Double-underlining indicates gisting for OPEN disclosure

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
(4) SECURITY SERVICE
(5) SECRET INTELLIGENCE SERVICE

Respondents

THE RESPONDENTS' CLOSED RESPONSE

[REDACTED]

A. THE RESPONDENTS' CLOSED POSITION ON THE FACTUAL ALLEGATIONS

Bulk Personal Data

1) A Bulk Personal Dataset ("BPD") is a dataset that contains personal data about individuals the majority of whom are unlikely to be of intelligence interest and that is incorporated into an analytical system and used for intelligence purposes. Typically such datasets are very large, and too large to be processed manually.

2) The Third to Fifth Respondents ("the Intelligence Services") obtain and exploit BPD for several purposes: to help identify subjects of interest or unknown people that surface in the course of investigations; to establish links between individuals and groups; or else to improve understanding of targets' behaviour and connections; and to verify information obtained through other sources.

3) BPD obtained and exploited by the Intelligence Services include a number of broad categories of data. By way of example only these include: biographical and travel (e.g.

passport databases); communications (e.g. telephone directory); and financial (e.g. finance related activity of individuals).

4) While each of these datasets in themselves may be innocuous intelligence value is added in the interaction between multiple datasets. One consequence of this is that intrusion into privacy can increase.

5) BPD is operationally essential to the Intelligence Services and growing in importance and scale of holdings. Examples of the vital importance of BPD to intelligence operations include:

   a) Identifying Foreign Fighters: [REDACTED]

   b) Preventing Access to Firearms: [REDACTED]

Section 94 of the Telecommunications Act 1984

6) A number of directions have been issued under section 94 of the 1984 Act. Such directions which fall within the scope of the present Claim are addressed below. These are essentially directions which involve the acquisition/use of Bulk Communications Data ("BCD").

[REDACTED]

Bulk Communications Data

7) Both GCHQ and the Security Service ("MI5") acquire Bulk Communications Data pursuant to directions made under section 94 of the 1984 Act. For the avoidance of doubt, SIS do not do so.

GCHQ

8) Since 2001 GCHQ has sought and obtained from successive Foreign Secretaries a number of section 94 directions relating to the ongoing provision of various forms of bulk communications data. In keeping with GCHQ's external intelligence mission, the datasets received under these directions are predominantly foreign-focused, and the data acquired is accordingly in most cases only a fraction of that possessed by the CNPs involved.

9) The data received is held by GCHQ and ingested into their broader data holdings where it is merged with communications data intercepted under the authority of external warrants issued in accordance with s.8(4) of RIPA. The s.94 data represents a more reliable and comprehensive feed of particular types of communication data than may usually be obtained from interception. The intelligence value of the s.94 data is derived from the merger with GCHQ's wider datasets, thus enriching the results of analytic queries made on those systems.

10) Such analysis of bulk communications data is vital for identifying and developing intelligence targets. Approximately 5% of GCHQ's original intelligence reporting is based wholly or partly on s.94 data.

MI5

11) Since 2005 successive Home Secretaries have issued and/or decided to maintain directions under s.94 of the 1984 Act requiring a number of CNPs to provide MI5 with [REDACTED] communications data in the interests of national security. [REDACTED] The data obtained is aggregated in a database. Successive Home Secretaries have agreed that they would keep these arrangements under review at six-monthly intervals. The review process involves a detailed submission being made to the Home Office by MI5, setting out the ongoing case for the database, including specific examples of its usefulness in the intervening period and setting out any errors in the use of the database which have occurred in that time. The Home Secretary considers the submission with the advice and assistance of senior Home Office officials.

12) The communications data provided by the CNPs under the section 94 directions is limited to "traffic data" and "Service Use Information" [REDACTED].

13) The data provided does not contain communication content or Subscriber Information (information held or obtained by a CNP about persons to whom the CNP provides or has provided communications services). The data provided is therefore anonymous. It is also data which is in any event maintained and retained by CNPs for their own commercial purposes (particularly billing and fraud prevention).

14) Such data is of significant intelligence and security value.

15) MI5 retrieves data from the database using sophisticated software. This software is run against the data to answer specific investigative questions. Requests of the database can be made only where an authorisation is granted under section 22 of the Regulation of Investigatory Powers Act 2000 ("RIPA") if judged necessary and proportionate.

[REDACTED]

16) Data is provided by CNPs on a regular basis. Data is retained by MI5 for 12 months before being deleted.

17) Prior to the creation of the database MI5 was limited in its ability to make use of Communications Data. [REDACTED]

18) Section 94 Directions were first laid in respect of the database on 21 July 2005. The view of successive Home Secretaries has been that disclosure of the Section 94 Directions in respect of the database would be against the interests of national security. Although the fact that Section 94 Directions have been issued has been avowed, the directions themselves have not

been published [REDACTED]. The directions remain in place but are reviewed every six months.

B. "BELOW THE WATERLINE" SAFEGUARDS FOR BULK PERSONAL DATA

19) The Open Response set out the relevant statutory regimes and the material provisions of the Open Handling Arrangements (§§28-29). However, in addition to the statutory regime and Open Handling Arrangements, the Intelligence Services have substantial "below the waterline" safeguards which apply to BPD.

20) This Section of the Closed Response considers the "below the waterline" safeguards of (a) the SIA jointly; (b) MI5; (c) SIS; and (d) GCHQ.

SIA

21) The Intelligence Services have agreed policy in relation to Bulk Personal Data. This is reflected not only in the Open BPD Handling Arrangements addressed in the Open Response, but is also set out in an internal "SIA Bulk Personal Data Policy" (SIA BPD Policy) which came into force in February 2015. A copy of the current policy is exhibited to this Closed Response as Exhibit "**A**". In addition, each of the Agencies has developed separate, Agency-specific policy guidance for its staff aligned with the SIA BPD Policy (see, inter alia, §4 and §10 of the SIA BPD Policy).

22) §4 of the SIA BPD Policy notes that it has been *"agreed by all three Agencies"*. Furthermore, the *"Agencies have aligned specific business processes where appropriate to allow for greater cooperation and consistency of approach."*

23) A definition of "Bulk Personal Data" is set out at §5:

> *"The Agencies lawfully collect a range of information from a variety of sources which is needed to meet their statutory functions in an effective and timely manner. The data collected includes datasets which contain personal data about a wide range of individuals, the majority of whom are not of direct intelligence interest. These datasets are known as Bulk Personal Datasets and are acquired via various statutory gateways...They share the following characteristics:*
> - *Contain personal data about individuals, the majority of whom are unlikely to be of intelligence or security interest.*
> - *Are too large to be manually processed (particularly given benefit is derived by using them in conjunction with other datasets);*
> - *Are held on analytical systems within the SIA."*

24) "Personal data" in this context has the meaning given to it by section 1(1) of the Data Protection Act 1998:

> *" '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."*

25) The policy explains that *"Whilst DPA refers only to 'a living individual', many bulk personal datasets will contain details about individuals who are dead. SIA policy and processes in relation to bulk personal data are the same for both the living and the dead.'* (footnote 1)

26) *"Sensitive Personal Data"* is also given the meaning found in the DPA:

"

- *Racial or ethnic origin;*
- *Political opinions;*
- *Religious belief or other beliefs or a similar nature;*
- *Membership of a trade union;*
- *Physical or mental health or condition;*
- *Sexual life;*
- *The commission or alleged commission of any offence; or*
- *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."*

27) The SIA BPD Policy also notes that each of the SIA may, in their individual policy guidance, treat additional categories of data with particular sensitivity:

> *"8. In addition to the DPA-defined statutory categories, each Agency may have additional policies (with additional controls) in which they define further categories as 'Sensitive Personal Data' (in a non-statutory sense). In practical terms, this means that the Agencies recognise and may, as judged appropriate, take additional steps to protect data relating to these subjects."*

28) The SIA BPD Policy requires each Intelligence Service to have arrangements in place for the effective management and legal compliance of BPD throughout its lifecycle (§9). The stages of the lifecycle are:

"

- ***Acquisition*** *– the initial authorisation processes, arrangements for collection, receipt, storage and loading of BPD onto Agency systems;*
- ***Use*** *– access to, and use of, the data by Agency staff, authorisations required for different types of use, reviews of use, safeguards;*
- ***Sharing*** *– sharing of data between the Agencies and with other partners, authorisations, reviews of use;*
- ***Retention*** *– ensuring Agencies do not retain data longer than is necessary, review processes;*

- ***Deletion/Destruction*** *- decision making, processes to ensure effective recording and confirmation of the deletion/destruction."*

29) The policy requires each Intelligence Service to have *"a governance structure and a process in place to ensure effective oversight of the BPD lifecycle."* These must *"provide robust frameworks to ensure that each Agency handles its information appropriately and in compliance with the law."* (§11) These structures *"support the Head of each Agency in the discharge of his statutory duties"*.

30) Each Intelligence Service must have a *"review panel"* (§13):

> *"Each Agency must have a review panel whose function is to oversee the lifecycle of the BPD it holds. The composition and specific processes may vary between the Agencies, but each must be chaired at senior (director or deputy or assistant director – as appropriate for each Agency) level, and include legal advisers, technical teams, compliance or policy teams and representatives from the business as judged appropriate. Invitations should also be extended to each of the other two Agencies."*

31) The external oversight provided by the Intelligence Services Commissioner and the Interception of Communications Commissioner, and the division of their respective roles, is explained in §14.

32) The SIA BPD Policy contains separate sections relating to (i) Acquisition (ii) Use (iii) Sharing (iv) Retention and (v) Deletion/Destruction which apply to each of the Intelligence Services.

<u>*SIA: Acquisition*</u>

33) The acquisition of BPD is a tightly controlled process. This is embodied in policy statements at §15 which apply to all Intelligence Services:

> "
>
> - *All acquisition must be authorised by a senior manager within the Agency (specific arrangements vary between Agencies);*
>
> ...
>
> - *Where a request is made to obtain a dataset it must be justifiable and deemed necessary and proportionate for the requesting Agency to acquire the dataset in pursuit of its statutory functions;*
> - *The acquisition of BPD must be authorised before any analytical exploitation of the data. Authorisation may need to be obtained at an earlier stage at the individual Agency's direction. If authorisation is not granted the relevant BPD must be deleted;*
>
> ...
>
> - *All BPD will be assessed to determine the levels of Intrusion and Corporate Risk during the acquisition process. These considerations will assist in the decision regarding the review periodicity for the dataset;*

[REDACTED]

- *It is the responsibility of the Agency that acquired the data to manage the relationship with the data supplier. Where an Agency shares a dataset with another, the receiving Agency is responsible for its copy. If the acquiring Agency decides to delete/destroy the dataset but the other Agencies wish to retain the data and have sufficient justification, the Agencies must agree between them the responsibilities for managing supplier equities, source, and/or technique protection. As judged appropriate, this may involve the transfer of responsibility for managing the relationship, sources or capability to one of the other Agencies, or the continued supply of data by one Agency on behalf of the others;*

- *All BPD sets held within and shared between the SIA must have a clearly identified lead Agency;*

- *The Agencies will coordinate to ensure efficiency in the acquisition of BPD. This includes de-confliction to prevent parallel or duplicative acquisition;*

[REDACTED]

- *After receipt of BPD there must be robust access controls, constrained to those with a business need, to all versions of information held on any medium/system;*
- *Any original media retained must be held securely, with appropriate and auditable records kept, including in relation to any copies made;*
- *BPD must only be retained on the original physical media for as long as is necessary."*

SIA: Use

34) Further policy statements are set out in relation to the **use** of BPD. §16 emphasises the key principles of **necessity** and **proportionality** which underlie those statements:

> *"The use of BPD is managed and monitored to ensure that the principles of necessity and proportionality are followed, thereby enabling the Agencies to fulfil their statutory requirements."*

35) The SIA-wide policy statements which apply to BPD are set out at §16:

> "
>
> - *The Agencies must consider the different levels and types of intrusion and the sensitivities inherent in the exploitation of BPD; ensure that BPD is hosted and available on suitable analytical systems; and ensure that appropriate safeguards are in place to prevent and detect inappropriate use;*
>
> [REDACTED]

- *Access to analytical systems which have the ability to interrogate BPD must be restricted to those with a business need and who have an appropriate level of security clearance;*
- *Users must complete relevant training and be made aware of their responsibilities (in relation both to the analytical systems and the data they access) before they are granted use of analytical systems which can interrogate BPD. In exceptional circumstances, if an individual has not complete the relevant training and a strong business case exists for his use of analytical systems containing BPD, his use of these systems must be guided by an experienced trained colleague;*
- *Each Agency must ensure that all use of BPD, in whatever context, is necessary and proportionate to enable the Agency to fulfil its statutory obligations, and that use must be authorised at an appropriate level commensurate with the use proposed, level of intrusion and assessment of risk;*
- *Users must ensure their queries against BPD are structured and focused so as to minimise collateral intrusion;*
- *BPD may be used to conduct experiments as part of the SIA drive to improve data analytics; however, the risks arising from use in an experiment must be considered and pre-authorised by a senior manager;*

  ...
- *Physical, technological and administrative safeguards must be in place to guard against the misuse, malicious or otherwise, of BPD and the analytical systems upon which it is hosted. These safeguards include (but are not limited to) audits, protective monitoring regimes, line management oversight, training and codes of practice;*
- *The Agencies will take appropriate disciplinary action against any person identified as abusing or misusing analytical capabilities, BPD, or any information or intelligence derived therefrom."*

SIA: Sharing

36) SIA-wide policy statements in relation to sharing BPD are set out at §17:

"

- *When sharing BPD the supplying Agency must be satisfied that it is necessary and proportionate to share the date with the other Agency/Agencies; and the receiving Agency/Agencies must be satisfied that it is necessary and proportionate to acquire the data in question. A log of data sharing will be maintained by each agency;*
- *The sharing of BPD must be authorised in advance by a senior individual within each Agency, and no action to share may be taken without such authorisation;*

  ...
- *Agencies must protect sensitive datasets* [REDACTED] *when sharing, if the risk of intrusion in doing so is not judged to be necessary and proportionate;*
- *BPD must not be shared with non-SIA third parties without prior agreement from the acquiring Agency;*
- *Were BPD to be shared with overseas liaison the relevant necessity and proportionality tests for onward disclosure under the SSA or ISA would have to be met. In the event that one (UK) Agency wished to disclose externally a dataset originally acquired by another*

Agency, Action-On would have to be sought in advance from the acquiring Agency. Wider legal, political and operational risks would also have to be considered, as appropriate.

