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

FORM FOR ACQUISITION

Section 1: Data Description *(to be completed by Data Sponsor)*

Dataset Codename: *(please consult **the relevant team** to obtain an MI5 codename)*		***Form for acquisition*** **Reference:** *(this should be obtained from **the relevant team**)*	
Data Sponsor: *(name and **Staff Role**)*			
Source Database:			
Supplier Organisation:			
Original Source: *(if different from supplier)*			
Supplier Contact Details:			
Supplier System Accreditation:			
Description of Data:			
Supplier Classification:	Please select	(no STRAP)	(no national caveat)
Adverseness:	please select		
Does the dataset contain Personal Data? *(provide further detail in the adjacent box)* ☐ Identifying Personal Data *(from the data itself or in combination with other data that is or likely to become held by MI5)* ☐ Information about Activities *(e.g. travel,* [REDACTION]*)* ☐ Sensitive Personal Data *(biometric, financial, medical, racial or ethnic origin, religious, journalistic, political, legal, sexual, criminal activity)*			

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

☐ Other			
Data on UK Nationals:			
Data on Minors: *(defined as anyone under 16, if possible please provide metrics)*			
Data Schema Provided:			
Size of dataset:	Please select please be more specific if possible		
Start of Dataset Coverage:		End of Dataset Coverage:	
Proposed Update Frequency:			
Change/Delta Size:			
[REDACTION]	[REDACTION]		

Section 2: Business Justification & Privacy Assessment *(to be completed by Data Sponsor)*

Proposed Destination System(s): *(please note that loading may only occur to destinations listed here)*:	[REDACTION] ☐ Other
Proposed Access Restrictions:	
Retention Period: This dataset will be automatically entered into a [REDACTION] rolling review period for deletion. Please state the business case for a different deletion review period here if appropriate.	
Statement of necessity and proportionality: Please now explain why the acquisition is necessary and proportionate covering the following points: • How will the data be used? • What results or benefit do you expect it to provide? • Are there alternative means of achieving the same results?	

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

Assessment of Privacy:	
Assessment of Actual Intrusion and measures taken to minimise this: *(Actual intrusion in this case is taken to mean the intrusion in this case is taken to mean the intrusion or interference with privacy caused by accessing the data as a result of analysis.)*	
Classification of Actual Intrusion:	Please select
Assessment of Collateral Intrusion and measures taken to minimise this: *(Collateral intrusion in this case is taken to mean the intrusion caused by holding the dataset in our analytical systems, prior to any action taken by an analyst or investigator.)*	
Assessment of Collateral Intrusion:	Please select
Referred to ***Ethics***:	Please select
If you have answered 'yes' to the above, please provide further detail:	
Business Justification Sign Off *(to be completed by Data Sponsor)*	
Name/ ***Staff Role:***	
Date:	
Please initial electronically once completed	
Business Justification Approval *(to be completed by Data Sponsor **Senior MI5 Official)***	
I am satisfied: • that the use of this dataset is necessary • that the use of this dataset is proportionate to what is sought to be achieved	
Name/ ***Staff Role:***	
Date:	
Please initial electronically once completed	

Section 3: Legality of Acquisition *(to be completed by **a legal adviser)***

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

Legal Adviser Comment:	
Legality of Acquisition Sign Off *(to be completed by **a legal adviser**)*	
Name/ ***Staff Role:***	
Date:	
Please initial electronically once completed	

Section 4: Technical Feasibility *(to be completed by technical team ingesting the data)*

Technical Team(s) Comment *(If required)*	
Technical Feasibility Sign Off *(to be completed by technical team ingesting the data)*	
Name/ ***Staff Role:***	
Date:	
Please initial electronically once completed	

Section 5: Information Assurance *(to be completed by **the relevant team**)*

Team Comment: Please comment on the following: • Intrusion • Proportionality • Necessity • Adverseness	
Does holding this dataset have the potential to cause political embarrassment or reputational damage to the Service and its partners?	
Overall Classification of Corporate Risk:	Please select

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

Access Restrictions:			
Handling Caveat:			
MI5 Classification:	Please select	(no STRAP)	(no national caveat)
Information Handling Category:			
Review Period:			
Referred to ***Ethics***:	Please Select		
Referred to ***Legal Adviser:***	Please Select		
Information Assurance Sign Off *(to be completed by **the relevant team**)*			
Name/ ***Staff Role:***:			
Date:			
Please initial electronically once completed			

Section 6: Final Approval *(to be initialled electronically by SIRO or designated person)*

I am satisfied: • that the use of this dataset is necessary • that the use of this dataset is proportionate to what is sought to be achieved • that legal, ethical and practical implications have been adequately examined • that satisfactory arrangements exist for ensuring proper management and protection of the data I authorise the acquisition of this dataset.
Final Approval Sign Off *(to be completed by SIRO or designated person)*
Name/ ***Staff Role:***
Date:
Please initial electronically once completed

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

Annex A Instructions for Completing this Form

The relevant forms are designed to ensure that the Service's bulk personal data acquisitions are necessary and proportionate. In legal terms, bulk personal data acquisitions are defined as:

> 'datasets acquired under Section 2(2)(a) of the Security Service Act 1989 or Sections 2(2)(a) or 4(2)(a) of the Intelligence Services Act 1994 which contain personal data about a wide range of individuals, the majority of whom are not of direct intelligence interest.'

