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

ARRANGEMENTS UNDER SECTION 2(2)(a) OF THE SECURITY SERVICE ACT 1989 AND SECTIONS 2(2)(a) FOR THE OBTAINING AND DISCLOSING OF BULK PERSONAL DATA

Contents

1.0 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 acquisition, use, disclosure and retention by MI5 of the category of information identified in 2.2 below, and set out the safeguards governing the Service's handling of BPD at each stage of the process, along with the oversight and management controls (internal and external) which are in force.

1.3 The rules set out in these Arrangements are mandatory and are required to be followed by all staff. Failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal.

1.4 These Arrangements have two functions. First, they describe the processes that MI5 applies in relation to BPD. Secondly, it sets out a list of requirements and considerations that must be followed/applied by staff when handling BPD. The key mandatory requirements are re-summarised in the boxes at the end of each section, or subsection, in bold.

2.0 The Information Covered by these Arrangements

2.1 MI5 lawfully collects BPD from a range of sources to meet its statutory functions.

2.2 "The Intelligence Services" (the Security Service, the Secret Intelligence Service and the Government Communications Headquarters) have an agreed definition of a "Bulk Personal Dataset" (BPD). A BPD means any collection of information which:

- Comprises personal data;
- Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;
- Is held, or acquired for the purpose of holding, on one or more analytical systems within the SIA.

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

2.3 Bulk Personal Datasets will in general also share the characteristic of being too large to be manually processed (particularly given that benefit is derived from using them in conjunction with other datasets).

2.4 In this context, 'Personal Data' has the meaning given to it in section 1(1) of the Data Protection Act 1998 (DPA) which defines 'personal data' as follows:

'data which relate to a living[1] individual who can be identified –

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of the data controller (i.e. the relevant agency), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

2.5 The definition of 'Sensitive Personal Data' has the meaning given to it in the DPA (1998), and so covers the following:

- Racial or ethnic origin
- Political opinions
- Religious belief or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sexual life
- The commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

2.6 The above list is not exhaustive, and MI5 take into account a number of other additional sensitive categories. For example, this includes – but is not limited to – areas such as legal professional privilege, journalistic material and financial data.

2.7 ***MI5's data governance team*** is responsible for the governance arrangements for BPD. It works in consultation with the investigative, operational, analytical, legal and policy branches to understand business requirements for BPD and ensure that BPD is subject to appropriate handling and protection throughout its lifecyle.

2.8 These Arrangements accordingly provide specific guidance to staff in MI5 with respect to the obtaining of bulk personal datasets and their use, retention and disclosure to persons outside MI5 where this is necessary for the proper discharge of MI5's statutory functions. Staff must ensure that no bulk personal dataset is obtained, used, retained or disclosed **except in accordance with section 2(2)(a) of the SSA 1989** and **these Arrangements.**

2.9 For the avoidance of doubt, these Arrangements apply to bulk personal datasets obtained under section 2(2)(a) of the SSA itself by agreement with third-party voluntary suppliers and by other non-covert access methods, and apply also to bulk personal datasets obtained by the exercise of other statutory powers.

[1] Whilst DPA refers only to 'a living individual', bulk personal datasets may contain details about individuals who are dead. SIA policy and processes in relation to bulk personal data is the same for both the living and the dead.

2.10 These other statutory powers include those exercisable under warrants issued under section 5 of the ISA in respect of property and equipment interference; intrusive surveillance warrants issued under section 32 of the Regulation of Investigatory Powers Act 2000) ('RIPA'); directed surveillance authorisations issued under section 28 of RIPA; covert human intelligence source authorisations issued under section 29 of RIPA; warrants issued under section 5 of RIPA for the interception of communications; and communications data notices or authorisations issued under Part 1 Chapter 2 of RIPA. The application of these Arrangements to bulk personal datasets obtained by exercise of these other statutory powers is without prejudice to the additional statutory requirements specified in the relevant legislation (whether section 5 of the ISA or RIPA).

Note: The list in para 2.10 above is non-exhaustive.

2.11 Where the bulk personal dataset in question engages the exercise of any of the other statutory powers referred to in paragraph 2.10, the processes provided for in these Arrangements need to be followed as well as (in parallel) the requisite warrantry or authorisation process involved in the specific statutory regime relating to the exercise of those powers.

3.0 The Law

3.1 The SSA 1989 and the Counter-Terrorism Act 2008 ("the CTA")

3.1.1 The SSA 1989 provides that the functions of MI5 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.

3.1.2 The information gateway provisions in section 2(2)(a) of the SSA 1989 impose a duty on DG 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 our 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) of the SSA 1989 (for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings).