[REDACTED]

SIA: Retention

37) The Intelligence Services are also required to review the **necessity** and **proportionality** of the continued retention of BPD (§18). This is reflected in the following SIA-wide policy:

"

- *Each Agency has a review panel which will review BPD retention by that Agency. In all three Agencies, panels sit once every six months;*
- *These panels will invite representatives from each of the other Agencies to discuss data sharing (both data and applications granting access to BPD), assist consistency of decision making across Agencies, and provide inter-Agency feedback;*
- *Each Agency must provide its own justification for the retention of a dataset. Where an Agency shares a dataset with another, the receiving Agency is responsible for its copy;*
- *Different Agencies may reach different conclusions about the value of, and requirement to retain (or delete), the same dataset, based on each Agency's ongoing business requirement, and assessment of risk, necessity and proportionality;*
- *If the acquiring Agency chooses to delete a dataset, the consequences for retention must be considered by all Agencies with access to that dataset. If the other Agencies wish to retain their copy and have sufficient justification, the Agencies must also agree between them the responsibilities for managing supplier equities, source and/or technique protection. As judged appropriate, this may involve the transfer of responsibility for managing the relationship, source or capability to one of the other Agencies, or the continued supply of data by one Agency on behalf of the others;*
- *All decisions on retention (either full or partial) must be recorded;*
- *The frequency of retention reviews for BPD varies across the Agencies, but all are periods determined by similar factors, including potential use (or lack of); levels of intrusion; and levels of sensitivity and corporate risk;*
- *The level of use and Intrusion and Corporate Risk for a BPD must be re-assessed during the review process;*
- *The review period assigned to a dataset can be altered if an acceptable justification can be made. Such changes must be authorised by the review panel and the justification recorded."*

SIA: Deletion/Destruction

38) Finally, the SIA Bulk Personal Data Policy sets out policy statements relating to the disposal of BPD, which reflect the *"legal requirement for the Agencies not to hold BPD for longer than is deemed necessary and proportionate."* (§19):

"

- *The review panel will instruct the deletion/destruction of BPD when its retention is no longer necessary and proportionate. BPD will not be archived unless there is a legal justification such as disclosure;*
- *If the primary acquiring Agency has to delete a dataset (e.g. following a Commissioner's intervention, or at the request of a data supplier) and one or both of the other Agencies decide to retain the data, the other Agencies must also review their justification for retention of the same dataset. The standard of justification for any ongoing retention in such circumstances is likely to be high;*
- *If one or both of the other Agencies decide to retain the data, the Agencies must agree between them the responsibilities for managing the data* [REDACTED]*;*
- *Where a dataset is to be deleted/destroyed by an Agency, it must consider any previous sharing of the data with liaison partners (e.g. foreign agencies, police, OGDs). Depending on the circumstances surrounding the deletion/destruction, a decision must be made as to whether to ask third parties to delete/destroy their copy or extract of the dataset. If the decision is to request deletion, the request must be made even if there is little prospect of being able to enforce deletion/destruction by the third party;*
- *The review panel can request the deletion/destruction of certain fields/criteria from within a dataset if they are not deemed to be necessary and proportionate whilst retaining the remainder of the dataset;*
- *The Agencies' relevant technical sections are responsible for conducting the deletion/destruction of the dataset.* [REDACTED]"

MI5

Introduction

39) MI5 has Closed Handling Arrangements for the obtaining and disclosing of Bulk Personal Data ("the MI5 Closed BPD Handling Arrangements"). These are made pursuant to section 2(2)(a) of the Security Service Act 1989 (see the MI5 Closed BPD Handling Arrangements, §1.1, §2.8). These came into force on 4 November 2015. A copy of the MI5 Closed BPD Handling Arrangements is exhibited at Exhibit **"B"** to this Closed Response.

40) The MI5 Closed BPD Handling Arrangements apply to MI5's management (acquisition, use, disclosure and retention) and oversight of the category of "bulk personal data" (§1.2). They are mandatory and must be followed by all staff (§1.3). Failure to comply with the Handling Arrangements may lead to disciplinary action, which can include dismissal (§1.3). For clarity, mandatory requirements are set out in boxes at the end of each section (§1.4).

41) The information to which the MI5 Closed BPD Handling Arrangements relate is defined in section 2. §2.1 notes that MI5 *"lawfully collects BPD from a range of sources to meet its statutory functions."* The definition of "Bulk Personal Dataset" is agreed by each of the SIA. The definition of "Bulk Personal Dataset" at §§2.2-2.3 mirrors the SIA BPD Policy (§2).

42) In line with the Open Handling Arrangements and SIA Closed BPD Policy, the terms "personal data" and "Sensitive Personal Data" are defined (at §2.4 and §2.5) as having the meanings given to them in section 1(1) and 2 of the Data Protection Act 1998.

43) §2.6 notes that the categories of sensitive personal data are non-exhaustive, as MI5 takes into account other additional sensitive categories including, but not limited to *"legal professional privilege, journalistic material and financial data."* (§2.6)

44) §2.7 notes that responsibility for governance arrangements for BPD lies with MI5's data governance team. The data governance team:

> *"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 lifecycle."*

45) The statutory powers by which MI5 can acquire BPD is set out at §§2.9-2.10. §2.11 sets out that the MI5 Closed Handling Arrangements must be followed even where the exercise of certain of those statutory powers requires compliance with other warrantry or authorisation processes in parallel.

46) Section 3.0 of the MI5 Closed BPD Handling Arrangements summarises the relevant provisions of the SSA, CTA, HRA and DPA.

47) The MI5 Closed BPD Handling Arrangements set out the arrangements in relation to

a) Authorisation;
b) Acquisition;
c) Use;
d) Disclosure;
e) Data Retention and Review; and
f) Oversight.

MI5: Authorisation

48) Any acquisition of a BPD must be authorised. The authorisation process is set out in detail at §4.1.4. Whenever MI5 considers acquiring a BPD, the officers responsible for acquiring it must first consider the **necessity** and **proportionality** of doing so at the earliest possible stage, having regard in particular to the following series of questions (§4.1.2):

"

a) *What is the likely content of the dataset?* [REDACTED]

b) *What business requirements*[1] *will be met by acquiring and using the dataset?*

[1] The MI5 "*business requirements*" which must be met are set by the relevant teams working to counter threats to national security (§4.1.1).

c) *How is exploitation of the dataset likely to contribute to MI5 business requirements?*

d) *How intrusive will acquisition and use of the data be, with particular reference to the degree of collateral intrusion?*

e) *Can the intelligence be obtained by other, less intrusive, means?"*

49) The authorisation process requires the completion of the relevant form (an example of which is exhibited to this Closed Response at Exhibit "**C**") (§4.1.4). The relevant form *must* be used where there is an intention to acquire BPD (§4.1.3) and must be supported by a business case approved by a senior MI5 official.[2]

50) §4.1.4 sets out the detailed authorisation process:

"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 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 adviser 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 significant 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.

---

[2] This would be at a level broadly equivalent in seniority to the Senior Civil Service.

- Once authorised, the completed application must be stored on a centrally receivable 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."

51) Specific guidance is given on how to decide whether acquisition is **necessary** and **proportionate** (§§4.1.5-4.1.7). Necessity is recognised as a matter of fact and judgment, taking all the relevant circumstances into account (§4.1.5). Staff are directed to 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."* (§4.1.5)

52) In relation to proportionality, MI5 staff are directed to 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. "Privacy" in this context is said to relate both to subjects of interest who are included in the relevant data and other individuals who are included in the data and who may be of no intelligence interest (§4.1.6). This means that 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."* They must also consider whether there is a *"reasonable alternative"* which *"involves less intrusion"* that will still meet the proposed objective (§4.1.6).

53) In difficult cases, staff should consult line or senior management and/or the legal advisors for guidance. They may also seek guidance or a decision from the relevant Secretary of State (§4.1.7).

[REDACTED]

MI5: Acquisitions

54) §4.2.1 notes the wide range of sources from which MI5 acquires BPD (such as SIA Partners, other HMG Departments, private business, interception and CNE). §4.2.2 sets out the broad categories of MI5's acquired datasets.

[REDACTED]

55) Transfer of BPD within MI5 is also tightly controlled.

MI5: Use

56) The MI5 Closed BPD Handling Arrangements set out requirements in relation to access to BPD which are intended to (i) ensure the maintenance of data security and protective security

standards; and (ii) reinforce compliance in relation to the necessity and proportionality of using BPD datasets (§5.1).

57) §5.1.1 states that:

> *"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."*

58) Compliance with the requirement to consider the necessity and proportionality of using BPD is reinforced by the additional measures at §5.1.2:

> *"- 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."*

59) Specific measures are also set out for the reduction of the level of interference with privacy arising from the acquisition and use of BPD (§5.1.3):

"-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."

60) MI5 staff can only access the corporate analytical systems through which BPD is primarily accessed after (i) reading and signing a Code of Practice (exhibited to this Closed Response as Exhibit "**D**"); and (ii) after completing a mandatory training course (§5.2.1). The conduct and training of such users are subject to the responsibility of a line manager (§5.2.2).

61) In addition to the above specific mandatory training and specialist mentoring, other training and courses are available to MI5 officers:

a) Legal Awareness Course;
b) Information Assurance Course;
c) [REDACTION] (MI5 internal intranet) guidance and policy documents relating to BPD.

62) Exploitation of BPD is subject to arrangements.

63) The use of BPD for *"experimental or innovation purposes"*, for example, the development of a novel analytical technique or testing a new IT system, is specifically addressed at §5.4.1. The potential for increased risk to, inter alia, the security of the data and risk of additional interference with the right to privacy are acknowledged and addressed. Any such use of BPD must be specifically *"considered and authorised in advance by a senior MI5 official."* A request for authorisation must describe the proposed activity and, inter alia, explain why it is necessary and proportionate to use BPD for this purpose and set out an assessment of the expected interference with privacy. The person authorising the requested experimental use may set conditions or restrictions on its use (§5.4.2), and such conditions/restrictions must be retained as part of the record for the dataset. If the request for experimental use is declined, the dataset must not be used for that purpose.

MI5: Disclosure

64) The MI5 Closed BPD Handling Arrangements specifically address the disclosure of BPD, i.e. sharing BPD outside MI5.

65) The decision to share any BPD outside MI5 *"rests with a senior MI5 official."* (§6.1) Specific arrangements are set out in relation to (i) Disclosure within the SIA; and (ii) Disclosure to liaison services.

66) Information in BPD held by MI5 can only be disclosed to persons outside MI5 if all of the following conditions are met (§6.2.1):

a) 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 Intelligence Services Act 1994 and section 2(2)(a) of the Security Service Act 1989;

b) It is necessary to disclose the information in question in order to achieve that objective;

c) The disclosure is proportionate to the objective;

d) Only as much of the information will be disclosed as is necessary to achieve that objective.

67) These conditions must be met for *all* disclosure, including between the Intelligence Services (§6.2.4).

68) §6.2.2 addresses the requirement of necessity, noting that MI5 staff must be satisfied that disclosure is "really needed" for the purpose of discharging a statutory function of MI5 and whether there is a reasonable, and less intrusive, alternative that will still meet the proposed objective (§6.2.2). An example of such an alternative is given: *"this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal data."*

69) §6.2.3 addresses proportionality. 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."*

70) Where the conditions are met, the BPD is formally requested from MI5 through an agreed disclosure procedure using an "Inter-Agency Data disclosure Form" (§6.2.5). The relevant MI5 data sponsor will then seek internal MI5 authorisation by submitting a Form for Sharing, which is exhibited to this Closed Response at Exhibit "**F**". The Form for Sharing will:

> *"outline[..] 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."* (§6.2.6)

71) Disclosure is only permitted once this authorisation process is completed (§6.2.5). Arrangements will then be made for the data to be disclosed to the relevant Agency (§6.2.6).

72) Disclosure to liaison services is subject to additional safeguards.

73) However, §6.3.2 notes that there are circumstances *"such as a pressing operational requirement"* where disclosure to a liaison service may be necessary and proportionate in the interests of national security. In such a case, in addition to applying the same tests for disclosure as when disclosing within the SIA, the relevant form would have to be completed, and MI5 would need to be satisfied that disclosure met the dual tests of necessity and proportionality.

74) In addition, prior to disclosure, MI5 must also 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. All enquiries *"should be directed to the data governance team."* (§6.3.2)

75) The necessity and proportionality of any disclosure of BPD is also subject to review by MI5's Bulk Personal Data Review panel. The panel also reviews whether the interests of the data provider are protected (§7.1.6).

MI5: Review of data retention and deletion

76) The retention and use of BPD in MI5's possession is reviewed by MI5's Bulk Personal Data Review ("BPDR") Panel (§7.1.3). The Panel consists of, amongst others, senior officials, non-executive director, Ethics Counsellor and legal adviser.

