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

SECURITY SERVICE
MI5

Bulk External Data Acquisition - Internal Authorisation Processes

Document History
Reviewed by: ***MI5 officials and legal advisers***
Status –Issued
Author: ***MI5 official***

Distribution
MI5 officials and legal advisers

[REDACTION]

[REDACTION]

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

Key Issues:

- Outside of specialist areas, current bulk data request authorisation processes are unclear and not widely understood.
- Bulk data requests are increasing and are often being made by desks unfamiliar with best practice.
- This combination generates risks:
  - Does the original request meet a national security requirement and has this been validated by Service management and can we prove this if challenged?
  - Is the request compatible with Service bulk data acquisition policy?
  - Is there a review process in place to ensure that its retention is lawful?
  - How do we ensure that we can cope technically with the data?

Key Recommendations:

To minimise these risks I propose that we should:

- Assert that ***the relevant team*** will not acquire and ***the analytical systems*** will not accept bulk data unless it is accompanied by evidence showing that its initial acquisition was correctly authorised and a review process is in place.
- Insist on all initial bulk data acquisition being authorised by a ***Grade 2*** in the relevant sections.
- Convert the grid created by the ***legal advisers*** into ***the relevant form*** (draft at Annex A).
- Give Service wide visibility to bulk data acquisition best practice.
- Examine whether we should use elements of the grid to create a [REDACTION] authorisation engine for bulk data requests.
- All Branches (with the **possible** exception of ***the relevant team***) should have central points of contact for all data related policy and data management issues (data coordinator- see annex B for draft list of functions).
- The dataset review process is currently the responsibility of the sponsoring section. In the future we should seek to manage this centrally [REDACTION]
- [REDACTION]
- Trial these proposals [REDACTION] before making them Service wide.
- Ensure that we do not duplicate existing necessity and proportionality processes used to obtain material under an Interception Warrant or Communications Data Notice/Authorisation or Property Warrants.

Overview of Current position

The relevant team holds a list of data already in the Service. [REDACTION] However, although it is likely to be accurate I cannot guarantee that it provides a total capture of all bulk data in the Service as there are no comprehensive central records.

[REDACTION] ***Legal advisers*** have been copied in on all reviews and the majority of the requests. Clearance has usually been at ***Grade 2*** level (occasionally higher).

Other sections with much lower data request volumes have less mature authorisation and review processes. [REDACTION] This ensures the application of standard processes and a single point for gathering information about data in each branch. There is no comparable central point in any other branch.

Some sections have been handling bulk data for some time. [REDACTION]

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

The relevant team has set policies for data ingest (copy of form attached) and make plain the responsibilities of the data sponsor. ***The relevant team*** are given a deletion date and will only change this if they are informed that a review has identified a new date. They also keep records of what data is in their system. [REDACTION] ***The relevant team*** applies standard RIPA handling arrangements, which imposes standard deletion dates, to this material.

Recommendations

Authorisation - As there is no central authorisation policy it is not possible to validate that best practice has been followed in all data requests. Any policy that we do establish has to cope with:

a) Other regimes for some data (eg RIPA)
b) Confusion over what is meant by 'Bulk Data'
c) Varying data sizes and sensitivities make a one size fits all solution difficult.
d) Low general awareness of guidance on issues to consider when seeking bulk data.

I propose that:

a) To avoid confusion we set a policy that applies to any data set that will be processed by ***the analytical system*** unless it has been obtained through interception, in which case the appropriate handling arrangements will apply.
b) Define bulk data as
    a. "Electronic data sets that are too large to be easily susceptible to manual
    b. processing and contain data about multiple individuals."
c) Make plain that this policy does **not** apply to any data that is acquired commercially (eg: [REDACTION])
d) We do not seek to broaden this policy to cover all data held by the Service (however those holding/exploiting data elsewhere in the Service may wish to consider similar arrangements).
e) Require that all bulk data acquisition is authorised by a ***Grade 2*** in the sponsoring
section. If the data request is particularly intrusive the ***Grade 2*** should consider seeking ***senior MI5 official*** endorsement.
f) Use the current ***legal adviser*** questionnaire as guidance on the intranet and as the basis for ***the relevant form*** (or possibly an intranet based form on ***the relevant team's*** website) that would capture these authorisations and endorsements.
g) Demand that all bulk data requests to ***the relevant team*** use this form and that all data for ingest into ***the analytical systems*** is accompanied by this form.
h) Use Service Update and ***the relevant team's*** intranet site to lift Service awareness of these decisions and general bulk data issues.
i) Trial these proposals in the [REDACTION] business before making them Service wide.