3.1.3 The SSA 1989 accordingly imposes specific statutory limits on the information that MI5 can obtain, and on the information that can be disclosed. 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.

3.1.4 Section 19 of the CTA confirms that '*any person*' may disclose information to MI5 or any of the Intelligence Services for the exercise of their respective functions, and disapplies any duty of confidence (or any other restriction, however imposed) which might otherwise prevent this. It further confirms that information obtained by MI5 or any of the Intelligence Services in connection with the exercise of any of their functions may be used by that Service in connection with the exercise of any of its other functions. For example, information that is obtained by the MI5 for national security purposes, it would subsequently be lawful for MI5 to use it in support the activities of the police in the prevention and detection of serious crime.

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

3.2 The Human Rights Act 1998 ("the HRA")

3.2.1 MI5 is a public authority for the purposes of the HRA. When obtaining, using, retaining and disclosing bulk personal data, the Intelligence Services 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. In practice, this means that any interference with privacy must be both necessary for the performance of a statutory function of MI5 and proportionate to the achievement of that objective.

3.3 The Data Protection Act 1998 ("the DPA")

3.3.1 MI5 is a data controller in relation to all the personal data that it holds. Accordingly, when MI5 use any bulk data that contains personal data, staff must ensure that they comply with the DPA (subject only to cases where exemption under section 28 is required for the purpose of safeguarding national security).

4.0 Authorisation and Acquisition

4.1 Authorisation

4.1.1 In determining whether to procure a dataset, MI5 business requirements are set by the relevant teams working to counter threats to national security. Each business area has formulated its requirements into a BPD strategy to ensure that BPD is acquired in line with investigative requirements.

4.1.2 Whenever MI5 considers acquiring a dataset the officers responsible for acquiring the BPD must consider the necessity and proportionality of doing so the earliest possible stage. Typically this will mean consideration of the following questions:

- What is the likely content of the dataset? [REDACTION]
- What business requirements will be met by acquiring and using the dataset?
- How is exploitation of the dataset likely to contribute to MI5 business requirements?
- How intrusive will acquisition and use of the data be, with particular reference to the degree of collateral intrusion?
- Can the intelligence be obtained by other, less intrusive, means?

4.1.3 The authorisation to acquire BPD is managed via ***the relevant form***. ***The relevant form*** must be used in any situation where it is the intention to acquire BPD and must be supported by a ***business case approved by a senior MI5 official.***

4.1.4 The detailed process to be followed is:

- The Data Sponsor for the relevant business area must draft ***a relevant form***, explaining why the data is required, its intended use, and its potential impact on investigations.
- ***The relevant form*** will give a justification of why the acquisition and retention, and subsequent updates (if appropriate), are both necessary and proportionate and give an assessment of the potential intrusion – collateral

and actual - into privacy by MI5 holding, accessing and utilising the proposed dataset.

- The business case must then be endorsed by ***the relevant team within MI5*** before being submitted to the ***data governance team*** who manage the authorisation process.
- The relevant legal and technical advisers will be consulted to ensure legality and feasibility of acquiring the dataset. ***The data governance team*** will then make an assessment of the political, corporate and reputational risk to MI5 and the data supplier of acquiring the data.
- ***The senior MI5 official*** is the authorising officer. They will review the necessity and proportionality of acquiring the BPD and ensure it will assist MI5 in pursuing its statutory functions; and if satisfied they will authorise the acquisition.
- Should the proposed BPD acquisition appear particularly contentious or difficult, the decision to authorise or not could be escalated to DDG. Ministers may be consulted if the political or reputational risks are judged to be of sufficient gravity.
- Legal Advisers should be consulted on all new BPD acquisitions. The Ethics Counsellor may be consulted by anyone at any stage of ***the relevant form*** process, or in the event of ethical concerns being raised.
- Once authorised, the completed application must be stored on a centrally retrievable record and include the date of approval. This record must also contain the date of acquisition of the relevant data in MI5 premises, which should be the date used for the subsequent review process.

4.1.5 What is **necessary** in a particular acquisition case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the '**necessity**' requirement in relation to acquisition, staff must consider why obtaining the BPD is 'really needed' for the purpose of discharging a statutory function of the relevant Intelligence Service. 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.

4.1.6 The obtaining and retention of the BPD must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must balance (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the data and who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the data. Staff 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.