77) The BPDR panel meets at least every six months to conduct such a review (§7.1.1). Representatives from SIS and GCHQ are normally invited to attend to observe and contribute to discussions (§7.1.4). The purpose of the review is to ensure that the retention and use of datasets in MI5's possession:

> *"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."*

78) In addition to satisfying themselves that the level of intrusion is justifiable under Article 8(2) of the ECHR, the BPDR panel must also be satisfied that it complies with the requirements of the Data Protection Act 1998 (§7.1.2). If at any time, including on a review, it is judged that MI5's retention of BPD is no longer necessary and proportionate *"all copies must be deleted or destroyed."* (§7.1.2)

[REDACTED]

79) The BPDR panel considers recommendations for each dataset under review and decides whether to retain or delete it (§7.1.5). When doing so the panel considers (§7.1.8):

> *"- 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"*

80) When a dataset is retained, it is given a retention review period of six to 24 months *"in accordance with the level of intrusion and risk posed by the retention and use of the dataset"* (§7.1.5). If the panel cannot agree on whether a dataset should be retained or deleted, the chair must seek advice and a decision from MI5's Deputy Director-General (§7.1.7). New datasets are subject to an initial full review at the first BPDR meeting after acquisition in order to ensure that the acquisition process has been properly followed (§7.1.5). This initial review (at the first BPDR meeting after acquisition) may proceed on the basis of the applicable acquisition form.

81) When a decision has been reached to delete BPD, its destruction is tasked to technical teams responsible for retention and deletion. Confirmation of complete deletion must be recorded with the data governance team and an update provided to the next BPDR panel meeting. Information specialists provide technical reassurance surrounding the deletion and destruction of the dataset (§7.2.1).

MI5: Oversight

82) MI5's use of BPD is subject to both internal and external oversight (§8.0).

83) The Chair of the BPDR Panel (a senior MI5 official) is a member of MI5's Executive Board, and keeps the Board apprised of MI5's bulk data holdings. In addition, use of BPD is audited in order to detect misuse or activity which gives rise to security concerns, either of which could lead to disciplinary action:

> *"§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."*

84) All audit investigations are available to the Intelligence Services Commissioner for scrutiny (§8.2.2).

85) The external oversight provided by the Intelligence Services Commissioner is specifically addressed at §8.3:

> ***"8.3 External Oversight***

8.3.1 The acquisition, use, retention and disclosure 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 judgments 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.

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 ...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."

MI5: Past policies and practice

86) In the period from 1 June 2014 (1 year prior to the issue of the present claim) and 4 November 2015, MI5's policies in relation to BPD were similar to those now in force.

87) As at 1 June 2014 MI5 had in place a "Policy for Bulk Data Acquisition, Sharing, Retention & Deletion". This had been in force since October 2010. A copy of this policy is exhibited to this Closed Response at Exhibit "**H**". In summary, it required:

a) Any acquisition and subsequent retention of BPD to be justified as necessary and proportionate by weighing up the value of the BPD against any resultant interference with privacy (p.4);

b) Legal Adviser's advice to be sought in relation to necessity and proportionality in cases of doubt (p.4);

c) Removal of extraneous sensitive/confidential data (such as data about large numbers of minors, details of earnings or medical information) (p.4)

d) Secure acquisition and storage of any BPD (pp.5-6);

e) Access to BPD to be limited to those with a business need and to those who had signed the necessary Code of Practice and completed necessary training (p.6);

f) All use and searches of BPD is limited to what is necessary and proportionate (p.7);

g) Disciplinary action to be taken against any person abusing their access (p.7);

h) Six-monthly reviews of BPD holdings by the Bulk Data Review Panel, to ensure its acquisition and retention was necessary and proportionate to enable MI5 to carry out its statutory functions (p.7);

i) Sharing of BPD with other Intelligence Services to be subject to necessity and proportionality considerations and to the approval of senior MI5 officials, and for the filtering out of any unnecessary data (pp.7-8);

j) Acquisition of BPD from other Intelligence Services to be subject to similar safeguards (p.8);

k) Deletion of data by secure means once its retention was no longer considered justified (p.9);

l) External oversight over BPD by the Intelligence Services Commissioner (p.10).

88) Annex A to the 2010 policy set out further guidance for staff in relation to these areas. In addition guidance was set out at an Annex to the 2010 policy in relation to how to complete the necessary forms (including setting out assessments of necessity and proportionality) and as to how to assess intrusion into privacy, including collateral intrusion, deletion and acquiring BPD from/sharing BPD with other Intelligence Services (Annex A).

89) In addition, as already set out above, from February 2015 the SIA BPD Policy was in force and replaced the 2010 policy.

90) Finally, as noted at §119 of the Open Response, prior to the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015, which came into force on 13 March 2015, BPD was already (including during the period June 2014 onwards) subject to the non-statutory oversight of the Intelligence Services Commissioner.

SIS

Introduction

91) SIS also has Closed Handling Arrangements for the acquisition, use, disclosure, retention and oversight of BPD ("the SIS Closed BPD Handling Arrangements"). They were made under section 2(2)(a) of the Intelligence Services Act 1994 and came into force on 4 November 2015. They are exhibited to this Closed Response at Exhibit "**I**".

92) §1.0.3 emphasises the mandatory nature of the SIS Closed BPD Handling Arrangements and the serious consequences of non-compliance:

> *"**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."*

93) For clarity, mandatory requirements are set out in boxes at the end of each section.

94) The information covered by the SIS Closed BPD Handling Arrangements is defined at §§1.1.5 to 1.1.8. The definition of Bulk Personal Dataset is the same as that used by other Intelligence Services. Like the other Agencies, SIS also adopts the definitions of "personal data" and "sensitive personal data" found in the Data Protection Act 1998.

95) §1.1.9 explains that responsibility for governance arrangements for BPD lies with a designated directorate, which:

> *"works in consultation with the operational, legal and policy directorates to understand operational requirements for BPD and ensure that BPD are subject to appropriate handling and protection throughout their lifecycle."*

96) A non-exhaustive list of the statutory powers by which SIS can acquire BPD is set out at §1.1.11. §1.1.12 sets out that the SIS Closed Handling Arrangements must be followed even where the exercise of certain of those statutory powers requires compliance with other warrantry or authorisation processes in parallel.

97) External oversight is addressed at §1.1.13:

> *"Oversight of the obtaining, use, retention and disclosure by the SIA of BPD is provided by the Intelligence Services Commissioner pursuant to the direction given by the Prime Minister on 12 March 2015, except where the oversight of such datasets already falls within the statutory remit of the Interception of Communications Commissioner."*

98) Section 2.0 of the SIS Closed BPD Handling Arrangements summarises the relevant principles of the ISA, CTA, HRA and DPA.

99) The SIS Closed BPD Handling Arrangements set out the arrangements in relation to:

a) Acquisition;
b) Authorisation;
c) Use;
d) Training;
e) Disclosure;
f) Data Retention and Review; and
g) Oversight.

SIS: Acquisition

100) Section 3.0 of the SIS Closed BPD Handling Arrangements sets out arrangements in relation to acquisition of BPD.

101) Management of BPD within SIS is the responsibility of a designated directorate.

102) SIS's consideration of whether to seek BPD is guided by the National Security Council ("NSC") priorities, which in turn guide [REDACTION], i.e. its intelligence collection priorities and effects for the coming year (§3.0.2).

103) SIS's sources of BPD include SIA partners and other HMG departments (§3.1.1). Types of BPD acquired broadly fall into the following categories: (§3.1.2):

"- Population – these datasets provide population data or other information which could be used to help identify individuals e.g. passport details

- Travel – these datasets contain information which enable the identification of individuals' travel activity.

- Financial – these datasets allow the identification of finance related activity of individuals.

- Communications – these datasets allow the identification of individuals where the basis of information held is primarily related to communications data e.g. a telephone directory."

[REDACTED]

104) Whenever SIS considers acquiring a Bulk Personal Dataset, the officers responsible for acquiring it must first consider the **necessity** and **proportionality** of doing so at the earliest possible stage (§3.1.4).

105) Necessity is recognised as a matter of fact and judgment, taking all the relevant circumstances into account (§3.1.5). Staff are directed to consider *"why obtaining the BPD is really needed for the purpose of discharging one or more of SIS's statutory functions."* 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."* (§3.1.5)

106) In relation to proportionality, SIS staff are directed to 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. "Privacy" in this context is said to relate both to subjects of interest

who are included in the relevant data and other individuals who are included in the data and who may be of no intelligence interest (§3.1.6) This means that 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."* They must also consider whether there is a *"reasonable alternative"* which *"involves less intrusion"* that will still meet the proposed objective (§3.1.6).

107) In difficult cases, staff should consult line or senior management and/or the legal advisors for guidance. They may also seek guidance or a decision from the Secretary of State for Foreign and Commonwealth Affairs (§3.1.7).

[REDACTED]

108) Safeguards exist for the storage of newly acquired data. [REDACTED]

SIS: Authorisation

109) Before a dataset is ingested for use by SIS, it is subjected to the authorisation process. Officers with relevant expertise and seniority consider and record the operational, policy and legal implications of holding and using the dataset. This culminates in a decision by [REDACTED] the head of the BPD authorisation team, having regard to all of these factors (§4.1.1).

110) The considerations are formally recorded on the relevant form (found at Annex A to the SIS Closed BPD Handling Arrangements, and exhibited to this Closed Response at exhibit "**J**").

111) The authorisation process comprises two stages: (i) assessment and (ii) authorisation. Assessment is carried out by a member of the relevant team (§4.2.1). [REDACTED]

112) No bulk dataset can be exploited on an SIS system without a completed authorisation being in place. [REDACTED]

113) The Bulk Data management team [REDACTED] is responsible for co-ordinating the authorisation process and to ensure that *"officers are aware of their responsibilities in the process."* (§4.3.3) All BPD must be authorised for retention or use within 6 months of acquisition *"save in exceptional circumstances"* (§4.3.4). If no adequate case can be made for BPD retention or use it will be deleted immediately (§4.3.4).

SIS: Use

114) The SIS Closed BPD Handling Arrangements address use by reference to (i) Access to BPD and (ii) Exploitation of BPD.

(i) Access

115) There are tight controls on access to BPD. [REDACTED]

116) SIS staff can only access BPD if there is an appropriate business case to do so. Use requires line manager approval and mandatory training.

[REDACTED]

117) Applicants are required to explain how they would use the database in their current role, and also:

a) *"Please explain why your use of the database would be necessary for the Service to exercise its functions for the purposes of national security, the economic wellbeing of the UK or the detection/prevention of serious crime."*

b) *"How would your use of the database be proportionate to fulfilling the Service's functions – for example is there a less intrusive way for you to achieve the same objective without access to the database data?"*

118) The Code of Practice also emphasises the importance of necessity and proportionality:

"2. Why is this Code of Practice necessary?

We need to share and exploit the information we hold both effectively and in accordance with the law. The database is a powerful data exploitation tool. But its use brings some information sharing risks. ***These need to be managed to ensure that the privacy of those whose data is within the database is respected and that data is held, accessed and disclosed only to the extent necessary for the purpose of our statutory functions and proportionate to those aims.*** *We get maximum value from the database by making its contents available to all users. This requires all users to act responsibly. It is extremely important that all users understand, and comply with, the legal requirements and record keeping conventions that apply to their use of the database.*

To do their jobs, the database users are given access to a wide range of data, which will include many individuals of no intelligence interest. ***For this reason searching and using bulk data are particularly sensitive activities, requiring careful consideration and strict adherence by users to that which is necessary and proportionate for their work.*** *"*

"C has a legal duty to ensure that there are arrangements in place to prevent the Service from disclosing material it obtains "except so far as necessary for the proper discharge of its functions." This obligation applies equally to disclosure to persons within and outside the Service. ***Whilst the database may afford you the potential to view information and/or data that you do not have a need to know, it is your duty and responsibility to avoid doing so.*** *" (§3)*

"Section 6 of the Human Rights Act 1998 states that it is unlawful for a public authority to breach any of the rights guaranteed by the European Convention on Human Rights.

These include the right to privacy (article 8). ***Access to data on the database will involve an interference with privacy. Under article 8 this can only be justified if it is necessary for the purposes of our functions and proportionate to what we are seeking to achieve.***"

"***The database must not be a 'free for all'.*** *Users will have potential access to* [REDACTED] *sensitive material. The Service's information policy and practices are designed to be compliant with the law, which dictates that users' actual access to information is limited to that which is necessary and proportionate for their work. Misuse of information, including unjustified and/or inappropriate access, would be unlawful and could in some circumstances constitute a criminal offence.*"

(emphasis added)

119) The responsibilities of line managers for ensuring proper use of the database, particularly with privacy in mind, is stressed in Section 8:

"*The database needs to be used in a way that ensures the privacy of individuals whose data is within the database. Data must be held, accessed, searched and disclosed only to the extent necessary for the purposes of SIS statutory functions and proportionate to those aims.*

Line managers of the database users are required to ensure their staff members with access to the database have agreed to comply with the Code of Practice and are aware of their responsibilities set out above."

120) Section 4 ("Conduct and Behaviour") sets out a non-exhaustive list of prohibited database activity which "will be regarded as a serious abuse of the system" and "could be unlawful and even amount to a criminal offence." They include:

"***You must not use the database to search for and/or access information other than that which is necessary and proportionate for your current work****. This includes (but is not limited to) searching for information about other members of staff, neighbours, friends, acquaintances, family members and public figures,* ***unless*** *it is necessary to do so as part of your official duties. You should be prepared to justify any searches you do make.*"

"***You must not use the database to search on your own records*** *(eg. to obtain your passport number). This is to avoid unnecessary collateral intrusion into the personal data of others. In certain circumstances, it may be acceptable to conduct a search on your own details as part of your official duties. You should not conduct a search until you have consulted the relevant team, who will advise on the proportionality issues.*"

"***You must not share information and intelligence derived from the database in a way that is not necessary, proportionate and within the remit of the Service and appropriate to your current role and responsibilities.***"

"The database users are able to export the results of their searches into Excel and Word. However users must remain mindful that subset results from the database still represent bulk personal data. As such results should only be disseminated to colleagues that the user has satisfied have a business requirement and where it remains proportionate for them to see the information. It is most important that the database Action On process is followed for each trace derived from SIS's bulk data holdings which are to be passed beyond SIA customers."

121) Users are informed that they *"may be subject to random and routine spot checks to explain their activities on the database at any time."* and that:

"over and above Security Department system audits, they may also be required to account for recent searches to the Intelligence Services Commissioner, as part of his regular scrutiny of the Service's work."

