BCD pursuant to authorisations under section 22 of RIPA and subsequent use, disclosure, retention and destruction; and

(c) the management controls and safeguards against misuse which MI5 has put in place.

4.6.5 This oversight is exercised by the Interception of Communications Commissioner on at least an annual basis, or as may be otherwise agreed between the Commissioner and MI5.

4.6.6 The purpose of this oversight is to review and test judgements made by the Home Secretary and MI5 on the necessity and proportionality of the Section 94 Directions and on MI5's acquisition and use of BCD, and to ensure that MI5's policies and procedures for the control of, and access to BCD are (a) are sound and provide adequate safeguards against misuse and (b) are strictly observed.

4.6.7 The Interception of Communications Commissioner also has oversight of controls to prevent and detect misuse of data acquired under section 94, as outlined in in 4.6.2 and 4.6.3 above.

4.6.8 The Home Secretary and MI5 must provide to the Interception of Communications Commissioner all such documents and information as he may require for the purpose of enabling him to exercise the oversight described in paragraph 4.6.4 - 4.6.7 above

4.6.9 ***The oversight team*** coordinate the Commissioners visits. The ***data governance team*** must provide copies of the directions and the reviews conducted. ***The relevant team*** provide access to individual copies of applications for access to the BCD and the decisions made, without exception. Additional papers requested by the Commissioner must be made available to them.

4.6.10 The Parliamentary Intelligence & Security Committee may also be briefed on BCD holdings as required.

Oversight of MI5 BCD holdings must include:

- **Chair of BCDGG reports to the Executive Board on BCD holdings;**
- **Internal audit of systems to detect misuse or identify activity of security concern with corresponding disciplinary measures;**
- **External, independent oversight by the Interception of Communications Commissioner of the acquisition, access, retention and disclosure of BCD holdings on an annual basis.**