2. EXTRA-STATUTORY FUNCTIONS

Under paragraph 59A of RIPA, inserted by the Justice and Security Act, the Prime Minister may direct me to keep under review the carrying out of any aspect of the functions of the intelligence services. I have requested that such directions are given in relation to my extra-statutory functions, but until they are, I will continue to provide oversight on an extra-statutory basis.

In my open report I have set out my statutory functions and one of my extra-statutory functions relating to the Consolidated Guidance to Intelligence Officer and Service Personnel on Detention and Interviewing Detainees and on Passing and Receipt of Intelligence Relating to Detainees (Consolidated Guidance).

In addition to this I have been asked to oversee certain other matters and report in the Confidential Annex on the same:

2.1 Bulk Personal Data

In 2010, my predecessor agreed to provide independent oversight of the intelligence services' holding and use of bulk personal data which is not already overseen by the Interception of Communications Commissioner and to report on the same in the Confidential Annex. I have developed, with the intelligence services, a system under which I am informed of all bulk personal data sets held and of the steps taken to ensure proper and proportionate use of the same. I have also made it known that in my view it would be preferable if this aspect could be reported openly and a direction given under section 59A.

2.2 Section 94

Additionally to my oversight of Bulk Personal Data, GCHQ asked my predecessor to oversee the activity of GCHQ in relation to data acquired by means of directions given by the Secretary of State under section 94 of the Telecommunications Act 1984. Such oversight will be reported whether directions are openly given, or whether directions are not given openly. I have continued to inspect these directions following a similar approach.

When I appeared before the Home Affairs Select Committee on 18th March 2014, I was asked what oversight there was as to how s94 of the Telecommunications Act is used. I explained that there was no statutory oversight but how the new legislation provided me with additional functions if directed and it would seem to me that this is an example of where it would be appropriate for me to write and suggest that I be formally directed to keep this under review.

2.4 Justice and Security Act

As I said in my open Report, my extra-statutory roles could be placed on a statutory footing through a direction from the Prime Minister.

The Prime Minister must publish such directions "except so far as it appears to the Prime Minister that such would be contrary to the public interest or prejudicial to:

- National Security,
- The prevention or detection of serious crime,
- The economic well-being of the United Kingdom, or
- The continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Intelligence Services Commissioner."

I would like to discuss further what directions should be given and how much should be made public. I would prefer my oversight in relation to bulk data and its use to be made public and [redacted] It may be possible to make public that an oversight of the Secretary of State's powers to give directions under section 94 exists but it is difficult to see how any report could be made in an open Annual Report. [redacted]

8. BULK PERSONAL DATA

On 14 October 2010, the Prime Minister wrote to my predecessor, Sir Peter Gibson, requesting that Sir Peter report to him, the Home Secretary (in relation to the Security Service) and the Foreign Secretary (in relation to SIS and GCHQ) on the adequacy of policies and procedures in the agencies, and on a proposed framework for ongoing oversight by the Commissioner on an extra-statutory basis, in respect of the acquisition, retention and deletion of bulk personal data holdings and in respect of the access to and use of such data.

Sir Peter Gibson reported "In my opinion such a regime will be an effective way of providing independent oversight of the agencies' holding and use of bulk personal data which is not already overseen by the Interception of Communications Commissioner. In the case of GCHQ, the Commissioner will adopt a similar approach in respect of data acquired by means of Directions issued under Section 94 of the Telecommunications Act 1984."

My oversight of Bulk Personal Data (Bulk Data) takes place in a number of ways.

- Firstly I require the services to provide me with a list of all data sets held. What I am concerned to do is to assess whether the test of the necessity and proportionality of acquiring and retaining the data sets has been properly applied in relation to decisions to acquire, retain or delete those data sets. This is normally quite straight forward because each service has an internal review body which considers the retention of data sets on a regular basis and records the decision in writing. These documents are available for me to inspect.

- I then consider how operatives and which operatives gain access to the data sets and review how the necessity and proportionality (ie the justification) of that intrusion into private information is maintained.

- Finally I review the possible misuse of data and how this is prevented. I consider this to be the most important part of my oversight in that is seems to me that
  - It is critical that access to bulk data is properly controlled and
  - It is the risk that some individuals will misuse the powers of access to private data which must be most carefully guarded against.

8.1 Details of my Oversight of Bulk Personal Data

8.1.1 Security Service

Datasets held at the start of year:	[redacted]
Datasets acquired in year:	[redacted]
Datasets deleted in year:	[redacted]
Datasets held at the end of year:	[redacted]

On each occasion during 2013 I reviewed a summary of all datasets current and active plus documents recording decisions as to acquisition and retention. I did not find it necessary to identify particular data sets on which to ask questions. I was satisfied that MI5 had properly considered and justified the retention of the data sets.