122) The seriousness of misuse of the database is again emphasised in Section 7 "Breach of Secops"[3]:

"The Service will take disciplinary action against any abuse or misuse of the database, or information and intelligence derived from it. This includes, but is not restricted to, those activities expressly identified under Conduct and Behaviour above. For staff, offences will be handled in accordance with the Service's disciplinary procedures.

Staff should be aware that deliberate or serious abuse of electronic facilities could amount to gross misconduct and may result in dismissal. For secondees, contractors and consultants, such misconduct is similarly likely to result in removal from site. In all cases, fitness to hold DV will also be examined. Furthermore, activity that cannot be justified by reference to our functions would be likely to be unlawful in article 8 terms and could in some cases even constitute a criminal offence."

[REDACTED]

123) SIS can also carry out operational experiments on data to fulfil intelligence requirements. [REDACTED]. It has its own security and access safeguards. [REDACTED]

(ii) Exploitation

124) Tight controls are also placed on the exploitation of data. [REDACTED]

SIS: Training

125) Training is addressed in Section 6 of the SIS Closed BPD Handling Arrangements. SIS staff are required to complete mandatory training as part of the application process to access analytical tools. [REDACTED] Advanced analysts complete not only mandatory training but

[3] "Secops" is an abbreviation of "Security Operating Procedures".

also supplementary training which includes guidance to support them in their authorisation, transformation and analysis tasks.

126) Further training is available, and in some cases mandatory for SIS officers generally (§6.0.3). This includes Operational Management and Compliance courses, the Legal Compliance with Data Course and Legal Adviser briefings.

SIS: Disclosure

127) Disclosure of BPD must only occur when permitted under the relevant statutory gateway. The decision to share a BPD outside SIS rests with [REDACTED] a senior manager in a designated directorate.

128) Whilst whether or not any BPD is shared with liaison services is neither confirmed nor denied, the SIS Closed BPD Handling Arrangements set out different levels of safeguards in relation to whether disclosure is (i) within the SIA or (ii) with liaison services.

129) BPD (including a subset of the BPD or an individual piece of data) acquired by SIS can be disclosed within SIA only if the following conditions are met (§§7.2.1-7.2.3):

> *"7.2.2 Disclosure must be 'necessary'. In order to meet this requirement, staff must be satisfied that disclosure of the BPD is 'really needed' for the purpose of discharging a statutory function of that Agency.*
>
> *7.2.3 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 SIS's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. 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."*

130) An SIA partner wishing to use a BPD acquired by SIS must follow the Data Sharing Process. [REDACTED]

131) Were BPD acquired by SIS to be disclosed to liaison services, such disclosure would be subject to the same conditions set out in §§7.2.2-7.2.5 but, in addition, further conditions would have to be met, including:

> *"As part of SIS's analysis of whether disclosure is in line with its legal obligations, in the event that SIS shares BPD with a liaison service, SIS would require any such service to agree to rigorous requirements in relation to the safeguarding of that BPD. These safeguards would cover, amongst other things, access to the BPD, use (in terms of systems as well as purpose), and onward disclosure and will be set out on handling instructions that accompany each BPD."* (§7.3.1)

SIS: Data Retention and Review

132) SIS has a Dataset Retention and Review Panel ("DRR") which meets every six months to review BPD (§8.0.1). The review is a formal process. The panel comprises a number of members including senior officials and a legal representative. Representatives from MI5 and GCHQ are also normally invited to attend to observe and contribute to discussion.

133) The aim of the DRR is stated in §8.0.2:

> *"The aim of the panel is to ensure that BPD are only retained by SIS where necessary and proportionate to enable SIS to carry out its statutory functions. When a dataset is authorised for retention, it will be given a retention period in accordance with the level of intrusion posed by the retention and use of the dataset. This retention period determines the frequency with which the dataset is reviewed by the DRR. On review, DRR members must satisfy themselves that the levels of intrusion are justifiable under SIS's governing legislation (including Article 8(2) ECHR 1998 and the DPA 1998). If it is judged (at any time, but including on review) that it is no longer necessary and proportionate to retain a dataset, it will be deleted."*

[REDACTED]

134) Consideration of the necessity and proportionality of retaining a dataset involves consideration by the DRR of the following matters set out at §8.0.3:

> *"– Use of the dataset, including action taken by SIS as a result of use.*
>
> *– The level of actual and collateral intrusion posed by retention and exploitation*
>
> *– Potential corporate, legal, reputational and political risk.*
>
> *– Frequency of acquisition and updates*
>
> *– Whether such information could be acquired elsewhere through less intrusive means.*
>
> *– The operational and legal justification for continued retention, including its necessity and proportionality.*
>
> *– Frequency of review of retention*
>
> *– Whether any caveats or restrictions should be applied."*

135) Recommendations are provided by relevant SIS teams in respect of each dataset. These recommendations are considered by DRR which decides whether to retain the dataset or to delete it. In particularly sensitive cases, the Panel may recommend an earlier review (§8.0.4).

[REDACTED]

136) Removal or deletion of data may only be undertaken by the relevant team who are the only officers with the appropriate access rights and technical knowledge to do so (§8.0.6).

137) The DRR's decisions are recorded and made available for consideration at a more senior level:

> *"8.0.7 The DRR panel report is formally recorded and passed to a senior SIS official who can raise relevant points to the SIS Executive Committee or SIS Board as necessary. A summarised version of the report and a list of SIS BPD holdings are also made available for the SoSFCA."*

SIS: Oversight

138) SIS's use of BPD is subject to a number of different forms of oversight, namely:

a) SIS internal audit;

b) Ministerial oversight; and

c) External oversight by the Intelligence Services Commissioner.

139) SIS has an audit team, which carries out investigations into analyst searches on SIS's databases.

[REDACTED]

140) All audit investigations are available to the Intelligence Services Commissioner for scrutiny (§9.1.4).

141) The Commissioner also spot checks all analysis [REDACTED] (§9.1.5):

> *"All analysts, if selected, would be expected to justify their searches in front of the IS Commissioner."*

142) As a matter of practice, the Commissioner considers a number of matters in relation to BPD during his visits, including:

a) BPD policies;

b) Authorisations;

c) Search justifications;

d) SIS audit investigations; and

e) Future innovation and planned changes.

143) Ministerial oversight is present in the form of the seeking of political clearance in particularly sensitive cases (§9.2.1):

> *"SIS does not routinely seek Ministerial approval for the acquisition or use of BPD. However, in acquisition operations where there is a risk that a particular activity could either cause significant embarrassment to HMG, or would conflict with or prejudice the policies of HMG, SIS would seek political clearance before proceeding. A submission seeking political clearance from SoSFCA would also give detail on the dataset which SIS was trying to acquire. In the last year the relevant team has sought clearance on one occasion."*

144) In addition the Secretary of State for Foreign and Commonwealth Affairs receives a copy of all DRR minutes, and will accordingly be kept aware of the scale of the BPD holdings and issues raised around retention of BPD.

145) The Intelligence Services Commissioner's oversight is summarised at §§9.3.1-9.3.3:

> *"9.3.1 Oversight of BPD is provided by the IS Commissioner pursuant to the direction given by the Prime Minister on 12 March 2015. The IS Commissioner scrutinises SIS's authorisations and use of BPD, including the audit of BPD, and makes twice yearly scrutiny visits.*
>
> *9.3.2 The purpose of the Commissioner's oversight is to review and test SIS judgments on the necessity and proportionality of acquiring and using BPD and to ensure that SIS policies and procedures for the control of, and access to, these datasets is both sound and strictly observed. SIS aims for the IS Commissioner to be able to report positively to the Prime Minister on its arrangements for working with and handling of BPD.*
>
> *9.3.3 All papers requested by the IS Commissioner must be made available to him. Those papers include, but are not limited to the following:*
> *- Selected Data Authorisations*
> *- Selected Audit challenges*
> *- All Audits challenges which require further investigation (i.e. potential audits resulting from the misuse of BPD)*
> *- A list of current datasets available for exploitation in SIS*
> *- The minutes of the previous Data Retention Review*
> *- Papers outlining any changes to current BPD policies."*

SIS: Past policy and practice

146) SIS's policy and practice in respect of BPD throughout the relevant period (June 2014 onwards) was similar to that set out in the Handling Arrangements which are now in force.

147) In September 2014 a new directorate with responsibility for BPD was created.

148) In October 2014 a new Code of Practice was introduced which expressly prohibited 'self-searching', highlighted the risk of collateral intrusion and included a re-training exercise for all users. [REDACTED]

149) From February 2015 the SIA BPD Policy was in force. In June 2015 a new team was created within SIS to oversee bulk data management and compliance.

150) In addition, as noted at §119 of the Open Response, prior to the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015, which came into force on 13 March 2015, BPD was already (including during the period June 2014 onwards) subject to the non-statutory oversight of the Intelligence Services Commissioner.

GCHQ

151) GCHQ has substantial "below the waterline" safeguards for the obtaining, use and disclosure of BPD. These are set out in (i) GCHQ's Closed Handling Arrangements for the obtaining, use and disclosure of BPD ("the GCHQ Closed BPD Handling Arrangements"), which were made under section 4(2) of the Intelligence Services Act 1994 and came into force on 4 November 2015 (and are exhibited at Exhibit "**O**" to this Closed Response; and (ii) other internal policy/guidance, in particular its Compliance Guide, Intelligence Sharing and Release Policy, the Reporter's Handbook and Reporting Standards.

152) §1.3 of the GCHQ Closed BPD Handling Arrangements emphasises their mandatory nature and the serious consequences of non-compliance:

> *"The rules set out in these arrangements are mandatory and must be followed by GCHQ staff. Failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal, and potentially to criminal prosecution."*

153) The information covered by the GCHQ Closed BPD Handling Arrangements is defined at §§2.1 to 2.4. The terms "personal data" and "Sensitive Personal Data" are defined (at §§2.3-2.4) as having the meanings given to them in section 1(1) and 2 of the Data Protection Act 1998. In addition, GCHQ treats other categories, including but not limited to legal professional privilege, journalistic material, and financial data, as sensitive (§2.5).

154) The statutory powers by which GCHQ obtains BPD are set out at §2.6:

> *"GCHQ acquires bulk personal datasets from a variety of sources and uses them to support the performance of its statutory functions, as defined in section 3(1) of ISA. Bulk personal datasets may be obtained under section 4(2)(a) of ISA by agreement with third-party voluntary suppliers and by other non-covert access methods, and also by the exercise of other statutory powers. These statutory powers include those exercisable under warrants and authorisations issued under Section 5 and Section 7 of ISA in respect*

of property and equipment interference, and warrants issued under Section 5 of the Regulation of Investigatory Powers Act 2000 (RIPA) for the interception of communications. More information on these laws and on other relevant laws may be found in the "Overview" and "Laws" sections of GCHQ's Compliance Guide."

155) The interference with individuals' right to privacy is specifically addressed at §2.7:

"Although bulk personal datasets constitute only a tiny proportion of the data GCHQ obtains, its possession and use of such datasets represent a significant interference with many people's right to privacy under the European Convention on Human Rights (ECHR). This interference must be justified in terms of its necessity and proportionality, in accordance with Article 8(2) of the ECHR. The use of such data for operational purposes is also especially sensitive and carries an elevated degree of corporate risk. GCHQ has therefore established special arrangements to ensure appropriate handling of such data throughout its lifecycle, both within and, where applicable, beyond GCHQ."

156) The GCHQ Closed BPD Handling Arrangements set out the arrangements in relation to:

a) Acquisition;
b) Authorisation;
c) Use;
d) Experimental use;
e) Disclosure;
f) Continued Retention;
g) Deletion; and
h) Oversight.

Overview

157) The importance of **necessity** and **proportionality** to each of the stages of the BPD lifecycle is emphasised at §3.2:

"Considerations of necessity and proportionality underpin each stage; no bulk personal dataset may be acquired, used for operational purposes, disclosed to other organisations, or retained unless it can be demonstrated to the satisfaction of the Authoriser (see paragraph 3.5 below) that it is genuinely necessary to do so for legitimate operational purposes and that doing so is a proportionate way of addressing these purposes."

158) Necessity is explained (§3.3):

"In this context, "necessary" means "really needed" for the purpose of discharging one or more of GCHQ's statutory functions."

159) Proportionality is also explained (§3.4):

" "Proportionate" means that the level of interference with the individual's right to privacy is justified when measured against the anticipated benefit to the discharge of GCHQ's statutory functions and the importance of the objective to be achieved. Staff must weigh (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest and to people of no intelligence interest whose data are included in the dataset, against (b) the operational value they expect to derive from the data. Staff must also consider whether there is a reasonable alternative way of achieving the objective that involves less intrusion."

160) In addition, GCHQ's Compliance Guide[4] requires all GCHQ operational activity, including BPD activity, to be carried out in accordance with three core principles. These are that all operational activity must be:

a) Authorised (generally through a warrant or equivalent legal authorisation;

b) Necessary for one of GCHQ's operational purposes; and

c) Proportionate.

(see Compliance Guide – Overview)

161) These principles, and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the GCHQ Closed BPD Handling Arrangements. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including BPD.

GCHQ: Acquisition and Authorisation

162) §3.5 of the GCHQ Closed BPD Handling Arrangements notes that:

"In accordance with the joint SIA Bulk Personal Data Policy, the following stages in a bulk personal dataset's lifecycle are subject to formal authorisation by a senior member of staff:
- acquisition and use for operational purposes;
- use for a novel or experimental purpose;
- disclosure of the dataset to another organisation; and
- continued retention and use of the dataset."

163) §3.8 explains that the purposes of the authorisation processes described in the GCHQ Closed BPD Handling Arrangements are:

"to ensure that:

[4] The Compliance Guide is a document which is made available electronically to all GCHQ staff. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner.

- GCHQ's use of bulk personal datasets for operational purposes is genuinely necessary and is proportionate to the outcomes it seeks to achieve;
- these factors have been properly and fully considered; and
- GCHQ minimises the interference with the right to privacy caused by use of bulk personal data for operational purposes."

