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

Bulk Personal Data Guidance

Introduction

The policy and legal environment which governs our use of bulk personal data is changing fast. The ground shifted significantly with the Prime Minister's decision earlier this year to avow publicly SIA use of bulk personal data, oversight arrangements and a safeguards regime. This was all in the context of the imminent publication of the ISC's report on privacy and security (the catalyst for the avowal), not to mention David Anderson's investigatory powers review, which was published on Thursday 11 June. The sharp increase in the political profile of bulk data was only too apparent to those parts of MI5 administering our bulk data holdings, with the need to forewarn each data provider that avowal was going to take place. But other parts of MI5, including bulk data users, perhaps felt this less.

Post the election, the new government is now considering changes to our powers and oversight – so-called 're-licensing' – in the light of the ISC and Anderson reviews. As part of this, the SIA use of bulk personal data may become subject to more onerous authorisation processes (beyond our current largely internal ones), as well as enhanced external oversight. At the very least we should expect increased and significant public interest and debate. Indeed, as of Monday 8 June, the Investigatory Powers Tribunal received a challenge to the SIA's use of bulk personal data from Privacy International following ISC avowal. Further scrutiny and debate will follow.

In this context we need to be exemplary in the way we operate our existing processes for bulk personal data. This falls on each and every one of us. Below we describe what we all need to do.

[REDACTION]

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

This guidance sets out the processes to be followed for the handling of Bulk Personal Data (BPD) throughout its lifecycle within MI5. It should be read in conjunction with the SIA Bulk Personal Data Policy.

At all stages of the lifecycle, the following is to be assessed:

- Business justification (necessity and proportionality)
- Intrusion into privacy (for guidance on assessing intrusion see Annex A)
- Corporate risk (for guidance on assessing corporate risk see Annex B)

Ethical considerations

Any person involved in this process, or using the data, may consult with ***an MI5 official in the ethics team*** should they have any concerns regarding MI5's acquisition or use of data. Consultation may take place at any stage of the process and will be treated in strict confidence.

Bulk Personal Data Lifecycle

Definition of Data Categories

BPD Categories

MI5 currently categorises its BPD holdings into the following:

Category	Description
LEA/Intelligence	***These datasets primarily contain operationally focussed information from law enforcement or other intelligence agencies.***
Travel	***These datasets contain information which enable the identification of individuals' travel activity.***
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.***
Finance	***These datasets allow the identification of finance related activity of individuals.***

[REDACTION]

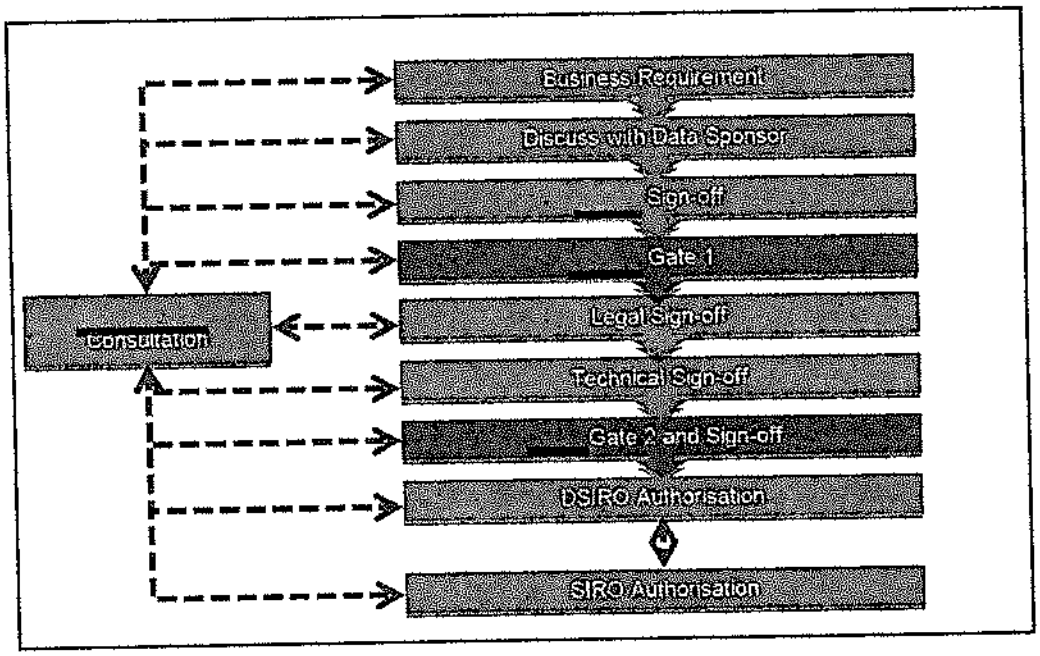
NOTE: REDACTIONS ARE INDICATED [REDACTION] AND GISTS ARE IN BOLD, DOUBLE-UNDERLINED AND ITALICS