4.1.7 These can be difficult and finely balanced questions of judgement. In difficult cases staff should consult line or senior management and/or the legal advisers in [REDACTION] for guidance, and may seek guidance or a decision from the relevant Secretary of State.

4.1.8 [REDACTION]

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

When considering seeking authorisation of a new set of BPD, MI5 officers must:

- **Consider the reasons why is it necessary to acquire and retain the data.**
- **Consider the proportionality of acquiring and retaining the data. In particular, officers must consider whether there is a less intrusive method of obtaining the data and a less obtrusive way of obtaining the same intelligence benefit.**
- **Consider the level of intrusion, collateral and actual, in MI5 holding, accessing and utilising the proposed dataset.**
- **Ensure that *the relevant form* process is adhered to and has been authorised.**

4.2 Acquisition

4.2.1 Once ***the relevant form*** has been authorised, MI5 are able to acquire the required dataset. ***MI5 acquires BPD from a wide range of sources such as SIA partners, other HMG departments, private business, interception and CNE.***

4.2.2 Whilst the source of the data varies, we are able to broadly categorise the acquired datasets into the following groups:

- Population

These datasets provide population data or other information which could be used to help identify individuals [REDACTION] e.g. passport details [REDACTION].

- Travel

These datasets contain information which enable the identification of individuals' ***travel activity.***

- Finance

These datasets allow the identification of [REDACTION] finance related activity of individuals [REDACTION]

- Communications

These datasets allow the identification of individuals where the basis of information held is primarily related to communications data [REDACTION] e.g. a telephone directory.

- Commercial

These datasets provide details of corporations/individuals involved in commercial ***activities.***

- LEA/Intelligence

These datasets primarily contain operationally focussed information from law enforcement or other intelligence agencies [REDACTION].

5.0 Use

5.1 Access

5.1.1 MI5 attaches the highest priority to maintaining data security and protective security standards. Robust handling procedures have been established so as to ensure that the integrity and confidentiality of the information in the BPD held is protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken. This is underpinned by the following protective security measures that must be adhered to:

- Physical security to protect any premises where there is access to MI5 information;
- IT security to prevent unauthorised access to IT systems;
- A security vetting regime for personnel who have access to this material which is designed to provide assurance that those with access are reliable and trustworthy.

5.1.2 The following additional measures have been put in place to reinforce compliance in relation to the necessity and proportionality of using these datasets:

- Access to the information is strictly limited to those with an appropriate business requirement to use these datasets;
- Individuals may only access information within a BPD if it is necessary for the performance of one of the statutory functions of MI5;
- If individuals access information within a BPD with a view to subsequent disclosure of that information, they may only access the relevant information if such disclosure is necessary for the performance of the statutory functions of MI5;
- Before accessing or disclosing information, individuals must also consider whether doing so would be proportionate. For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;
- 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 are in place: users should be made aware that their access to BPD will be monitored and that they must always be able to justify their activity;
- Appropriate disciplinary action is taken in the event of inappropriate behaviour being identified; and
- Users must be warned, through the use of Security Operating Procedures and Codes of Practice, about the consequences of any unjustified access to data, which in the most serious cases could lead to dismissal and/or the possibility of prosecution.

5.1.3 MI5 may also take measures to reduce the level of interference with privacy arising from the acquisition and use of BPD:

- Data containing sensitive personal data may be subject to further restrictions, including sensitive data fields not being acquired, being acquired but suppressed or deleted, or additional justification required to access sensitive data fields;
- Working practice seeks to minimise the number of results which are presented to analysts, although this varies in practice depending on the nature of the analytical query;
- If necessary, we can limit access to specific datasets to a very limited number of users.

5.2 Training

5.2.1 BPD is currently accessed primarily via MI5's corporate analytical systems. Before access is granted to such systems, all users must read and sign a Code of Practice. Once this is signed users must also complete a mandatory training course before access is granted. A small number of specialist analyst systems have a very limited cadre of users. As a result, there is no formal training course and new users are instead mentored by experienced colleagues with expertise in these systems and the datasets held within them.

5.2.2 ***Users of these analytical systems must also sign the relevant operating procedures form and there is line manager responsibility for their conduct and training.***

5.2.3 ***In addition to specific mandatory training and the specialist mentoring additional courses/resources are available for MI5 officers, including a legal awareness course and guidance and policy documents relating to BPD that are available electronically to MI5 officers.***

5.4 Experiments and innovation

5.4.1 Use of bulk personal data for experimental or innovation purposes, e.g. development of a novel analytical technique or testing a new IT system, potentially entails an elevated level of risk to the security of the data, increased corporate risk and an additional interference with the right to privacy. Any such use of bulk personal dataset must be considered and authorised in advance by ***a senior MI5 official.*** A request for authorisation will describe the proposed activity and explain why it is necessary and proportionate to use bulk personal data for this purpose. It will also include an assessment of the impact the experimental use is expected to have on corporate risk and interference with privacy.