164) Authorisations are granted or refused by designated senior GCHQ officials (§3.6):

"Within GCHQ, authorisations are granted (or refused) by senior GCHQ officials who are members of the Senior Civil Service. In the case of continued retention, authorisation is granted (or refused) by a Retention Review Panel, of which senior GCHQ officials are members."

165) Deletion of a BPD does not require authorisation, but *"should in principle occur as soon as retention can no longer be justified as necessary and proportionate."* (§3.7). Furthermore:

"It must certainly occur if the Retention Review Panel refuses authorisation to retain it or in the event of an intervention to that purpose by the Intelligence Services Commissioner or the Interception of Communications Commissioner."

166) §3.10 notes that *"Details of each dataset and the decisions and actions taken in relation to it are recorded on a single form, which is stored centrally and serves as a record of the dataset's entire lifecycle within GCHQ."*

GCHQ: Authorisation

167) The purposes for which GCHQ acquires BPD, and the methods by which it does so, are addressed at §§4.1-4.2. However, irrespective of the means of acquisition, §4.3 notes that:

"GCHQ gives careful consideration in advance to the value that the dataset is expected to provide to one or more of GCHQ's missions, and to whether it is genuinely necessary and proportionate for GCHQ to use bulk personal data in pursuit of that (those) mission(s)."

168) The types of BPD which GCHQ acquires fall broadly into the following categories (§4.7): biographical (e.g. passport details), travel, financial (e.g. finance related activity of individuals), communications and commercial.

169) Receipt of data is recorded. [REDACTED]

170) GCHQ's Compliance Guide also notes (under "Collection & data acquisition") that:

[REDACTED]

"*GCHQ treats all such data according to RIPA safeguards. This both demonstrates HRA compliance and enables systems to handle data consistently. You must ensure that there*

is appropriate authorisation in place to acquire data from these sources, in order to comply with the law or (in cases where no legal authorisation is needed) to demonstrate that its acquisition is necessary and proportionate. Further information is in 'Authorisations'."

GCHQ: Authorisation

171) Sections 5 and 6 of the GCHQ Closed BPD Handling Arrangements address authorisation.

172) §5.1 states that:

"If it is believed that a sufficiently robust case can be made, in terms of necessity and proportionality, authorisation to acquire (or create) the dataset must be sought."

173) Authorisation is sought by representatives of the relevant operational team completing a "Bulk Personal Dataset record of authorisation" form ("BPD form") (§5.2) (a copy of this form is exhibited to this Closed Response at Exhibit "**Q**"[5]). The staff in question must identify themselves as "Requester" and "Endorser". [REDACTED]

174) Specified details of the dataset must be entered on the BPD form (§5.5). These will enable the Authoriser, inter alia, to assess the intrusiveness of the dataset (§5.6). If examination of the data reveals significant new information that appears likely to change the Authoriser's assessments of, *inter alia*, intrusiveness (e.g. sensitive personal data is to be found) the new information must be recorded on the BPD form. If the acquisition has already been authorised, the form must be returned to the Authoriser for further consideration (§5.8).

175) The Requester/Endorser must also make a case to justify the acquisition and use of the dataset. This includes a statement of the necessity and proportionality of such use (§5.9). The Requester and Endorser must also describe *"credible plans for operational exploitation of the dataset."* (§5.10). The purpose of this is:

"to avoid possession of bulk personal data by GCHQ, and the associated interference with the right to privacy, to no operational benefit."

176) If no credible, short-term plans are in place, authorisation to acquire the dataset will be refused (§5.11).

177) Before the acquisition request is forwarded to the Authoriser for consideration, it must be endorsed by a GCHQ Legal Adviser to confirm that all legal criteria for the dataset's acquisition or creation have been satisfied (§6.1).

178) Within GCHQ, authorisations are granted or refused by senior GCHQ officials who are members of the Senior Civil Service (§6.2). The Authoriser must consider the following factors (§6.3):

---

[5] A new version of this form is currently being drafted.

"

- *the intrusiveness of the dataset: the number of people whose information it contains, the proportion of those people who are of no probable intelligence interest and the sensitivity of the information involved;*
- *the level of corporate risk incurred by GCHQ's possession and use of the dataset;*
- *whether the Requester and Endorser have demonstrated the necessity of using the dataset in support of an operational purpose;*
- *whether it is proportionate to use a bulk personal dataset of this intrusiveness and sensitivity for this purpose; and*
- *whether only as much information will be obtained as is necessary to achieve the objective(s)."*

179) The Authoriser's decision and assessments must be recorded on the form (§6.4).

180) The initial period of authorisation will normally be for 6 or 12 months (§6.5):

> *"depending on the balance between the dataset's anticipated value and its assessed levels of intrusiveness and corporate risk. A shorter (never longer) period might be authorised, in the case of a particularly intrusive or sensitive dataset."*

181) The Authorisation may, at his/her discretion, approve acquisition only for a brief period, for the purpose, inter alia, of determining its precise contents *"and hence achieving a better understanding of its intrusiveness, sensitivity and potential value."* (§6.6)

182) If the acquisition request does not make a convincing case for the acquisition and use of the BPD, the Authoriser will either reject the request or, at his/her discretion, may approve it for a short period during which its value must be clearly demonstrated (§6.7). If the request is rejected, the BPD must not be acquired or created, or must be deleted or returned to the provider, along with any copies that have been made (§6.8). [REDACTED]

183) Operational exploitation of the dataset before authorisation is not permitted (§6.9).

GCHQ: Use

[REDACTED]

184) Access to BPD on operational systems is controlled in a number of ways.

185) First, it is controlled by GCHQ's standard account management procedures. These ensure that systems access is *"granted only to those with a genuine operational requirement to access the data."* [REDACTED]

186) GCHQ's policy is to grant operational system accounts only to individuals who have completed appropriate Legal and Policy training, including by passing the associated tests (§7.6).

187) Second, such individuals must also sign up to appropriate operating procedures. These make clear that access to operational systems is granted, and must be used, *"only for legitimate, work-related purposes."* Furthermore, individuals' access to and use of GCHQ IT systems is recorded, and records are *"centrally logged and regularly monitored for evidence of abuse."* (§7.7) Importantly, in the case of systems containing operational data, such as BPD, specific details of individuals' *activities* while accessing the system (including who was accessing the system, when, and what they did) are logged and subject to audit (§7.8).

188) Third, users are required to provide a "Necessity & Proportionality Statement" ("N&P Statement") for conducting an analytical search of the data in the system (§7.8):

> *"[A]n N&P statement consists of a statement of the operational purpose of the search and an explanation of its necessity and proportionality. These justifications are also logged and are subject to periodic audits of their legitimacy and adequacy."*

189) GCHQ's Legal and Policy training addresses N&P statements. Full guidance on how to formulate legitimate and adequate justifications is also available to all staff via links from GCHQ's Compliance Guide.

GCHQ: Experimental use

190) The use of BPD for *"an experimental purpose"*, for example, the development of a novel analytical technique or testing a new IT system, is specifically addressed at §8.1. The potential for increased risk to, inter alia, the security of the data and risk of additional interference with the right to privacy are acknowledged and addressed. Any such use of BPD must be specifically authorised in advance by a senior GCHQ official (§8.2).

191) The Authoriser must consider the necessity and proportionality of the proposed use, in particular:

> *"whether it is genuinely necessary to use bulk personal data for this purpose, given its intrusiveness and the degree of corporate risk involved."* (§8.3)

192) The person authorising the requested experimental use may set conditions or restrictions on its use, and such conditions/restrictions must be recorded on the BPD form for that dataset. If the request for experimental use is rejected, the dataset must not be used for that purpose (§8.4).

GCHQ: Disclosure

193) Section 9 addresses disclosure of (i) the results of analysing BPD and (ii) disclosure of a BPD itself or a substantial part of it.

194) Disclosure of the results of analysing BPD to partner or customer organisations must be done via standard intelligence reporting mechanisms. This ensures that GCHQ intelligence is released *"in a secure, accountable, legally compliant manner"* (§9.1)

195) In the case of disclosure of a BPD, or substantial part of it, different processes apply depending on whether the disclosure is (i) to another of the Agencies or (ii) to any other partner.

196) If the proposed recipient is another of the Agencies, that Agency must formally request transfer of the data via the "Inter-Agency Sharing" ("IAS") process. Such a request will be considered and either authorised or rejected, by a GCHQ senior official, and his decision and reasons recorded on the dataset's BPD form, as well as on the IAS request form (§9.3.1).

[REDACTED]

197) In the case of disclosure to any other partner the procedure and substantive considerations are set out at §§9.5-9.6, and emphasise the need for a *"persuasive justification"* in terms, inter alia, of **necessity** and **proportionality**, and for the Authoriser (a GCHQ senior official) to consider particularly, amongst other things: the personal/intrusive/sensitive nature of any information to be disclosed; whether partial, rather than full disclosure, would meet the need; the possibility of deleting data relating to UK [REDACTED] nationals before disclosure [REDACTED]; and the nature of the receiving organisation's arrangements for safeguarding, using and deleting the data (and to seek additional reassurances if considered necessary):

"9.5 All requests for authorisation to disclose must provide a persuasive justification for the proposed disclosure, in terms of:

- *its necessity and proportionality, and*
- *the intelligence- or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.*

9.6 The Authoriser will consider:

- *the content of the dataset: the nature of any personal information it contains, its intrusiveness and sensitivity;*
- *the nature and extent of the corporate risk the disclosure would entail;*
- *the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;*
- *whether any caveats or restrictions should be applied; and*
- *the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary."*

198) Furthermore, the general rules, as set out in the Compliance Guide, the Intelligence Sharing and Release Policy, the Reporter's Handbook and Reporting Standards, which apply to the handling of operational material. [REDACTED] These general rules include, *inter alia*, a requirement for mandatory training on operational legalities and detailed rules on the

disclosure of such material outside GCHQ and the need to ensure that all reports are disseminated only to those who need to see them. By way of a summary only, these rules include requirements that:

a) Operational data is not to be disclosed outside GCHQ to any organisation [REDACTED] unless that organisation will accord the data a level of protection that is equivalent to GCHQ's own safeguards;

b) Operational data cannot be disclosed outside of GCHQ other than in the form of an intelligence report, save where there is specific policy approval or in circumstances where an analyst may "tip off" a customer about the content of a forthcoming intelligence report. All intelligence reports must identify the intelligence requirements with which they are concerned. Their contents must be necessary and proportionate (in the sense of avoiding gratuitous material). They must only be disseminated to those who need to see them;

c) Insofar as operational data comprises or contains confidential information (e.g. journalistic material) then any analysis or reporting of such data must comply with the *"Communications Containing Confidential Information"* section of the Compliance Guide. This requires GCHQ to have greater regard to privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved (e.g. legally privileged material, confidential personal information, confidential journalistic information, communications with UK legislators). GCHQ must accordingly demonstrate to a higher level than normal that retention and dissemination of such information is necessary and proportionate.

GCHQ: Continued Retention

199) Ongoing retention of every BPD is reviewed at least annually by GCHQ's Bulk Personal Data Retention Review Panel ("BPDRR") (§§10.1-10.2). The BPDR consists of senior GCHQ officials including a senior lawyer. [REDACTED]

200) In addition, representatives from MI5 and SIS are normally invited to observe and contribute to discussions (§10.3).

201) The BPDRR meets every six months to consider the BPD due to review and to review the functioning of the BPD lifecycle management process. Discussions, decisions and actions are minuted (§10.4).

202) If a dataset's Requester and Endorser consider that a convincing case can be made to justify the continued retention and exploitation of that dataset, they must submit a retention request to the BPDRR by means of the dataset's BPD form. If they do not believe a convincing case can be made, they must arrange for the deletion of the dataset as soon as they reach this conclusion (§10.5). In the request, they must:

"justify the interference with the right to privacy caused by GCHQ's continued retention and exploitation of the dataset. They must set out why it is genuinely necessary and proportionate to continue to hold and use the data. This rationale must be supported by concrete evidence, including specific examples, where possible, of the operational value provided by the dataset during the previously authorised period. They should explain why they expect the dataset to continue to provide similar value in future." (§10.6)

203) The value of a dataset to other GCHQ business units must be taken into account by the Requester and Endorser (§10.7). In the case of datasets containing older material:

"a specific justification must be provided to explain why the old material remains of value and should not be deleted as it ages past a certain (previously specified and context-dependent) threshold." (§10.8)

204) The BPDRR must consider (§10.9):

"

- *whether a persuasive case has been made;*
- *whether it continues to be necessary and proportionate to retain the data;*
- *whether the degree of intrusiveness and corporate risk associated with continuing to hold and use the data remains as previously assessed;*
- *whether it is now possible to obtain the data of interest (the whole dataset or a subset thereof) through less intrusive means;*
- *whether any caveats or restrictions should be applied; and*
- *whether the retention request should be approved."*

205) If the BPDRR approves the request, it will authorise continued retention for a specific period, usually for 12 months. Where some doubt remains as to the value of a dataset, or where it is particularly sensitive, the BPDRR may authorise a shorter retention period, typically six months, occasionally less. A 24-month retention period may be authorised if the dataset is deemed to be of low intrusiveness and to represent low corporate risk (§10.10).

206) If the BPDRR rejects the request, or a convincing retention request cannot be submitted, the dataset and any copies must be deleted from GCHQ systems as soon as practicable. Any removable media must be dealt with in accordance with GCHQ's security policy on removable media. Deletion must be confirmed to the relevant GCHQ policy team by the Endorser and the details recorded on the BPD form (§10.11).