Population	***These datasets provide population data or other information which could be used to help identify individuals e.g. passport details.***
Commercial	***These datasets provide details of corporations/individuals involved in commercial activities.***

These BPD categories have been aligned with GCHQ. [REDACTION]

Authorisation

Summary of the Process



The authorisation to acquire BPD is managed via ***the relevant form***. All ***relevant forms*** must be supported by an ***senior MI5 official*** approved business case. Business cases are completed and endorsed initially by the relevant Data Sponsors prior to the Data Sponsoring ***senior MI5 official*** [REDACTION] listed below:

Business area	**Data Sponsoring *Senior Management***	**Data Sponsors**
[REDACTION]	[REDACTION]	[REDACTION]

[REDACTION]

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

When to complete a ***relevant form***

[REDACTION]

A relevant form must be used in any situation where it is the intention to acquire BPD. In essence, this is in any situation where our intention is to 'collect the haystack' rather than 'collecting needles'. ***The data governance team*** and/or ***a legal adviser*** should be consulted in the event of uncertainty. As a rule, ***a relevant form*** must be completed and authorised prior to acquisition. If BPD is acquired unexpectedly or opportunistically (eg from a CHIS, or posted illegally on the internet) ***a relevant form*** must be completed retrospectively as soon as possible including an explanation of why prior authorisation was not sought. The data must not be loaded onto an analytical system until ***the relevant form*** has been authorised.

General points on writing ***the relevant forms***

- The text in the form should be drafted to a similar standard as a warrant application.
- Draft for an external audience (the Commissioner and the Home Office)
- Use 'plain English', avoid jargon, and/or explain any necessary technical terms.
- Be concise; 'more' is not 'better'.
- Be precise and measured in what you write, an easy phrase may give the wrong impression.
- Be aware of potential hostages to fortune; if the document were to be leaked or disclosed, is there anything you might regret having written?
- Attribute assessments - You should not say "It is assessed that". Instead please state who has made the assessment – e.g. "MI5 assess that", "We assess that", "GCHQ assess that".
- Link the case for acquisition, retention or sharing to a statutory function.
- Make sure your case contains the most up to date assessments and intelligence. The insertion of out-of-date assessments and/or contradictory assessments can undermine the submission.

Intrusion

- When assessing intrusion, the key question to consider is 'what is the level of expectation of privacy in relation to this data?'. Secondary questions may be 'would the people who feature in this data expect MI5 to hold this data?'

The following points need to be considered during completion of ***the relevant form***:

Section 1: Data Description

- The Data Sponsor must draft this section in its entirety and in all cases.

[REDACTION]

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

- 'Description of data' must provide a narrative which enables the reader to understand what the data is (its purpose; whether it contains entities/events/content; the sorts of fields available).

Supplier organisation should provide details of any covert authority to acquire the data if appropriate, eg intercept, CHIS, CNE and should be linked to warrant numbers where applicable.

- Where relevant, the type of 'sensitive personal data' should be noted.

Section 2: Business Justification and Privacy Assessment

The business justification also requires the requesting section(s) and the data sponsor to justify the acquisition and subsequent retention and/or updates of a dataset as necessary and proportionate by weighing up, on the one hand, the business gains of having the information against, and on the other hand, any resultant interference with privacy, also referred to as 'intrusion'. In the context of BPD two aspects of intrusion must be considered:

a. MI5 merely holding the data without any action being taken, particularly as the majority of individuals are not of direct intelligence or security interest – the collateral intrusion; and

b. MI5 interrogating the data – the actual intrusion (Guidance on how to assess intrusion levels is available at Annex A.)

If in doubt, you should consult ***a legal adviser*** for advice on these assessments.