Tracking and Review - a) above means that we need to widen the concept of the ***relevant team*** ingestion process to encompass an '***analytical system*** gatekeeper' role. This role ensures that anyone responsible for accepting bulk data onto ***the analytical system*** is given evidence of authorisation and an effective retention review process. This concept should also transfer to ***the analytical system domain information manager*** role.

We will also need to ensure that our systems for tracking data within ***the analytical system*** provide all the information we need. Key will be the sponsoring section who will need to own the review of the data where the data has a single section benefit. Where

service wide benefits are being seen it might be appropriate to expand this review process to include a selected user group.

Loose Minutes can be used to capture the information identified in' [REDACTION] guidance and can also be used to record authorisation. However, they are not an effective method for tracking or retrieving data requests. ***The relevant forms*** share the same strengths and weaknesses. We may need to create a more automated approach to this process [REDACTION]. However, in the short term the only viable option is ***the relevant form.*** A possible draft is shown below. It incorporates the information required in the [REDACTION] questionnaire but tries to make the language and structure more accessible to staff with no or limited experience of the issues associated with data exploitation.

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

Annex A.

Bulk Data Acquisition Authorisation

CC (when complete) to ***MI5 officials***, file ...

Bulk data can be defined as "Electronic data sets that are too large to be easily susceptible to manual processing and contain data about multiple individuals." This form does not apply to data that does not match this definition. It should be used for the initial acquisition of a dataset but should not be used to justify subsequent updates, so long as this was identified and justified in the initial acquisition form.

This form provides a means for authorising data acquisition where this is not provided by other processes. For example, the 'legal' portion of this form should not be used for material obtained under interception warrant (RIPA) or property warrant (ISA). However, without the information captured by this form ***the relevant team*** will not acquire data and [REDACTION ***the relevant team*** will not incorporate the data into any ***analytical systems***. It may therefore be useful to use the other sections of the form to provide ***the analytical system*** with the information it needs to accept data onto their systems.

When complete the original should be retained by your section's data exploitation Coordinator

Data Description

Name of Source Database:	
Organisation that owns the data:	
Brief description of source database:	
What data are you requesting?	
Who, in the Service, will be negotiating	
the acquisition of this data?	
Handling caveats	
Protective marking	

Data handling information

Proposed data retention period:	
Proposed retention review frequency (usually every 6 months):	
Details of point of contact within owning organisation (including telephone number and Email address):	
Point of contact (i.e. data sponsor) within the Service:	
Delivery method [REDACTION]	
Delivery frequency (One off, monthly etc)	
Storage and processing location (ie ***the relevant analytical systems***) and have you confirmed that they have the ability to process the data?:	

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

Will access to the data need to be controlled [REDACTION]	

Necessity and Proportionality

Please describe how you intend to use the data and why this is necessary to help the Service to meet its statutory requirements to protect national security.
Please explain the level of intrusion into privacy: (Issues you should explore include - The nature of the data (it is personal data etc?) Does the database contain a high or low proportion of people of no intelligence interest? Is the data anonymous and will it remain so? [for example could other data or techniques available to the Service be used to remove this anonymity?] Have you requested the totality of the database or a subset and does this help to manage intrusion? Who in the Service will have access to the data?)
What results and benefits will exploiting this data bring and could these be achieved by other means without the use of bulk data?