GCHQ: Deletion

207) Section 11 of the GCHQ Closed BPD Handling Arrangements deals with deletion. In particular:

a) Where a bulk personal dataset is no longer of use, or a persuasive case for its continued retention and use cannot be made, the data must be deleted (§11.1). Guidance on where a persuasive case for continued retention may be difficult is given at §11.2.

b) In such circumstances, the data must be deleted immediately by its Requester and Endorser, rather than wait for the next BPDRR meeting (§11.3).

c) Where old data is no longer essential, a "rolling deletion window" may be appropriate (§11.4).

d) Where retention can no longer be justified, the dataset's Endorser is responsible for ensuring that (§11.5):

i) The data (including any copies) is deleted;

ii) Confirmation is sent to the relevant GCHQ policy team.

iii) Details of deletion are recorded on the dataset's BPD form.

e) §11.6 addresses the situation where GCHQ has disclosed a dataset to another organisation, but can no longer itself justify keeping it. In such case:

"the Endorser must agree future responsibilities with the other organisation, with respect to ownership, further acquisition (if any), safeguarding and ultimate deletion of the dataset."

GCHQ: Oversight

208) The GCHQ Closed BPD Handling Arrangements also explain the oversight, both internal (including staff training and awareness of responsibilities) and external, which exists over BPD.

Internal oversight

209) §12.1.1 notes that unauthorised entry to computer records may constitute *"gross misconduct"* under GCHQ's employees' conditions of employment, and that this may be *"subject to disciplinary measures potentially including dismissal."* Furthermore, Security Operating Procedures ("SyOPs") make users of GCHQ IT systems aware *"of their responsibilities regarding proper use of corporate IT systems."* (§12.1.1)

210) §12.1.2 sets out the requirement for completion of legalities training *"which reiterates that GCHQ IT systems are to be used only for legitimate, necessary, work-related purposes and that access and use are subject to monitoring. It also contains a brief section specifically devoted to Bulk Personal Data."* In addition:

"anyone requiring access to systems containing "operational data" (which includes bulk personal data) must successfully complete Advanced Legal & Policy training before

accounts will be granted. This Advanced training contains detailed sections on necessity and proportionality and on N&P statements (including audit – see below)." (§12.1.3)

211) The importance of GCHQ's internal audit processes, which includes auditing whether access to bulk personal data has been properly justified on necessity and proportionality grounds, are referred to at §§12.1.4-12.1.7:

> *"12.1.4 Activity on IT systems holding bulk personal datasets is subject to audit, both from a security perspective (to ensure that there is no inappropriate access) and to verify that legitimate access is used only for properly authorised, necessary and proportionate purposes.*
>
> *12.1.5 The latter is termed "N&P audit" and looks specifically at the reasons and justifications for running queries and searches in data held on the systems in question. Before submitting a query, the analyst is required to enter into the system a clear explanation of:*
> - *the operational requirement in connection with which the query is made;*
> - *how the query relates to the requirement;*
> - *why it is necessary to run that particular query; and*
> - *how the interference with the right to privacy the query will cause is proportionate to the outcome it is expected to achieve.*
>
> *12.1.6 These justifications are centrally logged and are subject to N&P audit.*
>
> *12.1.7 A relevant senior official, who is a member of the BPD Retention Review Panel, will keep GCHQ's Executive Committee, of which that official is also a member, apprised of any pertinent issues relating to Bulk Personal Data."*

212) GCHQ's audit regime is described in the Compliance Guide (under "Audit"). In particular:

> a) *"**The audit scheme***
>
> *Auditing is applied to Operations in order to assess and demonstrate the degree of compliance with policy standards. These standards are designed to embody the legal requirement to demonstrate necessity and proportionality and to show that GCHQ is acting in accordance with its authorisations and meeting its human rights obligations."*
>
> [REDACTED]

External oversight

213) The external oversight provided by the Intelligence Services Commissioner over *"the use by the intelligence Agencies of non-targeted bulk personal data (except where that data has been obtained via interception..."* is referred to in GCHQ's Compliance Guide (under

"Oversight") and addressed in more detail at Section 12 of the GCHQ Closed BPD Handling Arrangements:

"12.2.1 The majority of the bulk personal datasets held by GCHQ are acquired by means other than interception under RIPA warrant; they therefore fall within the oversight purview of the Intelligence Services Commissioner (ISComm). The remaining few datasets, formed from intercepted material (see the section on Acquisition above), are overseen by the Interception of Communications Commissioner (IOCC).

12.2.2 The Commissioners each visit GCHQ at least twice a year for formal inspections and will typically inspect a sample of bulk personal datasets of their choice on each occasion. They will examine records (including the BPD forms) and interview officers responsible for the acquisition and management of the datasets; they may also request information on how data is handled and used. GCHQ must be able to demonstrate to the Commissioners that proper judgments have been made on the necessity and proportionality of acquiring, using, disclosing and retaining bulk personal datasets.

12.2.3 The ISComm also reviews the adequacy and effectiveness of GCHQ's policies and procedures for managing bulk personal datasets, and oversees controls to prevent and detect misuse of bulk personal data. Any reports on investigations arising out of auditing activity (see paragraph 12.1.4 above) will be drawn to the attention of the ISComm. The IOCC reviews the adequacy and effectiveness of GCHQ's arrangements to minimise retention and dissemination of intercepted material ("RIPA Safeguards").

12.2.4 The Commissioners provide independent oversight of GCHQ's arrangements and report their findings to the Prime Minister: the ISComm annually, the IOCC biannually."

214) §12.2.5 notes that *"From time to time, GCHQ may additionally report significant issues relating to BPD to the Foreign Secretary."*

215) In addition, GCHQ's Compliance Guide states (under "Errors"):

a) "*GCHQ policy is to abide by all UK laws that relate to GCHQ's operations, but errors with respect to legal compliance, and to apply the safeguards do sometimes occur*. This section outlines GCHQ's process for handling errors and your role.

We need to be able to recognise and detect errors of legal compliance. We are obliged to investigate them and report to our oversight authorities."

b) *"**Reporting potential errors***
You should not hesitate to report to the relevant GCHQ policy team any activity that appears to be erroneous or unauthorised. This includes any activity that does not appear to comply with GCHQ's systems and processes and may therefore have resulted in unauthorised, unjustified or disproportionate interference with privacy rights or property. You may wish to consult your line management or your local Legal and Policy Lead, but do not allow this to cause unnecessary delay."

c) *"**Handling of errors***

...

If an error does occur, the relevant GCHQ policy team will:

- *advise whether it is necessary to stop a task, destroy material or cancel reporting*
- *coordinate any reporting to oversight authorities – i.e. the relevant Commissioner*
- *help develop recommendations for preventing a recurrence, e.g. changes to procedures, processes or training, and ensure they are implemented..."*

GCHQ: Past policy

216) GCHQ's acquisition, use, retention and disclosure of BPD has been subject to the policies set out above from its Compliance Guide, Intelligence Sharing and Release Policy, Reporting Standards and Reporter's Handbook throughout the relevant period (June 2014 and onwards) and, indeed, from before then. Amongst other things, this meant that all BPD was handled in accordance with RIPA safeguards and was subject to GCHQ's operational data retention policies, including default retention limits. It was also subject to external oversight throughout that period: as noted at §119 of the Open Response, and above in relation to MI5 and SIS, prior to the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015, which came into force on 13 March 2015, BPD was already (including during the period June 2014 onwards) subject to the non-statutory oversight of the Intelligence Services Commissioner.

217) GCHQ's past policies in relation to BPD were accordingly similar to those now in force.

C. SUBMISSIONS IN RELATION TO THE BPD REGIME

Issue: Does the BPD Regime contain adequate safeguards to provide proper protection against arbitrary conduct?

218) The Open Response sets out at §§158-179 the Respondents' submissions on the law in relation to the requirement that any interference be "in accordance with law". Those submissions are not repeated in this CLOSED response.

219) It is the Respondents' position that the "below the waterline" safeguards, which can be taken into account by the Tribunal are such that the regime contains adequate safeguards to provide proper protection against arbitrary conduct. In particular there are detailed internal arrangements which provide comprehensive safeguards in terms of the authorisation for BPD activities and the use, storage of, access to, retention, and disclosure of any material obtained as a result of such activities. Those important safeguards include, *inter alia*:

a) Detailed internal guidance on the requirements of necessity and proportionality (having regard to the privacy of those whose data is contained in the BPD) including the need to consider other, less intrusive, methods of obtaining the information);
b) Specific consideration of sensitive data and confidential data;

c) A clear policy on the storage of and access to BPD;
d) Specific retention periods and retention/deletion policies which apply to BPD;
e) Policies on the handling and disclosure of BPD;
f) Clear guidance on the serious consequences of failure to comply with the Handling Arrangements, which include disciplinary action, including potentially dismissal, and prosecution;
g) Training; and
h) Oversight, both internal and external.

D. "BELOW THE WATERLINE" SAFEGUARDS FOR SECTION 94 OF THE TELECOMMUNICATIONS ACT 1984

220) The Open Response set out the relevant statutory regimes (insofar as possible in Open[6]) and the material provisions of the Open Handling Arrangements in relation to Section 94 of the 1984 Act (§§28-57 and 90-111). However, in addition to the statutory regime and Open Handling Arrangements, the Respondents have substantial "below the waterline" safeguards which apply to section 94 of the 1984 Act.

221) This Section of the Closed Response considers the "below the waterline" safeguards of (i) MI5 and (ii) GCHQ respectively.

MI5

222) MI5 also has internal arrangements for the acquisition of Bulk Communications Data pursuant to directions under section 94 of the Telecommunications Act 1984, and access thereto pursuant to authorisations under section 22 of the Regulation of Investigatory Powers Act 2000 and its subsequent use and disclosure of such data ("the MI5 Closed Section 94 Handling Arrangements"). These are made pursuant to section 2(2)(a) of the Security Service Act 1989 (see §1.1) and came into force on 4 November 2015. The MI5 Closed Section 94 Handling Arrangements are exhibited to this Closed Response at Exhibit "**S**".

223) As noted at §1.4, since 2005 successive Home Secretaries have issued and/or decided to maintain directions under section 94 of the Telecommunications Act 1984 ("the Section 94 Directions") requiring Communications Network Providers ("CNPs") to provide MI5 with bulk communications data in the interests of national security. [REDACTED]

224) The rules set out in the MI5 Closed Section 94 Handling Arrangements are mandatory. Failure to comply with them may lead to disciplinary action, which can include dismissal and prosecution (§1.3).

225) The purpose and importance of the arrangement is also stressed at §§4.0.1-4.0.2:

---

[6] However, MI5's use of section 22 of RIPA to authorise access to/use of BCD is not avowed, and so was not referred to in the Open Response.

"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.*** *"*

The information to which the MI5 Closed Section 94 Handling Arrangements relate is defined in section 2. §2.1 notes that the communications data provided by the CNPs under the Section 94 Directions is limited to "traffic data" and "Service Use Information" (as defined in §3.11, citing section 21(4)(a) and (b) of RIPA) [REDACTED].

226) The data provided does not contain communication content or Subscriber Information (as defined at §3.11).

227) An overview of the stages of **transfer** and **retrieval** of section 94 data is set out. At the **transfer** stage

"the CNPs each transfer their data" (§2.3)

228) The section 94 directions under which this transfer takes place:

"require the Home Secretary to be satisfied that it is necessary in the interests of national security and that the level of interference with privacy involved in the transfer and secure storage of the data is proportionate to what it seeks to achieve." (§2.4)

229) The second stage involves the **retrieval** of specified data from the database by MI5 officers [REDACTED].

230) Importantly, §2.7 notes that individual authorisations for requests are obtained under s.22 of RIPA, and that data is only retrieved from the database, and viewed and retained by MI5, if judged **necessary** and **proportionate** (as required by s.22(1) and (5) of RIPA).

[REDACTED]

231) Section 3 of the MI5 Closed Section 94 Handling Arrangements explains the relevant legal basis, including a summary of MI5's functions under the SSA, the duty on the Director-General of MI5 to ensure arrangements are in place under s.2(2)(a) and the statutory limits on the information that MI5 can obtain and disclose.

232) Further summaries of relevant provisions, including s.19 of the Counter-Terrorism Act 2008, the Human Rights Act 1998, the Data Protection Act 1998, s.94 of the Telecommunications Act 1984, Part 1 Chapter II of RIPA (including definitions of "communications data" and the test for authorisation of obtaining communications data in s.22 of RIPA), and Article 8(2) of the ECHR, are set out at §§3.5-3.18.

233) The MI5 Closed Section 94 Handling Arrangements set out the arrangements in relation to:

a) Authorisation of Acquisition – Stage 1;
b) Acquisition;
c) Authorisation of Use/Access – Stage 2;
d) Authorisation of Disclosure; and
e) Review of Ongoing Acquisition and Retention and Deletion;
f) Oversight.

MI5: Authorisation of Acquisition – Stage 1

234) Section 4.1 of the MI5 Closed Section 94 Handling Arrangements sets out the process and safeguards in relation to acquisition of BCD. The involvement of senior MI5 officials, extensive preparatory work by MI5 on questions of necessity and proportionality, consultation with the CNP, and ultimately the consideration by the Secretary of State that the tests of necessity and proportionality are satisfied are emphasised:

> *"**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 Secretary of State 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 relevant ethical issues.

4.1.3 The 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 section 94(4) of the Act."

235) If the Home Secretary issues a direction, it must be served on the CNP by the Home Office, so enabling MI5 to receive the requested dataset (§4.2.1). [REDACTED]

MI5: Authorisation of Use/Access – Stage 2

236) Section 4.3 of the MI5 Closed Section 94 Handling Arrangements concerns authorisation of use or access to data from the database.

237) Each request for specific data from the database must be authorised pursuant to s.22 of RIPA. Any such authorisation must meet the tests of **necessity** and **proportionality** and is also subject to the oversight of the Interception of Communications Commissioner. Such authorisations are appropriately recorded and stored.

238) The seniority of officer who may act as a Designated Person for the purpose of the RIPA authorisation process is addressed at §§3.14-3.18:

"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 data 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 or analysis of up to 365 days' of BCD product (if necessary and proportionate to do so)."*

[REDACTED]

239) Applicants are required to include **necessity** and **proportionality** considerations which are detailed in §4.3.4:

*"**(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."

