*All gists in the following extract have been underlined

Bulk Data Policy v1 2009 – November 2010

CHAPTER XX: BULK DATA ACQUISITION AND EXPLOITATION

Responsible Controller: The relevant SIS official

PURPOSE AND DEFINITION

1. SIS acquire and exploit bulk data to produce operational intelligence and targeting leads. The following terms and definitions are used in this policy:

a. **Bulk data**: raw electronic information on multiple individuals or organisations, which may contain the details of untargeted individuals and which is sought or processed for intelligence purposes.

b. **Targeted data**: raw electronic information on targeted individuals or organisations [redacted] that does not fall into the category of Traditional Information.

c. **Traditional Information**: SIS's electronic corporate data [redacted] or intelligence reporting from other agencies (e.g SIGINT, liaison reporting).

CO-ORDINATION

2. The relevant teams generate service-wide data acquisition and exploitation requirements in consultation with other operational teams, and prioritise requirements against current and future capability.

LEGAL FRAMEWORK OVERVIEW

3. Bulk data, in particular, contain large amounts of personal information. In acquiring and exploiting personal data, SIS are subject to the Intelligence Services Act 1994 (ISA), the Human Rights Act 1998 (HRA) and the Data Protection Act 1998 (DPA). To comply with the statutory obligations, the acquisition, retention, use and disclosure of bulk data must be necessary, pursuant to SIS statutory functions in the ISA, as exercised for one or more of the statutory purposes (in the interests of national security, the prevention and detection of serious crime, or to safeguard the economic well-being of the UK).

4. The Service at all times acts in accordance with the law. Exploitation of personal data amounts to an interference with privacy in ECHR terms, so in order to comply with the HRA and the ISA, SIS must ensure that its conduct in relation to each process is necessary and is proportionate to the operational need. The Service seeks to comply with the data protection principles in the DPA, but where it cannot do so for the purpose of safeguarding national security, its actions will be covered by the exemption for national security in section 28 DPA.

5. Acquiring, retaining, using and/or disclosing personal data will amount to conduct that can be examined and assessed for its lawfulness by the Investigatory Powers Tribunal and/or the Information Tribunal.

6. Accordingly, Service policy has been devised to comply with the law. This policy will be kept under review and updated when necessary or desirable.

SERVICE POLICY

7. The relevant team is responsible for overall service data policy. A legal advisor oversees legal aspects of data management.

8. Whilst the law applies to all data that SIS hold, different types of data have distinctive characteristics. As guiding principles:

a. **Bulk data** – Acquiring and processing bulk data may entail greater interference with privacy. SIS must consider this intrusion carefully when assessing the necessity and proportionality of acquisition and exploitation. If there is a risk of embarrassment to HMG or if authorisation is required under the ISA, SIS will submit or seek other relevant authorisations on data acquisition. If a submission is unnecessary, the relevant SIS official is responsible for authorising bulk data acquisitions. The relevant SIS official is also responsible for authorising the transformation into an exploitable form of data that has been acquired unsolicited [redacted]. Authority is delegated to an alternative SIS official in the relevant SIS official's absence. The Data Acquisition/Transformation Authorisation Form is in Appendix A.

b. **Targeted Data** – Data acquisition relating to specific targeted individuals or organisations is subject to operational procedures (Previous SIS policy guidance Chapters 1, 4, 28, 29 and 30). Where data is exploited systematically using SIS's data exploitation tools, it should be managed in accordance with the DPA principles, responsibility lying with the desk officer who acquired it (the Data Owner). Processes are specific to the data exploitation system used but must reflect these principles.

c. **Traditional Information** – Procedures governing traditional information acquisition are covered in previous SIS policy guidance Chapters 2, 3, 17, 18 and 19. The appropriate section is responsible for policy and procedures on data management for Traditional Information.

9. By its nature bulk data does not lend itself to compartmentalisation. The Service meets its legal obligations by other measures to ensure that data access and the use of exploitation tools are subject to management control and oversight. These include:

a. structuring data in such a way that identities are only revealed by specific searches, rather than browsing;
b. applying an audit trail to the use of bulk data tools (reinforced by a log-on message, highlighting the active monitoring and auditing of the system and users' obligations);
c. restricting access to data exploitation systems to those with a business need to search and access bulk data;

d. pre-use training to ensure that all users of data exploitation systems understand the need to search for and access bulk data only when necessary and proportionate;
e. pre-use requirement for all users to agree to and act in accordance with data exploitation system Security Operating Procedures (SOPs) and usage policy;
f. requirement for each data set to have a data owner, responsible for ensuring that information (including intelligence reporting and data sharing) is transformed and exploited appropriately (see paras 11-19)
g. biannual review of bulk data sets, including utility, necessity, proportionality and sensitivity, leading to the removal and destruction of data as appropriate (see para 20);
h. backing up of datasets, to ensure integrity, and destruction or secure retention of original media (see para 24)

DATA ACQUISITION

10. [redacted]. Teams are advised to co-ordinate acquisition with the relevant team, who can also advise on best practice. Data can also be obtained from GCHQ and BSS through the appropriate process.