- If the proposal requests ingest of data into a location that is not a corporate system [REDACTION] detail the additional controls you propose to implement. Describe how this will impact on the level of intrusion, no matter how marginal it is assessed to be.
- Describe the criteria upon which the data will be deleted [REDACTION].
- Clarify the priority of acquisition and ingest within the context of the relevant acquisition strategy.
- Explain how you propose to use the data, including the types of analysis [REDACTION]. If you know that you intend to put the data to any particularly intrusive use, please comment upon this.
- Describe the benefits that you anticipate will be derived from holding this data and its context compared with other data that is already held.
- If there are alternatives such as case by case requests, explain why acquisition in bulk is proportionate not just expedient.
- Sections should consider whether the acquisition of unnecessary/extraneous data, such as a large proportion of minors (individuals under the age of 16), or sensitive personal data (as outlined in the SIA Bulk Personal Data Policy) is proportionate with respect to the desired outcome. The threshold for acquisition of this type of data is necessarily higher and will require additional explicit justification when permission is sought to acquire it.

Submission and Approval

[REDACTION]

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

1. Following completion of sections 1 and 2, the ***relevant form*** must be approved by the Data Sponsor in the first instance before being endorsed by the Data Sponsor's ***senior management***, prior to submission to the ***relevant team***.
2. The ***relevant team*** will triage the ***relevant form*** and return them where there are pertinent questions or unresolved issues.
3. ***Relevant forms*** that do not require amendment will be sent to a ***legal adviser*** for comment on the legality of the proposed acquisition.
4. ***A legal adviser*** will make their own assessment on the legality of acquiring the data. If they are not satisfied by the legality of the acquisition it will not be progressed further.
5. ***The relevant forms*** will be sent by ***the relevant team*** to the relevant technical team(s) responsible for ingest to ensure that the dataset can be loaded.
6. ***The relevant team*** will complete Section 5 before submitting the ***relevant form*** for authorisation.
7. Once authorised ***the relevant team*** shall inform the data sponsor.
8. In light of the responses from ***a legal adviser*** [REDACTION], ***the relevant team*** will then conduct a final assessment of the necessity and proportionality (which might result in recommending restricted access to part or all of the dataset). They will also make an assessment (high/medium/low) of the extent of political, corporate, or reputational risk and/or damage a compromise of the data would cause, including to the data supplier.
9. ***A legal adviser*** and ***an MI5 official in the ethics team*** may be consulted by any party and at any stage of the ***relevant form*** process, where the necessity and/or proportionality are unclear.
10. Where a relationship with the supplier is required to obtain the data, but the Service does not have one, the authorised ***form*** allows contact to be established with a view to acquiring the data.
11. Written confirmation should be obtained from the data supplier that approval to provide the data has been granted at Board or senior management level (e.g. Senior Civil Service, ACPO rank, Chief Executive) from within the data providing organisation, department or agency. The providing organisation may seek further (higher) approval which in the case of government data may include the Permanent Under Secretary or a Minister. ***The relevant team*** must receive a copy of this confirmation.
12. ***The relevant team*** will escalate the completed ***relevant form*** to a ***senior MI5 official*** on behalf of DSIRO[1] . ***A senior MI5 official*** will review the necessity and proportionality of acquiring the BPD and ensure it will assist MI5 in pursuing its statutory functions; and once satisfied they will authorise the acquisition. As part of this, ***a senior MI5 official*** must also be satisfied that any resulting interference with individuals' right to privacy, as enshrined in Article 8(1) European Convention on Human Rights (ECHR), is justifiable under Article 8(2) for the purpose of protecting national security.

Time Sensitive Acquisition

BPD should only be acquired once ***the relevant form*** has been authorised by ***a senior MI5 official*** on behalf of DSIRO. Where a time-sensitive business requirement is identified, ***a senior MI5 official*** can authorise acquisition verbally however the associated paperwork should be completed within 5 business days.

[1] ***A senior MI5 official*** has the option to escalate to DSIRO or SIRO as necessary.

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

Unsolicited offers to provide a Bulk Personal Dataset

If staff are offered BPD by a contact, the relevant section's ***senior MI5 official*** must be informed and the relevant Data Sponsor consulted. The authorisation process should then be followed if the Service can identify a genuine requirement for the dataset.

[REDACTION]

Acquiring BPD from SIA Partners

When a section becomes aware of BPD held by an SIA partner which may assist MI5 in progressing its work, the section concerned must discuss their requirements and potential access to the information with the relevant Data Sponsor. A formal request to acquire the data must be made on ***a relevant form.***

Once ***the relevant form*** has been authorised by ***a senior MI5 official***, Data Sponsors will complete ***a relevant form*** outlining the business case for acquiring the data, details of the data fields required, update frequency and intended use of the data. This is sent to the relevant SIA partner and once they are satisfied the business case is justifiable and sharing the data will not breach any sensitivity considerations they may have, arrangements will be made to share the data. Timescales are dependent on agreeing a number of necessary procedures, such as:

- The frequency and timings of supply,
- How access to the data will be controlled within MI5,
- Filtering out any unnecessary data (where possible),
- Safe and secure transportation of the BPD,
- Automation of the extract, delivery and ingest process.