240) All applications must also state whether the applicant believes that the data returned will relate to a sensitive profession. [REDACTED] If an application is related to a sensitive profession the applicant must send the application to an independent Designated Person, i.e. an officer who is not in the applicant's management chain, for consideration (§4.3.8).

241) Once a request has been submitted, it is automatically directed [REDACTED] to a Designated Person for consideration. The Designated Person must consider, inter alia, the

necessity and proportionality justification, the intrusion into privacy which will result, and any measures identified for the mitigation of collateral intrusion, and whether the time period of data requested is proportionate (§4.3.5). Designated Persons are required to reject any application for communications data where they are not convinced of both the necessity and proportionality of the request, and must give reasons for doing so (§4.3.6).

242) If a request is approved by the Designated Person, the requested data will be sent to the applicant.

[REDACTED]

243) §4.3.19 and §4.3.20 set out detailed additional safeguards governing access to BCD. These additional safeguards address, inter alia, the obtaining of communications data relating to an individual known to be a member of a *"sensitive profession"* – i.e. a profession *"that handles privileged information or information that is otherwise confidential* (medical doctors, lawyers, journalists, Members of Parliament, Ministers of religion)". In such cases, staff are required to *"give* ***special consideration*** *to the necessity and proportionality justification for the interference with privacy that will be involved"* and must (as above) send the application to an independent Designated Person for consideration (§4.3.20, §4.3.8).

MI5: Authorisation of Disclosure

244) Disclosure of BCD is addressed in Section 4.4 of the MI5 Closed Section 94 Handling Arrangements. §4.4.1 notes that disclosure must be *"carefully managed"* to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway.

245) Disclosure of an entire bulk communications dataset, or a subset, outside MI5 *"may only be authorised by the Home Secretary or a Senior Official in the Home Office"* (§4.4.1).

246) Disclosure of individual items of bulk communications data outside MI5 can only be made if the following conditions are met:

> *"- The objective of the disclosure falls within MI5's statutory functions or is for the additional limited purposes set out in 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."*

247) Explanations of the **necessity** and **proportionality** considerations are given at §§4.3.4-4.4.4. In addition before disclosing any BCD staff must take reasonable steps to ensure 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" (§4.4.5)

248) These conditions must be met for all disclosure, including between other Intelligence Services, and in relation to entire datasets, sub-sets and individual pieces of data from datasets (§4.4.6).

249) Where these conditions are met, in the case of disclosure of an entire bulk communications dataset, or subset thereof, to another Intelligence Service, the BCD must be formally requested from MI5 through an agreed sharing procedure using an Inter-Agency Disclosure Form. The relevant data sponsor within MI5 must then submit a Form for Sharing that will seek approval within MI5 – see Exhibit "**F**". [REDACTED]

250) If MI5's Director General is content, a submission will be prepared for the Home Office and/or Home Secretary (§4.4.8). Disclosure of the whole (or a subset) of a bulk communications dataset is only permitted once this has been authorised by the Home Secretary or a Senior Official at the Home Office (§4.4.8).

MI5: Review of Ongoing Acquisition and Retention and Deletion

251) Section 4.5 of the MI5 Closed Section 94 Handling Arrangements addresses review of ongoing acquisition and retention and deletion of Bulk Communications Data.

252) MI5's data governance team must conduct a review every six months on behalf of the "BCD Governance Group" ("BCDGG") that includes, 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 ongoing acquisition, 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; and

- The adequacy of security arrangements." (§4.5.1)

253) 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 six months to consider the Data Governance Team's report (§4.5.2).

254) The BCDGG consists of senior MI5 officials, including the Ethics Counsellor and the Legal Adviser.

255) 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. 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 (§§4.5.4-5).

256) Data is retained for 365 days after which it must be deleted (§4.5.6). Data that has been retrieved from BCD following the procedures on use and access set out in section 4.3 will be retained in accordance with MI5's Information Management policy.

257) If MI5 or the Secretary of State no longer deem it necessary and proportionate to acquire and retain the BCD, the Secretary of State will cancel the relevant section 94 direction and will instruct the relevant CNP(s) to cease supply (§4.5.8).

258) Where a decision is taken to delete data, MI5 must task the technical teams responsible for Retention and Deletion with a view to ensuring that any retained data is destroyed. Confirmation of completed deletion must be recorded with the data governance team (§4.5.8).

MI5: Oversight

259) Section 4.6 of the MI5 Closed Section 94 Handling Arrangements address internal and external oversight of BCD.

260) Internal oversight comprises (i) the BCDGG Chair, who is a member of MI5's Executive Board, keeping the Board apprised of BCD holdings (§4.6.1); and (ii) audit of use of IT systems. Audit is addressed at §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."

261) All reports on audit investigations are made available to the Interception of Communications Commissioner (§4.6.3).

262) The external oversight provided by the Interception of Communications Commissioner is specifically addressed at §§4.6.4-4.6.9:

*"**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 judgments 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) 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 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

[REDACTED]*"*

263) In addition, §4.6.10 notes that the Parliamentary Intelligence & Security Committee may also be briefed on BCD holdings as required.

MI5: Past practice and policy

264) Neither MI5's process or policy in relation to Section 94 of the 1984 Act have changed materially in the relevant period. The regime for acquisition, use, disclosure, review, retention of BCD has as a matter of practice been similar to that set out above for the period June 2014 onwards. In addition, throughout that period (and earlier) MI5's use of BCD has been subject to the oversight of the Interception of Communications Commissioner on a non-statutory basis.

GCHQ

265) GCHQ also has internal arrangements for the acquisition and use and disclosure of Bulk Communications Data pursuant to directions under section 94 of the Telecommunications Act 1984 ("the GCHQ Closed Section 94 Handling Arrangements"). These are made under section 4(2)(a) of the Intelligence Services Act 1994 and came into force on 4 November 2015. The GCHQ Closed Section 94 Handling Arrangements are exhibited to this Closed Response at Exhibit "**T**". Relevant policy and guidance is also set out in GCHQ's Compliance Guide, Intelligence Sharing and Release Policy, Reporting Standards and Reporter's Handbook.

266) The introduction to the GCHQ Closed Section 94 Handling Arrangements states (at §1.2) that:

> *"In brief, section 94 data is to be handled in the same way as related communications data obtained pursuant to warrants issued by the Secretary of State under section 5 of the Regulation of Investigatory Powers Act 2000 ("RIPA")."*

267) §1.3 emphasises the mandatory nature of the Handling Arrangements for GCHQ staff and the serious consequences of non-compliance:

> *"Failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal, and potentially to criminal prosecution."*

268) The purpose and importance of the arrangements is also stressed at §§4.0.1-4.0.2:

> *"4.0.1 The acquisition, use, retention and disclosure of section 94 data 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 GCHQ with respect to the acquisition of section 94 data, access to and use of the data, retention of the data, and disclosure of the data to persons outside GCHQ where this is necessary for the proper discharge of GCHQ's statutory functions. Staff must ensure that no section 94 data is accessed, used, retained or disclosed except in accordance with section 4(2)(a) of ISA, section 94 of the Telecommunications Act 1984 and these Arrangements."*

269) The nature of GCHQ's Section 94 activities, which relate to communications data with a non-UK focus, is set out at §1.4:

> *"Since 2001 successive Foreign Secretaries have given directions, under section 94 of the Telecommunications Act 1984 ("the section 94 directions"), requiring a number of providers of public electronic communications networks ("CNPs") to provide GCHQ with various sets of bulk communications data in the interests of national security. All the sets of communications data currently being provided have a foreign focus insofar as one or both ends of each communication will be located overseas and/or one or both communications devices will be foreign-registered."*

270) The existence of a review process is emphasised (§1.4):

> *"GCHQ provides a review of the use of this communications data, and of the continuing need to acquire it (where this can be justified), to the Foreign Secretary at six-monthly intervals."*

Information covered

271) §§2.1 to 2.8 explain the information which the GCHQ Closed Section 94 Handling Arrangements cover:

> *"The communications data provided by the CNPs under the section 94 directions is limited to various forms of "traffic data" (as defined in section 21(6) RIPA and "service use information" (as defined in section 21(4) RIPA)."* (§2.1)

272) The data provided explicitly does not contain communications content or *"subscriber information"* (as defined in section 21(4)(c) RIPA) (§2.2).

Overview of acquisition and use of section 94 data

273) An overview of the stages of **acquisition** and **use** of section 94 data is set out. At the **acquisition** stage

> *"the CNPs each transfer their data to GCHQ for secure retention in operational systems accredited to hold bulk communications data."* (§2.3)

274) The section 94 directions under which this transfer takes place:

> *"require the Foreign Secretary to be satisfied that the supply of data is necessary in the interests of national security and that the conduct required by the direction – including any interference with privacy – is proportionate to what it seeks to achieve."* (§2.4)

275) The **use** stage involves trained GCHQ analysts running queries against the operational systems containing the section 94 data. [REDACTED]

276) The ability to query and view such data is limited to cases where:

> *"the conduct involved is in accordance with GCHQ's statutory functions and purposes and is considered necessary and proportionate. Individual analysts are required to provide a statement of necessity and proportionality ("N&P statement") for any analytical search of a system containing section 94 data or related communications data."* (§2.7)

277) §2.7 adds that "N&P statements may be audited."

278) Section 3 of the GCHQ Closed Section 94 Handling Arrangements addresses the legal basis for section 94 activity, emphasising the requirements of **necessity** and **proportionality**, and of consultation of CNPs by the Secretary of State prior to giving directions (§3.2). The existence of such directions, and GCHQ's provision to the Foreign Secretary of a review of the same every six months since 2013 is also noted (§3.3). §3.4 notes that:

> *"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". The Foreign Secretary is of the view that disclosure of the section 94 directions given on the application of GCHQ would be against the interests of national security, and so these directions have not been published, nor has the fact of their existence with respect to particular CNPs."*

GCHQ: Authorisation of Acquisition – Stage 1

279) Section 4.1 of the GCHQ Closed Section 94 Handling Arrangements sets out the process and safeguards in relation to acquisition of section 94 data. The involvement of senior GCHQ officials, extensive preparatory work by GCHQ on questions of necessity and proportionality, consultation with the CSP, the endorsement of a GCHQ Legal Adviser that all legal criteria have been satisfied, and ultimately the consideration by the Secretary of State that the tests of necessity and proportionality are satisfied are emphasised:

> *"**4.1 Authorisation of Acquisition – Stage 1***
>
> *4.1.1 Where the relevant senior GCHQ official has agreed to request a section 94 direction from the Foreign Secretary, a submission will be drafted by the relevant team in order to enable the Secretary of State to consider:*
>
> *- whether 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 conduct required by the direction is proportionate to what is sought to be achieved by that conduct;*
>
> *- whether there is a less intrusive means of achieving the national security objective(s) of the direction;*

- any political and reputational risks in directing the CNP to provide the specific communications data.

4.1.2 This submission will be informed by extensive preparatory work by GCHQ in order to consider and articulate the necessity and proportionality of acquiring and using the communications data to be requested under the direction. GCHQ will also consult the CNP concerned on behalf of the Secretary of State and the submission will reflect the views of the CNP as part of the overall consideration.

4.1.3 The submission must be endorsed by a GCHQ Legal Adviser, to confirm that all legal criteria for requesting a section 94 direction have been satisfied.

4.1.4 The submission must also outline any national security argument as to why the Foreign Secretary cannot lay the direction before each House of Parliament in accordance with section 94(4) of the Act."

280) In addition, GCHQ's Compliance Guide requires all GCHQ operational activity, including BPD activity, to be carried out in accordance with three core principles. These are that all operational activity must be:

a) Authorised (generally through a warrant or equivalent legal authorisation;
b) Necessary for one of GCHQ's operational purposes; and
c) Proportionate.

(see Compliance Guide – Overview)

281) These principles apply to each stage in the lifecycle of section 94 data (as to all operational activity and data).

GCHQ: Acquisition

282) GCHQ's Compliance Guide states (under "Authorisations"):

*"**Direction under s.94 of the Telecommunications Act***
A Direction under s.94 of the Telecommunications Act may be issued by the Secretary of State and served upon a CSP. The Direction cannot direct the CSP to disclose communications content; it can, however, direct the CSP to disclose other information i.e. communications data in the interests of national security and where SoS judges it proportionate. GCHQ's relevant team makes of these Directions."

283) GCHQ's Compliance Guide also notes (under "Collection & data acquisition") that:

*"**6. Other data acquisition***

GCHQ receives operational data from various sources other than its own interception. The principal sources are:

- *communications data acquired under Telecommunications Act s94 directions and through partnerships (see communications data for further details.*

...

GCHQ treats all such data according to RIPA safeguards. This both demonstrates HRA compliance and enables systems to handle data consistently. You must ensure that there is appropriate authorisation in place to acquire data from these sources, in order to comply with the law or (in cases where no legal authorisation is needed) to demonstrate that its acquisition is necessary and proportionate. Further information is in 'Authorisations'."

284) If the Foreign Secretary issues a direction, it must be served on the CNP, so enabling GCHQ to receive the requested dataset (GCHQ Closed Section 94 Handling Arrangements, §4.2.1). [REDACTED]

GCHQ: Authorisation of Use/Access – Stage 2

285) Access to section 94 data on operational systems is controlled in a number of ways. 320 (first and third sentences)

286) First, it is controlled by GCHQ's standard account management procedures. [REDACTED] Within systems further limits are placed on access to particularly sensitive data *"through electronic access control measures such as "Communities of Interest" and "Access Control Groups."* (§4.3.1) [REDACTED]

287) Second, such individuals must also sign up to appropriate operating procedures. These make clear that access to operational systems is granted, and must be used, *"only for legitimate, work-related purposes."* Furthermore, individuals' access to and use of GCHQ IT systems is recorded, and records are *"centrally logged and regularly monitored for evidence of abuse."* (§4.3.3) Importantly, in the case of systems containing operational data, such as section 94 data, specific details of individuals' *activities* while accessing the system (including who was accessing the system, when, and what they did) are logged and subject to audit (§4.3.4).