Authorisations

Applicant

Name ***Staff Role*** Ext

Authorising officer

Grade 2 *within the sponsoring section (your role is to ensure that the issues of necessity and proportionality have been properly considered and that alternative approaches would not deliver the same results).*

Name ***Staff Role*** Ext

Endorsement (optional)

Senior MI5 official *endorsement should be sought by the* ***Grade 2*** *authoriser if they feel that the request is particularly intrusive (for example does the data include unusually large numbers of people of no intelligence interest or is the data extremely intrusive/delicate eg* [REDACTION]*).*

Name ***Staff Role*** Ext

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

Annex B

Role of the Section Data Coordinator

a) To provide guidance to ***the analytical system*** on their section's bulk data requirements.
b) To review whether the retention of any bulk data held in ***the analytical system***, on their section's behalf, remains necessary and proportionate (usually every six months).
c) To coordinate with ***the relevant teams*** all bulk data requests from their section.

[REDACTION]

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

Date	**Users of Process**	**Communication strategy**
13/10/2006	Trial Process in ***the relevant team***	Note circulated in ***the relevant team***
6/11/2006	Extend to ***the relevant team***	Note circulated in ***the relevant team***
15/01/2006?	Extend to all ***the relevant team***	Summary in Service update, Intranet guidance, briefing of ***Grade 2's and Grade 3's.***
15/03/2006?	Extend to all Service	Announcement in Service update. Use Intranet to identify all Service coordinators.

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

Bulk Data Acquisition Authorisation

CC (when complete) to ***MI5 officials and legal advisers*** file …

Bulk data can be defined as "Electronic data sets that are too large to be easily susceptible to manual processing and contain data about multiple individuals." This form does not apply to data that does not match this definition. It should be used for the initial acquisition of a dataset but should not be used to justify subsequent updates, so long as this was identified and justified in the initial acquisition form.

This form provides a means for authorising data acquisition where this is not provided by other processes. For example, the 'legal' portion of this form should not be used for material obtained under interception warrant (RIPA) or property warrant (ISA). However, without the information captured by this form ***the relevant team*** *will not acquire data and* ***the relevant team*** *will not incorporate the data into any* ***analytical systems.*** *It may therefore be useful to use the other sections of the form to provide* ***the analytical system*** *with the information it needs to accept data onto their systems.*

When complete the original should be retained by your section's data exploitation coordinator

Data Description

Name of Source Database:	
Organisation that owns the data:	
Brief description of source database:	
What data are you requesting?	
Who, in the Service, will be negotiating the acquisition of this data?	
Handling caveats	
Protective marking	

Data handling information

Proposed data retention period:	
Proposed retention review frequency (usually every 6 months):	

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

Details of point of contact within owning organisation (including telephone number and Email address):	
Point of contact (ie data sponsor) within the Service:	
Delivery method [REDACTION]	
Delivery frequency (One off, monthly etc)	
Storage and processing location (ie ***the relevant analytical systems***) and have you confirmed that they have the ability to process the data?:	
Will access to the data need to be controlled [REDACTION]	

Necessity and Proportionality

Please describe how you intend to use the data and why this is necessary to help the Service to meet its statutory requirements to protect national security.	
Please explain the level of intrusion into privacy: (Issues you should explore include- The nature of the data (it is personal data etc?) Does the database contain a high or low proportion of people of no intelligence interest? Is the data anonymous and will it remain so? [for example, could other data or techniques available to the Service be used to remove this anonymity?] Have you requested the totality of	

the database or a subset and does this help to manage intrusion? Who in the Service will have access to the data?)	
What results and benefits will exploiting this data bring and could these be achieved by other means without the use of bulk data?	

Authorisations

Applicant

Name ***Staff Role*** Ext

Then convert the document to 'comment only'.

Authorising officer

Grade 2 *within the sponsoring section (your role is to ensure that the issues of necessity and proportionality have been properly considered and that alternative approaches would not deliver the same results).*

Grade 2 **- Use the comment facility here to approve the above (including your name in the comment):**

Endorsement (optional)

Senior MI5 official *endorsement should be sought by the* ***Grade 2*** *authoriser if they feel that the request is particularly intrusive (for example does the data include unusually large numbers of people of no intelligence interest or is the data extremely intrusive/delicate eg* [REDACTION].

[REDACTION]

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

Senior MI5 official **- Use the comment facility to here to approve the above (including your name in the comment):**

[REDACTION]