Formal applications for acquisition of bulk data from SIA partners must be submitted on the appropriate form and authorised before being sent to the SIA partner. Once the relevant SIA partner is satisfied that the business case is justified and that sharing the data will not breach any security considerations that they may have, arrangements will be made to share the data.

Collection and Storage

Transfer of Data from Suppliers

To ensure the security and integrity of BPD which MI5 relies heavily upon, and to reassure data providers their data will be handled securely, it is essential the appropriate physical controls are in place. These safeguard against unauthorised access to, or loss

of, BPD during transportation to and subsequent storage in MI5 premises.
[REDACTION]

[REDACTION]

Permitted Users and Usage

Access to Bulk Data is limited to those with a business need. Before access is granted all users must read and sign the relevant Code of Practice. They must also attend a compulsory training course that lasts two days (full time or integrated in other courses).

Users and Systems

BPD is currently accessed primarily via MI5's corporate analytical systems [REDACTION].
The size of the user community for analytical systems has a direct impact on intrusion, which will increase as the number of users grows. Owing to the inherent sensitivity associated with BPD, it must be carefully matched to the analytical system it will be loaded into. [REDACTION]
Before access is granted to corporate analytical systems, all users must read and sign a Code of Practice [REDACTION]. Once this is signed [REDACTION] users must also complete a mandatory training course before being granted access to these systems. There is no formal course for the ***specialist*** user community. Users of these systems are instead mentored by experienced colleagues with expertise in these systems and the datasets held within them.
In addition Privileged Users of these analytical systems must also sign the Privileged User Security Operating Procedures (SyOPs) [REDACTION] and there is line manager responsibility for their conduct and training. [REDACTION]

Usage

Permitted queries are typically focused on fully identifying an individual that is subject of a lead or an ***subject of interest*** for whom we hold limited information. By extension it is often also necessary to identify the associates of an ***subject of interest*** to determine if they also pose a threat to national security.

[REDACTION]

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

Sharing Bulk Personal Data

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

Sharing within the SIA

To the extent the SIA all have a common interest in acquiring information for national security purposes, it may be lawful for MI5 to share BPD with SIS or GCHQ. Within the SIA, the relevant gateways for these purposes are (i) section 2(2)(a) so far as **disclosure** by the Security Service is concerned, and (ii) sections 2(2)(a) and 4(2)(a) respectively of Intelligence Services Act so far as **acquisition** by SIS and GCHQ are concerned.

In relation to each dataset, there are two sides to the information transaction, whereby both the disclosing and receiving agency have to be satisfied as to the necessity and proportionality of sharing a particular dataset. MI5 need to establish in each case that both (i) disclosure by the Security Service under section 2(2)(a) is necessary for the proper discharge of the Security Service's statutory function of protecting national security, and also (ii) that acquisition by SIS and GCHQ is necessary for their respective statutory functions in respect of national security under sections 2(2)(a) and 4(2)(a) respectively of ISA.

In circumstances where GCHQ or SIS identifies a requirement, they should discuss their requirements with the relevant MI5 data sponsor. If the requesting agency and the MI5 data sponsor believe there is a business case to share the data a formal request must be made to MI5 via ***a relevant form.*** The relevant data sponsor is then responsible for submitting ***the relevant form***.

When to complete *the relevant form*

The relevant form.

See General points on writing ***the relevant form*** above

The relevant form must be completed when a request for data has been received and the data sponsor believes there is a case to share data (in terms of this guidance BPD). ***The relevant form*** must be completed and authorised prior to the commencement of any sharing.

[REDACTION]

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

Section 1: Data Description

- The Data Sponsor must draft this section in its entirety and in all cases.
- 'Description of data' must provide a narrative which enables the reader to understand what the data is (its purpose; whether it contains entities/events/content; the sorts of fields available.
- Where relevant, the type of 'sensitive personal data' should be noted and justified.

