*All gists in the following extract are double-underlined

AUTHORISATION OF BULK DATASET

1. Definition

This Authorisation Form records the justification for SIS' handling and usage of specific bulk datasets. In legal terms, bulk 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 data about a wide range of individuals including (adverse) data about individuals who are not of direct intelligence interest.*

Authorisations **are** required where a bulk dataset:

- is likely to include large amounts of superfluous or non-targeted data;
- includes data about individuals of no intelligence interest that may be of a personal or sensitive nature;
- has been generated by any external organisation or partner agency and exhibits the above characteristics;
- will be exploited through the use of intrusive data mining techniques, however it is acquired.

2. Acquisition Case *to be completed by the Acquiring Officer*

Dataset Codename and File Reference	
Data Owner **NB: A senior SIS official will be the data owner unless specified. This means a senior SIS official will have devolved responsibility for 'Action On'.**	
Brief Description of Dataset Content	
Source [redacted]	
Date of Acquisition (DD/MM/YYYY)	
Proposed frequency of update	\<select>
Protective Markings	\<select> \<select>
National Caveat	\<select> Other:
Action On (Designation/Organisation) **NB: Please specify only if different from the data owner or if data is not owned by SIS [redacted]. The Officer stated will be expected to respond to enquiries from HO teams [redacted] and Duty Officer when required**	
Can this Data be Shared?	SIA: Yes ☐ No ☐ [redacted]
Media Serial Number	

Necessity

Please explain why it is necessary for SIS to hold and, where relevant, exploit this data covering the following points:

- Which NSC strategic intelligence priorities does this acquisition meet?
- What results or benefit do you expect it to provide?

Risk Assessment

Please comment on the following:
- What are the risks of holding this dataset that might have the potential to cause political embarrassment?
- What is the reputational damage to HMG or to SIS' operational equities should SIS possession of this dataset become known?

Overall classification of Corporate Risk	\<select\>
Designation/Staff Number	
Date	

3. Data Intrusiveness (to be completed by the Transformation Officer)

Contains Data on UK Nationals?	Yes ☐	No ☐	Unable to identify ☐
If 'Yes' or 'Unable to Identify', please provide further details.			
Contains Data on Minors (under 16s)?	Yes ☐	No ☐	Unable to identify ☐
If 'Yes' or 'Unable to Identify', please provide further details.			
Is this to be exploited?	Yes ☐ No ☐		

(To be agreed with <u>an officer from the relevant team</u>)				

Contains Protected Characteristics				Contains Confidential Information			
	Yes	No	Exploit		Yes	No	Exploit
Religion	☐	☐	☐	Financial	☐	☐	☐
Political	☐	☐	☐	Criminal Activity	☐	☐	☐
Racial/Ethnic Origin	☐	☐	☐	Legally Privileged Info	☐	☐	☐
Disability/Medical Condition	☐	☐	☐	Journalist Info	☐	☐	☐
Sexual Orientation	☐	☐	☐	Medical Info	☐	☐	☐
				Spiritual Counselling	☐	☐	☐

If 'Yes' please provide further details	
Designation/Staff Number	
Date	

4. Exploitation Case (*to be completed by the Exploitation Officer*)

<u>Intrusion of Exploitation</u>

What is the assessment of the level of actual and collateral intrusion?

- Actual: the intrusion of (or interference with) privacy caused by accessing personal data as a result of analysis;
- Collateral: the intrusion or interference with privacy caused by holding the dataset in our analytical systems, prior to any action taken by an analyst.

Classification of Actual Intrusion	<select>
Classification of Collateral Intrusion	<select>
Proposed Exploitation System [redacted]	
Proposed <u>database</u> description	

<u>Justification</u>

- What intelligence benefits are to be derived from the exploitation of the data?
- How will SIS make use of this data?
- Explain why the continued retention and/or exploitation of the data is proportionate and necessary.

Designation/Staff Number	
Date	

5. Legal Advice *(to be completed by <u>Legal Advisers</u>)*

I am satisfied that the legal and ethical implications have been adequately examined. I authorise the retention and/or exploitation of this dataset.	
Designation/Staff Number	
Date	

6. Data Authorisation *(to be completed by <u>a senior SIS official</u>)*

I am satisfied that it is necessary and proportionate for SIS to retain and/or exploit this data set as described above, and that satisfactory arrangements exist for ensuring proper management and protection of the data. I authorise the retention and/or exploitation of this dataset.	
Designation/Staff Number	
Date	