5.4.2 If the request to use the bulk personal dataset for the proposed experimental purpose is approved, the Authoriser may, at his/her discretion, set conditions or restrictions on its use. If the request is rejected, the dataset must not be used for that purpose. The decision and any conditions or restrictions must be retained as part of the record for that dataset.

Access to MI5 BPD must be controlled by:

- **Physical, IT and vetting security regimes;**
- **Strict controls on access to and disclosure of BPD information;**
- **User training on appropriate usage and in professional and legal responsibilities;**
- **Appropriate audit regime, SyOPs and Codes of Practice with corresponding disciplinary action.**

6.0 Disclosure

6.1 The disclosure of BPD is carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The decision to share a BPD outside the Security Service rests with ***a senior MI5 official.***

6.2 Disclosure within the SIA

6.2.1 The SIA all have a common interest in acquiring information for national security purposes, and it is both necessary and lawful for the agencies to share BPD providing certain circumstances are met. Information in BPD held by MI5 can only be disclosed to persons outside the Service if the following conditions are met:

- that 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;
- that it is necessary to disclose the information in question in order to achieve that objective;
- that the disclosure is proportionate to the objective;
- that only as much of the information will be disclosed as is necessary to achieve that objective.

6.2.2 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the BPD is 'really needed' for the purpose of discharging a statutory function of MI5. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal data.

6.2.3 The disclosure of the BPD 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.

6.2.4 These conditions must be met for all disclosure, including between the Intelligence Services. They apply equally to the disclosure of an entire BPD, a subset of the dataset, or an individual piece of data from the dataset.

6.2.5 Disclosure of **the whole (or a subset) of a bulk personal dataset** is subject to prior internal authorisation procedures in addition to the requirements in 6.2.1-6.2.3 above. Where these requirements are met, the BPD is formally requested by the requesting Agency from MI5 through an agreed disclosure procedure using ***the relevant form***. The relevant data sponsor is then responsible for submitting ***the relevant form*** that will seek authorisation within MI5.

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

6.2.6 The ***relevant 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. Disclosure of the whole BPD (or subset thereof) is only permitted once such authorisation has been given under this process. Once the authorisation has been given, arrangements will be made for the data to be disclosed to the relevant acquiring Agency.

6.3 Disclosure to liaison services

6.3.1 [REDACTION]

6.3.2 There are however some circumstances, such as a pressing operational requirement, where disclosure to a liaison service [REDACTION] may be necessary and proportionate in the interests of national security. In this event, the same legal disclosure tests would need to be applied as when disclosing to SIA partners, and ***the relevant form*** would have to be completed. MI5 would need to be satisfied that disclosure to the relevant liaison service met the dual tests of necessity and proportionality. All enquiries should be directed to ***the data governance team***. Prior to disclosure, staff must (a) take reasonable steps to ensure that the liaison partner has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data (including with regard to both source protection and the protection of the privacy of the individuals in the BPD) and ensuring that it is securely handled, or (b) have received satisfactory assurances from the liaison partner with respect to such arrangements.

Disclosure of MI5 BPD 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;**
- **Authorised by *a senior MI5 official* using *the relevant form*.**

7.0 DATA RETENTION AND REVIEW

7.1. Bulk Personal Data Review Panel

7.1.1 The Bulk Personal Data Review (BPDR) Panel currently meets at least every 6 months to conduct a review of bulk personal datasets in MI5's possession, to ensure that their retention and use remains necessary and proportionate for MI5 to carry out its statutory duty to protect National Security for the purposes of s.2(2)(a) Security Service Act 1989.

7.1.2 Panel members will satisfy themselves that the level of intrusion is justifiable under Article 8(2) of the ECHR and is in line with the requirements of the Data Protection Act 1998. MI5 can only retain BPD where it is necessary and proportionate to do so, and if it is judged (at any time, but including on review) that it is no longer necessary and proportionate to retain a dataset, all copies must be deleted or destroyed.