Section 2: Business Justification and Privacy

- How the data will be used and how the purpose of the sharing falls within the MI5's statutory functions. If the data will be put to any particularly intrusive use, please comment upon this.
  The necessity and proportionality case for disclosure of that data and the proposed data handling arrangements.
- What results or benefit do you expect it to provide to the recipient and MI5.
- Any alternative means of achieving the same results.
- Examples of use should be succinct, use codenames/nicknames and be suitable for sharing with SIS/GCHQ where the dataset is acquired from these Agencies.
- Ensure that additional intrusion from the sharing is reflected, rather than the acquisition/retention assessment.

Section 3: Method of Movement and Retention

- Explain how the data will be transferred (or accessed), and the security measures in place such as encryption. If there are any cover arrangements required when sharing then capture these here.
- Provide as much detail as possible about who the data will be able to access the data and how this will be achieved.

Submission and Approval

1. Following completion of sections 1-3, they must be approved by the Data Sponsor in the first instance before being endorsed by ***the senior MI5 official***, prior to submission to ***the data governance team*** with the accompanying ***relevant form*** from the requestor.
2. ***The relevant team*** will triage ***the relevant form*** and return them where there are pertinent questions or unresolved issues.
3. The relevant forms that do not require amendment will be sent to the relevant technical team and ***a legal adviser*** for endorsement.
4. ***The relevant team*** will complete Section 6 of ***the relevant form*** before submitting ***the relevant form*** for authorisation. ***The relevant team*** will confirm the strength of the business case for sharing data is sufficient, and any security, ethical and reputational risks have been adequately considered. This might include undertakings given by MI5 to the data provider that we would not share their information without their prior consent, in which case a higher test of necessity would apply if they were not to be informed (see below).
5. Once authorised ***the relevant team*** shall inform the data sponsor and arrangements will be made for the data to be shared with the relevant Agency using suitably accredited network for electronic transfer. Where electronic transfer is not possible, physical transfer must be conducted in accordance with policy.

[REDACTION]

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

Sharing data and applications in-situ

[REDACTION] Sharing data in this way requires both the requesting and disclosing agencies to assess the necessity and proportionality of the access and use being sought, [REDACTION]
The senior MI5 official should be consulted in relation to any proposals to access data on other SIA systems, or to allow SIA access into MI5 systems.

Sharing outside the SIA

MI5 neither confirms, nor denies the existence of specific BPD holdings to organisations outside the SIA or a limited number of individuals within OSCT. Therefore any request to share BPD with an organisation other than GCHQ or SIS should reiterate this position as the requestor should approach the provider themselves. Attempts to ascertain MI5 BPD holdings by non-SIA organisations should be reported to ***the relevant team***.

In the event that a formal request is made to MI5 for BPD to be shared, the same legal disclosure tests would need to be applied as when sharing with SIA partners. The requestor would also require a legal gateway to acquire the data, which the Security Service would need to be satisfied met the test of necessity and proportionality. All enquiries should be directed to ***the senior MI5 official.***

Informing Data Providers about Sharing Bulk Personal Data

Beyond assuring data providers their information will be handled securely and used to meet our statutory obligations, MI5 will not routinely volunteer any special conditions/limitations regarding sharing.

[REDACTION]

Retention and Review

The Review Process

The Bulk Personal Data Review Panel (BPDR Panel) meets every 6 months to review BPD based on its review category. The aim of the Panel is to ensure BPD has been properly acquired and its retention remains necessary and proportionate to enable MI5 to carry out its statutory function to protect national security. Panel members must satisfy

themselves the level of intrusion generated by a dataset is justifiable under Article 8(2) of the ECHR and is in line with the requirements of the Data Protection Act 1998.

The BPDR Panel operates under the authority of the Executive Board. The BPDR Panel Terms of Reference are available [REDACTION].

When to complete *the relevant form*

The BPD review categories dictate when each dataset will be reviewed. The review of BPD retention must be captured on ***the relevant form***. This should occur when:

- It is more than 6 months since a dataset was acquired and it has not been reviewed since acquisition;
- It is scheduled for review based on the intrusion/risk criteria set out in the BPD policy;
- A Panel member has requested the dataset be reviewed.
- It meets the criteria for referral to the Panel [REDACTION]