In non-legal terms, Bulk Personal data may be described as a dataset or database containing personal data about a large range of individuals, including individuals who are of no intelligence interest to the Service, and which is too large to be susceptible to manual processing.

Instructions for completing this form:

The following process is intended to ensure the correct authorisations are in place **prior** to acquiring bulk data.

1. The Data Sponsor completes *Section 1* and 2 and electronically initials the form.
2. The Data Sponsor's ***senior MI5 official*** approves *Section 2* electronically initials the form.
3. The Data Sponsor emails the ***relevant team*** to ***the relevant team*** who log the requirement and distributes to ***Legal advisers and the relevant team.***
4. ***Legal advisers*** complete *Section 3* and gives approval to proceed by electronically initialling the form.
5. ***The relevant team*** complete *Section 4* and electronically initial the form.
6. ***The relevant team*** complete *Section 5* and electronically initial the form.
7. DSIRO provides final approval for the acquisition to proceed and electronically authorises the form.
8. The completed ***relevant form*** is then stored by ***the relevant team*** in a cabinet shared with Data Sponsors and ***the relevant team*** for future reference.

[REDACTION]

Sensitive Source

If the dataset you wish to acquire is from a sensitive source, such as an agent, then it is possible to limit the knowledge of the source, however the acquisition of a dataset must be recorded. The ***relevant form*** process must be followed however following business ***senior MI5 official*** authorisation the ***relevant form*** can be sent directly to ***a senior MI5 official*** for authorisation. CIRP must be provided with a separate ***relevant form*** to be stored centrally and used for review purposes, this should also be authorised by ***a senior MI5 official***. This ***relevant form*** should contain as much detail in Section 1 (Data Description) as possible. The supplier reference should inform the reader that the completed ***relevant form*** is held by the relevant data sponsor.

Assessing Intrusion

When requesting authorisation you will need to assess the interference with privacy resulting from:

a. the Service merely holding that data without any action being taken – the **collateral intrusion**; and

[REDACTION]

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

b. the Service interrogating that data – the **actual intrusion**

Collateral interference with privacy refers to the intrusion resulting from the Service holding information on an individual who is of no intelligence interest, prior to that information being interrogated or looked at in any way. This sort of interference with privacy is the 'price' we pay for being able to use bulk personal datasets to find those who are of intelligence interest. Due to the measures which the Service takes to only acquire those parts of a dataset which are really necessary, hold bulk personal datasets securely, and restrict access to bulk personal datasets, the collateral interference with privacy will almost always be very low and, in any event, lower than the actual interference (as to which see below).

Actual interference with privacy refers to the intrusion which takes place when analysts or investigators perform a search on against the dataset, resulting in a 'hit' which then prompts them to look at the information on a specific individual and take action. The level of interference with privacy will rise at this point; the extent to which it will rise will depend upon the factors set out below.

Both collateral and actual interference with privacy are assessed at 3 levels: LOW, MEDIUM and HIGH and each type of interference is assessed separately since they will not usually be the same.

As a general guideline, you should bear in mind that collateral interference will almost always be LOW and that actual interference will almost always be higher than collateral interference.

When making your assessment, be it of collateral or actual interference, you should assess the expectation of privacy that the average person would have in the data within the dataset.

As a general guideline, the higher the expectation of privacy, the higher the level of interference with privacy. When assessing expectation of privacy, there are a number of factors that need to be taken into account which will require you to understand the nature of the data you are acquiring, as follows:

- 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 that the data had been collected by the data provider?
- would the individual be aware that the data provider might share their data with other bodies?
- does the dataset contain sensitive personal information (e.g. relating to finances or medical conditions), 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 that takes into account all the characteristics of the dataset in the round. Check that you have considered all the relevant factors and that you

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

have given appropriate weight to those factors. Ask yourself whether the intrusion level you have arrived at sounds reasonable.

Understanding the nature of the data you are acquiring coupled with the common-sense test outlined above will enable you to make an assessment of whether the intrusion (or interference with privacy) is LOW, MEDIUM or HIGH.