7.1.3 ***The Panel consists of, amongst others, senior officials, Ethics Counsellor, non-executive director and legal adviser.***

7.1.4 Representatives from SIS and GCHQ are normally invited to attend to observe and contribute to discussions.

7.1.5 The Panel considers recommendations for each dataset under review and decides whether to retain the dataset or to delete. When a dataset is retained it will be given a retention period in accordance with the level of intrusion and risk posed by the retention and use of the dataset and may range from 6 to 24 months. All new datasets will be subject to an initial full review by the panel at the first BPDR meeting of 4.1.4 after acquisition to ensure the acquisition process has been properly followed.

7.1.6 The Panel will also examine the terms under which any BPD have been shared to review the necessity and proportionality of the sharing of the data and ensure the interests of the data provider are protected.

7.1.7 Where the panel cannot agree on whether a dataset should be retained or deleted, the chair will seek advice and a decision from DDG.

7.1.8 All BPD to be reviewed will be submitted to the Panel on ***the appropriate form*** in which users will outline the case for retention. When making the decision to either retain or delete a bulk dataset, the Panel consider:

- An assessment of the value and use of the dataset during the period under review
- the operational and legal justification for continued retention, including its necessity and proportionality
- The level of actual and collateral intrusion posed by retention and exploitation
- The extent of corporate, legal, reputational or political risk
- Frequency of acquisition and updates
- Whether such information could be acquired elsewhere through less intrusive means
- Whether any caveats or restrictions should be applied
- Any relevant ethical issues

7.1.9 It is possible for a data sponsor to request the deletion of a dataset at any stage of its life; however it is also possible that the BPDR Panel may conclude that on the balance of the evidence, it is no longer necessary and proportionate to retain a dataset.

7.2 Deletion

7.2.1 When a decision has been reached to delete BPD, its destruction is tasked to the technical teams responsible for Retention and Deletion. Confirmation of completed deletion must be recorded with ***the data governance team*** and an update provided to the following BPDR Panel meeting. Information specialists provide technical reassurance surrounding the deletion and destruction of the dataset.

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

- **Use the BPDR Panel to regularly review BPD holdings (at not less than**

six-monthly intervals) to ensure that retention and use remains necessary for MI5's proper discharge of its statutory functions and proportionate thereto;

- **Review all new datasets at the first BPDR Panel meeting after acquisition;**
- **Appoint the appropriate review period for the dataset according to the associated level of intrusion and risk;**
- **Delete BPD holdings after the decision is made that it is no longer necessary or proportionate to hold the data;**

8.0 Oversight

8.1 Executive Board

8.1.1 The Chair, who is a member of MI5's Executive Board, keeps the Board apprised of MI5's bulk data holdings as appropriate.

8.2 Audit of Use

8.2.1 Use of analytical 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. Failure to justify a search can result in disciplinary action, which in the most serious cases could lead to dismissal and/or the possibility of prosecution.

8.2.2 All audit investigations are available to the Intelligence Services Commissioner for scrutiny.

8.3 External Oversight

8.3.1 The acquisition, use, retention and disclosure of BPD by MI5, and the management controls and safeguards against misuse they put in place, will be overseen by the Intelligence Services Commissioner on a regular six-monthly basis, or as may be otherwise agreed with the Commissioner, except where the oversight of such data already falls within the statutory remit of the Interception of Communications Commissioner.

8.3.2 The purpose of this oversight is to review and test our judgements on the necessity and proportionality of acquiring, using and retaining bulk personal datasets and to ensure our policies and procedures for the control of, and access to, and retention of these datasets (a) are sound and provide adequate safeguards against misuse and (b) are strictly complied with, including through the operation of adequate protective monitoring arrangements. Although we brief the Home Secretary on MI5's use of these techniques and provide a list of datasets on an annual basis, independent oversight by the Intelligence Services Commissioner provides a third party view of the arrangements that have been agreed. It also affords an independent view on our judgements that provides assurance to MI5, the Home Secretary and the Prime Minister.

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

8.3.3 The Intelligence Services Commissioner also has oversight of controls to prevent and detect misuse of bulk personal data, as outlined in paragraph 8.2.1 and 8.2.1 above.

8.3.4 ***The Service must provide to the appropriate Commissioner all relevant documents and information such that he can exercise the oversight described above. Additional papers requested by the Commissioner must be made available to him.***

Oversight of MI5 BPD holdings must include:

- **Chair of BDRP report to the Executive Board on BPD holdings;**
- **Internal audit of systems with access to BPD to detect misuse or identify activity of security concern with corresponding disciplinary measures;**
- **External, independent oversight by the Intelligence Services Commissioner of the acquisition, use, retention and disclosure of BPD holdings on a six monthly basis.**