See General points on writing ***a relevant form*** above

Summary

- The Data Sponsor must draft this section in its entirety and in all cases.
- This section is designed as a 'summary' and replaces the need for an additional 1-page document that was produced between 2010 and 2014 for the Commissioners visit. It should therefore reflect the general guidance, particularly regarding the need to be concise.
- The date of review should reflect when the ***sponsoring senior MI5 official*** sponsored the case for retention.
- 'Description' must provide a high-level narrative which enables the reader to understand what the data is (its purpose; whether it contains entities/events/content; the sorts of fields available).
- The necessity (and proportionality) case for retention must weigh up, on the one hand, the business gains of having the information against, and on the other hand, any resultant interference with privacy, also referred to as 'intrusion'. It must include:
    - An explanation of how you use the data and the benefits derived at a high level, including the types of analysis [REDACTION], examples should be reserved for section 3a;
    - How the purpose falls within the statutory functions of MI5;
    - If the data has, or will be put to any particularly intrusive use, please comment on this;
    - Any alternative means of achieving the same results;

Highlight any changes to the dataset since the latter of acquisition or last review

Section 1: Data Description

- The Data Sponsor must draft this section in its entirety and in all cases.

[REDACTION]

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

Supplier organisation should provide details of any covert authority to acquire the data if appropriate, eg intercept, CHIS, CNE and should be linked to warrant numbers where applicable.

- Information about sharing should only cover 'ongoing' instances, or one-off sharing that has taken place during the review period. Historic one-off sharing does not need to be recorded.

Section 2: Extent of Intrusiveness

- Ensure that as well as covering the intrusion from retention that, where applicable, the additional intrusion from the sharing is reflected.
- Where relevant, the type of 'sensitive personal data' should be noted.
- If data has been ingested into new analytical systems since the acquisition/the last review, describe how this has impacted on the level of intrusion, no matter how marginal it is assessed to be.
- If the data has been put to any particularly intrusive use, please comment upon this.

Section 3a: Retention case

- Capture the current understanding and account for any changes that have taken place since acquisition or the previous retention case.
- If it is not possible to determine the value of the dataset, a reason must be provided within the necessity case for retention.
- Be concise, the case should be no longer than 3-4 paragraphs.
- Make sure your case contains the most up to date assessments and intelligence. The insertion of out-of-date assessments and/or contradictory assessments can undermine the submission.
- Do not oversell the case; if the value is only limited (or none), be honest.
- Examples of use should be succinct, use codenames/nicknames and be suitable for sharing with SIS/GCHQ where the dataset is acquired from these Agencies.
- Do not rely on 'potential value in the future' in the face of lack of evidence of use – this could be claimed of almost anything.

Section 3b: Sharing case

- Only continued sharing with another Agency requires review. One-off sharing does not require further justification.
- Examples should be drawn from the Agency the data has been shared [REDACTION] with (***The relevant team*** will seek to facilitate the exchange of 'use examples' with compliance teams in GCHQ and SIS; if feedback is not available, the MI5 sponsor will be required to comment on perceived value).

Submission and Approval

1. Following completion of sections 1-3, they must be approved by the Data Sponsor in the first instance before being endorsed by the Data Sponsor's ***senior management,*** prior to submission to ***the data governance team***.
2. The ***data governance team*** will triage ***the relevant form*** and return them where there are pertinent questions or unresolved issues.
3. ***The relevant forms*** that do not require amendment will be sent to ***a legal adviser*** if required for additional comments.

[REDACTION]

4. The ***data governance team*** will complete Section 5 and 6 of ***the relevant form*** and ensure it is available to Panel members at the next review.
5. Once the Panel has met, ***the relevant form*** will be completed by a member of the Panel to reflect the decision of the Panel.
6. The ***data governance team*** will notify sponsors of the Panel's decisions.

At the review the Panel decides whether to retain the dataset for a further review period or to delete it. In particularly sensitive cases, the Panel may recommend an earlier review. Where the Panel cannot agree on retention or deletion, the case will be referred to SIRO, the Executive Board or DG as necessary for a decision.

The BPDR Panel will also review sharing of data, applying similar tests to those for retention. It will also commission and review thematic work in relation to BPD to inform policy development and effective risk management as it judges appropriate.

High Sensitivity Datasets

Specific arrangements are in place for particularly sensitive datasets.

Deletion of Data

Deletion process

If data is no longer required, the relevant Data Sponsor should request its deletion via ***the senior MI5 official***, and not wait for the next review. A ***relevant form*** must be completed.