DATA TRANSFORMATION

11. Acquired data needs to be evaluated, transformed and loaded into the appropriate security-approved exploitation system (e.g. the database). This is initiated as part of the Data Acquisition/Transformation Authorisation Form workflow. Each dataset should have a file reference (the one used for the data acquisition or a separate one for the exploitation of data from a particularly sensitive operation). This reference should also be used for substantive reporting of intelligence derived from exploitation.

12. Each dataset must have a designated Data Owner, usually the officer who acquired it. The Data Owner is responsible for ensuring that data is transformed and exploited appropriately, and will be advised and supported by a data specialist. Unless the acquisition was the subject of a submission (in which case it is necessary only to quote the submission reference), the Data Owner must record within the Data Acquisition/Transformation Authorisation Form workflow the justification for exploiting the data, in terms of operational necessity and proportionality. The dataset must have a declared shelf-life, which can be extended against a valid and auditable justification.

EXPLOITATION AND REPORTING

13. Once data has been transformed and is exploitable, the Data Owner is responsible for Action On (but may delegate this). Guidelines are available on the database.

14. Information derived from data exploitation may be shared with other UK intelligence agencies, subject to appropriate source protection and handling caveats. Before passing data to a third party, staff must consult the Data Owner for Action On approval and an appropriate form of words – some data acquisition is sensitive and its source may need to be disguised.

15. To help justify the acquisition, exploitation and continued retention of individual sets of bulk data, the relevant team need to know any outcomes (eg new information

on a target, other operation benefits or any lessons learned) from using the data. For this reason the database users are asked to add a reference to any such outcomes to the system 'hits' file [redacted]. Particularly for sensitive cases, it is not necessary to include operational detail (although users will wish to know that access to the file is very restricted); but where operational security permits, copying a document to the file is the quickest way to do this. Where relevant, users should also add the reference to the SIS records system.

DATA SHARING

16. Bulk data is shared between SIS, GCHQ and BSS through the relevant process, managed by the appropriate team. This records what has been shared, covers the legal and policy basis for sharing and ensures that there are appropriate security controls. Sharing with UK agencies outside the relevant process requires Data Owners to be satisfied that these conditions have been met. In summary: an audit trail needs to be kept of data shared; sharing should serve a justifiable purpose and be proportionate to it; and the data must be securely held. The appropriate team, legal advisors and security officers can advise. Data must not be shared without the Data Owner's authorisation.

17. Bulk data can be shared with other third parties (eg a liaison partner) with the Data Owner's permission and subject to certain assurances. Were there to be such sharing, the assurances would require a liaison to handle the data securely, not to share it further without permission, and to share, as far as is practicable, results that have an impact on UK National Security.

18. Were data to be acquired from joint operations with partners (e.g.GCHQ/SIS operations), that data may be shared by the partner organisation without additional written legal assurances from SIS. Those parties involved are deemed to have jointly acquired the data and are both regarded as the data owner. Good practice requires that reliable records are kept on what data has been sent where.

19. Subject to these authorisations, the Data Transformation team will copy the data but it is the duty of the officer sharing the data to ensure that it is securely transferred. Security team guidance should be followed (see para 26).

DATA RETENTION REVIEW

20. To comply with legal obligations, a senior SIS officer is responsible for ensuring that bulk datasets on the database are reviewed every six months. The review body should include a senior SIS officer, a Legal Advisor [redacted] and a member of the relevant team. External attendees may be invited on an ad hoc basis at SIS discretion. Data is reviewed, against set criteria and assessments of both its intrusiveness and sensitivity, to ensure that:

(a) Data was acquired in lawful exercise of an SIS function;

(b) Each dataset is up to date for the purposes of exploitation, and does not comprise redundant or inaccurate data;

(c) Based on necessity and proportionality, and taking into account its utility, data needs to be retained (on the database or in storage) or destroyed.

21. The review mechanism will articulate the reason for each decision and its compliance with UK law. Data Owners will be consulted before any changes are made.

22. Some datasets may be unique (e.g. if repeat access is not guaranteed) but become obsolete or of little worth. However, if it is likely that they may be of future use, data can be retained off the database in storage. If a dataset has been completely replaced by a newer version, the older version will be destroyed.

DATA SECURITY AND MEDIA STORAGE

23. The database is accredited to TOP SECRET STRAP 2 UK EYES ONLY.

24. [redacted]

25. [redacted]

26. SIS have a duty to ensure the security of all data, whatever and wherever its origins. The officer(s) collecting or acquiring the data is responsible for ensuring that the relevant security team guidance is followed.