*All gists in the following extract are double-underlined

Information Policy: Bulk Personal Dataset Retention v2.3

	Intrusion Levels		
	High intrusion	Medium intrusion	Low intrusion
Review period	6 months	12 months	24 months

Table 1 – Retention periods

1. Retention periods shall be applied to all bulk personal datasets based on the level of intrusion they represent.
2. It is the Data Owner's responsibility to assign a level of intrusion and a justification for assigning that level. This can be amended by the Data Retention and Review Panel. The rationale for assigning or amending an intrusion level will be held on the central register.

Version: 2.3

Introduction

1. During a review of policy for the lifecycle of a bulk personal dataset a decision was taken to reconsider the retention, review and disposal schedules for bulk-acquired data. The document 'Information Policy: Bulk Personal Dataset Retention v1.1' was approved by the Information Policy Group in January 2014. This paper, v2, is an update to reflect new retention periods for bulk personal data. In parallel with this update, the guidance 'Bulk Personal Data: Guidance on the Authorisation Process' has been revised. As part of drafting this paper, discussions were held with members of the relevant directorate and Legal Advisors, as well as a review of relevant papers.

Scope of Policy

2. To cover all SIS bulk personal datasets.

Rationale

3. SIS needs actively to manage bulk datasets such that they are not held for longer than the Service requires and can be justified. This conforms to legal requirements. Bulk personal data sets are acquired and go through a process of assessment, authorisation and transformation before the data is in an exploitable state

4. After authorisation, bulk personal datasets are reviewed periodically to ensure that they are only retained for so long as is necessary and proportionate. As part of Information Policy: Bulk Personal Dataset Retention v1.1' it was agreed that SIS would no longer review each bulk personal dataset every six months, and that there would instead be different review periods depending on the intrusion level of the dataset (12, 24 and 36 months). The policy incorporated a 6 month grace period for new datasets to allow a period for authorisation and ingestion.

5. This updated policy set review periods at six months, 12 months and 24 months. Each dataset will be assessed for intrusion level; and the intrusion level will determine the review period. High intrusion datasets will be reviewed at least every six months; medium intrusion datasets should be reviewed at least every 12 months and low intrusion datasets at least every 24 months. This is in line with policy at MI5 and with established practice at GCHQ. The policy also removes the six month grace period to improve still further the risk mitigation on intrusive datasets.

6. SIS guidance 'Bulk Personal Data: Guidance on the Authorisation Process' contains guidance on how datasets should be assessed for, and allocated to, an intrusion level. The Guidance has been revised with input from SIS lawyers.

7. Separately, datasets are given a corporate risk rating of high, medium or low during the assessment and authorisation process. This relates to the corporate risk to SIS and HMG of holding the data and considers the potential for political or reputational embarrassment, any economic impact on the UK or the risk of litigation. The Data Owner and subsequently the Data Retention and Review Panel may decide to assign a dataset to a more regular review period than the level of intrusion might dictate (but never a less regular review period).

8. It is important that central registers of information relating to bulk personal datasets continue to be kept as this will assist in management and compliance activities, including oversight. There must be a central register for hard copy media as well as for the details and status of the individual bulk personal datasets, including any incremental components. This paper contains information policies based on these central registers existing and being actively managed.

9. The revised policy will be communicated to the Intelligence Services Commissioner for information and any feedback.

Possible adverse impact
10. N/A

Who will lead the Implementation and Monitoring
11. The relevant team with the Data Retention and Review Panel

Proposer: A senior SIS official Date: 22/10/2015

Information Policy Group Approval:
IPG Chair: A senior SIS official Date: 22/10/2015