Section 1: Deletion Request

1. The Data Sponsor must complete this section.
2. If data is stored in areas other than ***the Service's corporate systems***, a detailed description of where the data is stored (giving a full file path where appropriate or an information flow path), and a point of contact who can provide assistance with any deletion queries that may arise, e.g. who has responsibility for the data in ***the relevant team.***
3. Provide details of the date and method of acquisition, including details of original media where applicable, to ensure that all instances of the data are destroyed or deleted.
4. Clearly articulate the deletion requirement, particularly when it is not a full source deletion, including details of date ranges where applicable.
5. Where data has been shared with another agency or the police, ensure that you consult them, before you request full source deletion, to see if they intend to retain the data, and advise ***a senior MI5 official*** of the outcome.
6. The data sponsor ***senior MI5 official*** must sign and electronically approve the deletion request.

[REDACTION]

If agreed, ***an MI5 official*** will authorise the deletion of the relevant data and ***the relevant team*** will manage the deletion in collaboration with the appropriate technical section. Further detail is included in the SIA Bulk Data Policy.

Annex A – Frequently Asked Questions

What is intrusion?

In the context of BPD, intrusion relates to the level of interference with the privacy of individuals (and, in particular, those individuals of no national security interest) caused by the acquisition, retention and use of the dataset. The legal framework is set out in ECHR 8(2) which states that 'there shall be no interference by a public authority with the exercise of this right to privacy except such as is in accordance with the law and is necessary in a democratic society in the interests of national security…'.
In relation to BPD, MI5 recognises a key distinction in levels of intrusion between (i) the simple holding of data (Inherent intrusion) and (ii) the use of that data (Actual and Collateral intrusion). The level of intrusion arising from the holding of data is generally assessed to be very limited. The level of intrusion rises significantly when data is used. Analytical processes are aimed at minimising the collateral intrusion, and distilling out the ***subject of interest*** relevant information as quickly as possible.

How do I assess intrusion?

The overall level of intrusion associated with a bulk personal dataset represents a combination of the following factors, each of which must be assessed on acquisition and review;

Holding Data:

Inherent Intrusion – Level of intrusion inherent in the data, i.e. that which arises from the simple holding of the data, including;

- The extent of 'metadata'[2] v 'content'[3]
- The extent to which the data is publically available
- The extent to which sensitive and personal data are present

Using Data:

Actual Intrusion – the level of intrusion resulting from the analysis and exploitation of data in relation to ***subjects of interest.***

[2] Meaning the combination of 'Communications Data' and 'Content Meta-data' [REDACTION]
[3] Meaning Narrative Data [REDACTION].

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

Collateral Intrusion – the level of intrusion into the privacy of individuals who are not the subject of national security interest ***people of no intelligence interest***), once safeguards to minimise collateral intrusion have been implemented.

The following table illustrates the relationship between Inherent, Actual and Collateral Intrusion, and the characteristics of intrusion at each stage.

	Subjects of interest	***People of no intelligence interest***
Analysis of Data Intrusion arising from analysis and exploitation of data	**Actual Intrusion** • Intrusion levels vary depending on types of analysis • Intrusion levels likely to be highest but deemed necessary and proportionate • Intrusion should always be minimised when conducting analysis	**Collateral Intrusion** • Intrusion levels may be high initially, but greatly reduced when analysis identifies this data relates to ***people of no intelligence interest*** • Intrusion should always be minimised when conducting analysis
Holding Data Intrusion arising from holding data	**Inherent Intrusion** • Level of intrusion determined by; metadata v content; availability (public/private); presence of sensitive data • Level of intrusion the same for ***subjects of interest*** and ***people of no intelligence interest***. • Levels of intrusion limited, until data is accessed and used.	

The overall assessment of the level of intrusion (HIGH, MEDIUM and LOW) associated with a dataset is based on consideration of the following criteria:

Intrusion

High Dataset:

- Contains highly intrusive data
- Contains significant amounts of sensitive and personal data
- Contains significant amounts of content as well as metadata

Medium Dataset:

- Contains limited amounts of highly intrusive data
- Contains limited amounts of sensitive personal data
- Metadata and moderate amounts of content
- Majority of records are non-adverse

Low Dataset:

[REDACTION]

- Does not contain highly intrusive data
- Contains little or no sensitive personal data
- Contains mostly metadata and little or no content
- Mostly adverse records (dataset contains a high proportion of adverse records)

When making an assessment of intrusion, the assessment should be based on the expectation of privacy an average member of the public would have about the data within the dataset. In general, the higher the expectation of privacy, the higher will be the level of interference with privacy. When assessing expectation of privacy, a number of factors need to be taken into account, and the nature of the data needs to be understood:

- has the data been provided willingly by the individual to another government department or agency?
- has the data been provided by the individual to a non-governmental body (e.g. within the commercial sector)?
- has the data been made publically available by the individual (e.g. published on-line)?
- would the individual be aware the data had been collected by the data provider?
- would the individual be aware the data provider might share their data with other bodies?
- does the dataset contain sensitive personal information (please see the MI5 BPD Lifecycle Policy), albeit in a non-detailed format ?
- does the dataset consist of more than basic personal details (e.g. more than name, date of birth, address etc)?
- does the dataset include details of travel movements?
- is the information contained in the dataset anonymous?
- does the dataset include a disproportionate number of minors?
- what amount of data about individuals is contained within the dataset?