288) Third, the GCHQ Closed Section 94 Handling Arrangements emphasise the requirement that *"Any analytical search or query with respect to an operational system containing section 94 data or related communications data"* must be **necessary** and **proportionate** (§4.3.5). §§4.3.5 to 4.3.9 explain the relevant process and what such considerations involve:

"4.3.5...Before conducting any such search or query, individual analysts must provide a justification in the form of an N&P statement. An N&P statement consists of a record of the operational purpose of the search or query and a free-text explanation of its necessity and proportionality.

4.3.6 In this context, "necessary" means "really needed" for the purpose of discharging one or more of GCHQ's statutory functions.

4.3.7 In deciding whether a search or query is necessary, analysts must consider:

- *The background and aims of the intelligence operation in question.*

- *Where the query relates to a known target, what is the significance of the target in the context of the intelligence operation?*

- *How does the communications address that is the subject of the query relate to the target and/or to the intelligence operation?*

- *How will the data to be retrieved assist in taking forward the intelligence operation?*

4.3.8 In this context, "proportionate" means that the level of interference with the individual's right to privacy is justified when measured against the anticipated intelligence benefit and the importance of the objective to be achieved.

4.3.9 In deciding whether a search or query is proportionate, analysts must consider:

- *What exactly is being sought in the data to be retrieved?*

- *What will be the intrusion into the privacy of the target of the query? Can this be justified by the intelligence benefits?*

- *Is there another, less intrusive way of obtaining the information required?*

- *If a time period of data has been specified, why is this particular time period required? Would a shorter time period be sufficient?*

4.3.10 Any collateral intrusion must considered as part of proportionality. In particular analysts must consider:

- *Will the data to be retrieved result in collateral intrusion into the privacy of persons unconnected with the aims of the intelligence operation? Can this be justified by the intelligence benefits?*

- *If a time period of data has been specified, how will this impact on the identified collateral intrusion?*

- *How will any identified collateral intrusion be managed? For example, if seeking to retrieve call records data for a landline used by individuals of no intelligence interest as well as the target, how will the data be analysed to identify usage by the target?*

289) Particular emphasis is placed on the need to give *"special consideration"* to any search or query which is likely to retrieve communications data relating to a member of a *"sensitive profession"*. Examples given are *"lawyers, journalists, medical professionals, ministers of religion or UK Members of Parliament)."* This consideration must be recorded in the N&P statement (§4.3.11). Further, wherever analysts include in an intelligence report information based on communications data relating to individuals known to be members of sensitive professions *"this must be recorded and brought to the attention of the Interception of Communications Commissioner at the next inspection."* (§4.3.12). Provision is made for exceptional cases involving journalists' sources at §4.3.13.

290) GCHQ's Legal and Policy training addresses N&P statements. Full guidance on how to formulate legitimate and adequate justifications is also available to all staff via links from GCHQ's Compliance Guide (§4.3.14).

291) All records of searches and queries, together with accompanying N&P statements, are centrally logged and subject to periodic audits of their legitimacy and adequacy. Furthermore, the Interception of Communications Commissioner may inspect records relating to section 94 data and related communications data (§4.3.15).

GCHQ: Authorisation of Disclosure

292) Section 4.4 addresses disclosure of (i) the results of analysing section 94 data and (ii) disclosure of a section 94 dataset itself or a substantial part of it.

293) Disclosure of the results of analysing section 94 data to partner or customer organisations must be done via standard intelligence reporting mechanisms. This ensures that GCHQ intelligence is released *"in a secure, accountable and legally compliance manner"* (§4.4.1).

294) In the case of disclosure of section 94 dataset, or substantial part of it, different processes apply depending on whether the disclosure is (i) to another of the Agencies or (ii) to another UK partner or foreign partner.

295) If the proposed recipient is another of the Intelligence Services, that Intelligence Service must formally request transfer of the data via the "Inter-Agency Sharing" ("IAS") process. Such a request will be considered, and either authorised or rejected, by a senior GCHQ official, and his decision and reasons recorded on the IAS form (§4.4.3).

[REDACTED]

296) In the case of disclosure to another UK partner or a GCHQ foreign partner, the procedure and substantive considerations are set out at §§4.4.5-4.4.7, and emphasise the need for a *"persuasive justification"* in terms, inter alia, of **necessity** and **proportionality**, and for the Authorises (a senior GCHQ official) to consider particularly, amongst other things: the personal/intrusive/sensitive nature of any information to be disclosed; whether partial, rather than full disclosure, would meet the need; the possibility of deleting data relating to UK [REDACTED] nationals before disclosure to a non-UK partner; and the nature of the

receiving organisation's arrangements for safeguarding, using and deleting the data (and to seek additional reassurances if considered necessary):

"4.4.5...the relevant team will submit a request for authorisation to disclose the dataset to a senior GCHQ official.

4.4.6 All requests for authorisation to disclose musts provide a persuasive justification for the proposed disclosure, in terms of:

- *its necessity and proportionality, and*
- *the intelligence benefit or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.*

4.4.7 The Authoriser will consider:

- *the content of the dataset: the nature of any personal information it contains, its intrusiveness and sensitivity;*
- *the nature and extent of the corporate risk the disclosure would entail;*
- *the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;*
- *whether the caveats or restrictions should be applied; and*
- *the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary.*

[REDACTED]

297) The general rules, as set out in the Compliance Guide, the Intelligence Sharing and Release Policy, the Reporter's Handbook and Reporting Standards, which apply to the handling of operational material have already been referred to above. They apply equally to section 94 data.

GCHQ: Data Retention, Review and Deletion

298) Section 5 of the GCHQ Closed Section 94 Handling Arrangements deals with data retention, review and deletion.

299) The starting-point is that, subject to the review process, section 94 data will be retained by GCHQ for a maximum of 12 months (in line with GCHQ's overall operational data retention policy with respect to bulk communications data) (§4.5.1)[7]

300) If, in exceptional circumstances, there is a case for retention of section 94 data beyond the default 12-month retention limit, the dataset becomes subject to GCHQ's handling arrangements for BPD. §4.5.2 notes specifically that *"authorisation to retain the dataset must be sought in accordance with [the BPD] Handling Arrangements."*

[7] Data may be deleted at any time before that threshold (e.g. for capacity reasons) (§4.5.1).

301) This is subject to a review process, whereby the relevant team reviews section 94 data and directions every six months in order to determine whether retention and use of each dataset remains **necessary** and **proportionate**. The results of the review are delivered to a senior GCHQ official, who, if satisfied the review has been properly conducted, will submit it, with any comments or recommendations, to the Head of the Intelligence Policy Department at the FCO for the attention of the Foreign Secretary. The review is also copied to the Interception for Communications Commissioner. The detailed process is set out at §§4.5.3-4.5.8:

> *"4.5.3 A Review Panel conducts a comprehensive review of GCHQ's section 94 data, and of the directions used to acquire the data, at six-monthly intervals. The review determines whether acquisition/retention and use of each dataset remains necessary and proportionate for GCHQ to discharge its statutory functions.*
>
> *4.5.4 The Panel consists of senior GCHQ officials, including a senior Legal Advisor.*
>
> *4.5.5 In conducting its review, the Panel will consider:*
>
> - *the value and use of each dataset during the period under review, including specific examples that may serve to illustrate the benefits;*
> - *the operational and legal justification for continued acquisition/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*
> - *whether such information could be acquired elsewhere through less intrusive means.*
>
> *4.5.6 If the Panel determines that it is no longer necessary or proportionate to retain a section 94 dataset, all copies of the data must be deleted and that must be noted in the record of the Panel. If such a determination in respect of one or more datasets means that it is no longer necessary to rely on the associated direction, that must also be noted.*
>
> *4.5.7 The relevant senior GCHQ official will submit a six-monthly report to the Head of Intelligence Policy Department, FCO for the attention of the Foreign Secretary, together with such comments and recommendations as he sees fit. Any deletion of a dataset should be noted. If it is no longer necessary to rely on a section 94 direction, relevant senior GCHQ official will recommend to the Foreign Secretary that it be allowed to lapse (there being no provision in the Act to cancel a direction). The report will be copied to the Interception of Communications Commissioner.*
>
> *4.5.8 The review process provides an opportunity for the Foreign Secretary to oversee the use of the directions, to seek further information or to raise concerns about any*

particular issues. If the Foreign Secretary agrees that a section 94 direction should be allowed to lapse, the relevant team will notify the relevant CNP accordingly.

4.5.9 Any deletion of a section 94 dataset will be tasked to the technical teams responsible for the relevant operational system(s). Confirmation of completed deletion must be notified to the relevant teams."

GCHQ: Oversight

302) The GCHQ Closed Section 94 Handling Arrangements also explain the oversight, both internal (including staff training and awareness of responsibilities) and external, which exists over section 94 activities.

303) §4.6.1 notes that unauthorised entry to computer records may constitute *"gross misconduct"* under GCHQ's employees' conditions of employment, and that this may be *"subject to disciplinary measures potentially including dismissal."* Furthermore, Security Operating Procedures ("SyOPs") make users of GCHQ IT systems aware *"of their responsibilities regarding proper use of corporate IT systems."* (§4.6.1)

304) §4.6.2 sets out the requirement for completion of legalities training *"which reiterates that GCHQ IT systems are to be used only for legitimate, necessary, work-related purposes and that access and use are subject to monitoring."* In addition:

"anyone requiring access to systems containing "operational data" (which includes section 94 data) must successfully complete Advanced Legal & Policy training before accounts will be granted. This Advanced training contains detailed sections on necessity and proportionality and on N&P statements (including audit – see below)." (§4.6.3)

305) The importance of GCHQ's internal audit processes, which includes auditing whether access to section 94 data has been properly justified on necessity and proportionality grounds, are referred to at §§4.6.4-4.6.7:

"4.6.4 Activity on operational systems holding section 94 data is subject to audit, both from a security perspective (to ensure that no inappropriate access or misuse of access is taking place) and to verify that legitimate access is being properly justified with respect to necessity and proportionality.

4.6.5 The latter is termed "N&P audit" and looks specifically at the reasons and justifications for running queries and searches in data held on the systems in question. Before submitting a query, the analyst is required to enter into the system a clear explanation of:

- *the operational purpose in connection with which the query is made;*
- *how the query relates to that purpose;*
- *why it is necessary to run that particular query; and*

- *how the interference with the right to privacy the query will cause is proportionate to the outcome it is expected to achieve.*

4.6.6 Queries and justifications are centrally logged and are subject to N&P audit.

4.6.7 All reports on security audit investigations are made available to the Interception of Communications Commissioner. Any incident where a member of staff has abused his/her access to communications data will be brought to the attention of the Commissioner.

4.6.8 The relevant senior GCHQ official will keep GCHQ's Executive Committee, of which she is a member, apprised of any pertinent issues relating to section 94 data."

306) GCHQ's audit regime is described in the Compliance Guide (under "Audit"), as set out above. GCHQ's policy on "Errors" as set out in the Compliance Guide is also set out above.

307) The external oversight provided by the Interception of Communications Commissioner is addressed at §§4.6.9-4.6.11:

"4.6.9 The Interception of Communications Commissioner is responsible for overseeing the necessity and proportionality of section 94 directions given by the Secretary of State, the access to and use of the data acquired pursuant to the directions, and the arrangements put in place for the retention, disclosure, storage and destruction of the data; and the controls and safeguards against misuse of the data. The Commissioner will normally discharge his responsibilities through his regular six-monthly inspection visits to GCHQ, or as may be otherwise agreed between the Commissioner and GCHQ.

4.6.10 The relevant team coordinates the Commissioner's inspection visits and makes available to him copies of the section 94 directions and associated paperwork (as required), and a copy of the latest six-monthly review. Any additional papers requested by the Commissioner must also be made available to him."

308) §4.6.11 notes that the Interception of Communications Commissioner provides a biannual report to the Prime Minister on section 94 matters.

GCHQ: Past policy

309) GCHQ's acquisition, use, retention and disclosure of data pursuant to section 94 directions has been subject to the polices set out above from its Compliance Guide, Intelligence Sharing and Release Policy, Reporting Standards and Reporter's Handbook throughout the relevant period (June 2014 and onwards) and, indeed, from before that period. Amongst other things, this meant that all data acquired as a result of a section 94 direction was handled in accordance with RIPA safeguards and was subject to GCHQ's operational data retention policies, including default retention limits. It was also subject to external oversight throughout that period: in 2011 GCHQ invited the Intelligence Services Commissioner to begin ongoing scrutiny of its use of section 94 directions on a non-statutory

basis. GCHQ's past policies in relation to section 94 were accordingly similar to those now in force.

E. SUBMISSIONS IN RELATION TO THE SECTION 94 REGIME

Issue: Does the Section 94 Regime contain adequate safeguards to provide proper protection against arbitrary conduct?

310) The Open Response sets out at §§158-169 and 180-189 the Respondents' submissions on the law in relation to the requirement that any interference be "in accordance with law". Those submissions are not repeated in this CLOSED response.

311) It is the Respondents' position that the "below the waterline" safeguards, which can be taken into account by the Tribunal are such that the regime contains adequate safeguards to provide proper protection against arbitrary conduct. In particular there are detailed internal arrangements which provide comprehensive safeguards in terms of the authorisation for Section 94 activities and the use, storage of, access to, retention and disclosure of any material obtained as a result of such activities. Those important safeguards include, *inter alia*:

a) Detailed internal guidance on the requirements of necessity and proportionality (having regard to the privacy of those whose data is contained within section 94 data) including the need to consider other, less intrusive, methods of obtaining the information;
b) Specific consideration of sensitive data and confidential data;
c) A clear policy on the storage of and access to section 94 data;
d) Specific retention periods and retention/deletion policies which apply to section 94 data;
e) Policies on the handling and disclosure of section 94 data.
f) Clear guidance on the serious consequences of failure to comply with the Handling Arrangements, which include disciplinary action, including potentially dismissal, and prosecution.
g) Training.
h) Oversight, both internal and external.