As well as consideration of the expectation of privacy, the assessment of intrusion process should always include a "common sense" test which takes into account all the characteristics of the dataset in the round. Understanding the above will enable you to make an assessment of whether the intrusion is LOW, MEDIUM or HIGH.

Examples of Intrusion Assessments

Actual Intrusion Level	**LOW**	**MEDIUM**	**HIGH**
Dataset	OLYMPIC ACCREDITATION	Travel Data [REDACTION]	[REDACTION]
Commentary	The dataset has been knowingly provided to UK	Results of a query would identify the movements of	

HMG for security reasons. There will be an expectation this data would be shared with MI5, and tracing would be conducted against it in the interest of national security. The intrusion is therefore low however any intrusion is still minimised through limiting access and ensuring that all searches are specific and subject to audit.	the individuals subject to the query. Due to limited intelligence it is common for queries to be conducted and return data on people of no intelligence interest. Intrusion is minimised through limiting access and ensuring that all searches are specific and subject to audit. Handling caveats are also imposed to limit risk.

Collateral Intrusion Level	**LOW**	**MEDIUM**	**HIGH**
[REDACTION]	[REDACTION]	[REDACTION]	[REDACTION]

What is Corporate Risk?

Corporate Risk refers to the potential for political embarrassment and/or damage to the reputation of MI5 and its SIA partners, data providers and HMG were it to become public knowledge MI5 holds certain datasets in bulk. It is ***the data governance team's*** responsibility to assess the level of risk, be it LOW, MEDIUM or HIGH by taking the following factors into account:

- the general expectation of privacy in any given dataset, and the assessed levels of collateral and actual intrusion (see 'Intrusion' above),
- the public foreseeability of MI5 holding the data, and the possible media and public response were it to become known that MI5 held certain datasets in bulk;
- The impact on MI5 capabilities, including the potential compromise of sensitive sources and techniques, the impact on investigations and operations, or the identification of MI5 staff;
- the impact on the reputation of the data providers and our relationship with them [REDACTION];
- the impact on liaison partners and our relationship with them [REDACTION];

- the resulting reputational and operational damage to MI5 and HMG more widely.

[REDACTION] ***Were it to become widely known that the Service held this data the media response would most likely be unfavourable and probably inaccurate.***

Annex B – Corporate Risk

HIGH	Dataset: • Is not publically available and/or not avowed in public and/or viewed as highly protected by the owner • It is not publically foreseeable that MI5 would hold the data or have access to it • [REDACTION]
MEDIUM	Dataset: • is not publically available; and viewed as moderately sensitive by the owner. • it is partially foreseeable to the public that MI5 would be interested in (and may hold or have access to) such data in bulk. • [REDACTION]
LOW	Dataset: • Is generally available (publically or nearly publically available) • It is publically foreseeable MI5 would have access to the data (or possibly hold it) to support their statutory functions. • [REDACTION]

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

Examples of Corporate Risk Assessments

	LOW	MEDIUM	HIGH
Dataset	[REDACTION] passport data [REDACTED]	[REDACTION]	[REDACTION]
Corporate Risk Explanation	The corporate risk is LOW as the public has a reasonable expectation MI5 holds travel-related data and may hold it in bulk. Moreover, passport forms state that details may be passed to other departments and agencies when it is in the 'public interest' to do so.	[REDACTION]	[REDACTION]

How long will it take before I can access the data?

Following approval, timeliness will in part depend on the priority of the acquisition. The acquisition and ingest phases of data require necessary procedures to be followed before it is exploitable, such as:

- Defining the business requirements (scope, frequency and priority of the dataset)
- Cover arrangements for the MI5 relationship for this provision
- Prior agreement for any payment relating to data provision
- Ensuring the data owner can supply the data as securely as possible,
- Agreeing the frequency and timings of supply with the provider,
- Organising the data so it can be ingested into MI5 systems as efficiently as possible,
- Filtering out any unnecessary data (where possible)