The Security Service has a series of mitigations and safeguards to prevent the misuse of bulk personal data. The collection of bulk personal data is carefully managed, with appropriate security procedures to minimise the risk of data loss in transit, and access to data is limited to only individuals (vetted to DV) with a valid business requirement. Additionally, some bulk personal datasets are only made available to a limited number of analysts in relevant business areas. Some fields of data containing particularly sensitive personal data may be removed or suppressed from datasets, or require specific justification to be accessed. All staff who require access are trained on the use of relevant analytical techniques, and on the sensitivities around the use of Bulk Personal Data. They are also required to read and sign Security Operating Procedures to demonstrate they understand acceptable and unacceptable behaviours.

8.1.2 Secret Intelligence Service

The following figures have been derived from the [redacted] interactive reporting function. The following fields were used "Date Acquired", "Date Removed from [redacted]" and "Date Completely Deleted".

For the calendar year 2013:

Datasets held at start of year
Datasets acquired in year
Datasets deleted in year
Datasets held at end of year
[redacted]

SIS maintains a complete list of all bulk data holdings which is made available to me. There is a defined assessment and authorisation process to enable any data set to be exploited or retained. This approval is reviewed every 6 months, the usage of the data is assessed, and the necessity of the data re-evaluated. Data sets that no longer meet the requirements are removed from general access, and if they continue to provide no value are deleted entirely. The minutes and assessment results from the reviews are all made available to me during my visits.

I was satisfied in all instances that retention of the data sets retained was necessary and proportionate.

SIS place most of their bulk data sets on a system called [redacted] A limited number of analysts have access to [redacted] who will have been trained and signed a code of practice. They will then have a unique personal login. These analysts cannot search on any particular item of bulk data. All they can do is to interrogate the system eg by putting in a telephone number to see whether that will bring up other information.

There are then in addition a very limited number of analysts [redacted] who can do advanced searches ie search particular bulk data sets; they are again trained and carefully selected.

8.1.3 Government Communications Headquarters

Datasets held at the start year:
Datasets acquired in year:
Datasets deleted in year:
Datasets held at the end of year: [redacted]

GCHQ supply me with a complete list of the bulk personal data sets they hold. For those datasets I select for inspection they also supply me with copies of the minutes recording the justification for acquisition and the associated retention reviews which they carry out on a regular basis. I am satisfied GCHQ can justify retention of the data sets held by them.

GCHQ again have systems under which much of this bulk data cannot be trawled through by analysts indiscriminately. The systems limit analysts to putting in a specific search term such as a number and the system searches over those of the bulk data sets to which the analyst has access – not all datasets are accessible to every analyst. A search cannot be run without the entry into the system of a justification that sets out the necessity and proportionality of the action.

There are at GCHQ, as at SIS, a limited number of persons, again carefully selected who can perform more detailed searches by reference to particular data sets but again justification must be entered before a search can commence.

8.2 Statistics

In summary the data sets held by the intelligence services containing bulk personal data in 2013 are:

	SIS	MI5	GCHQ	Total
Held at the start of the year[3]	[redacted]	[redacted]	[redacted]	[redacted]
Acquired in year[4]	[redacted]	[redacted]	[redacted]	[redacted]
Deleted in year	[redacted]	[redacted]	[redacted]	[redacted]
Held at the end of the year	[redacted]	[redacted]	[redacted]	[redacted]

[3] Some data sets will be held by more than one of the intelligence services
[4] Some data sets will be acquired from another of the intelligence services

9.2 Secret Intelligence Service

Proactive auditing of SIS bulk data stores commenced in September 2011, with users asked to formally justify particular queries on the bulk data applications. A total of 1067 justifications requests have been issued up until end March 2014.

	Total Justification Requests Issued	Targeted Justification Requests	Random Justification Requests	Disciplinary	Serious Breach	Moderate Breach	Minor Breach
FY 11/12 *(commenced Sept 2011)*	[redacted]	[redacted]	[redacted]	2	0	1	1
FY 12/13	[redacted]	[redacted]	[redacted]	0	3	0	1
FY 13/14	[redacted]	[redacted]	[redacted]	0	4	1	3
Total	[redacted]	[redacted]	[redacted]	2	7	2	5

The increase in justification requests over the years reflects changes in detection methods and an increase in the number of random query justifications issued (as a deterrent against misuse). In response to my advice, technical modifications were made to the application to enable an increase [redacted]

Some query justification requests require further additional detail from users e.g. a document reference, operational context. No statistics are recorded for these instances.

Of the [redacted] justification requests, 2 resulted in disciplinary referral or equivalent and 14 in the issue of security breaches (7 serious). A summary of each is in the chart below but I have been given full details during my Inspection.

9.2.1 DISCIPLINARY CASES

1	Oct 2011	A contractor in the bulk data ingestion team was detected performing a query on a member of Service staff. Unable to provide an appropriate explanation, further investigation established that the contractor had performed repeated, unnecessary queries with no justifiable business reason. Their contract was terminated and they were walked off the premises. Their security clearance was subsequently revoked.
2	Dec 2011	A user was detected performing a query on a member of staff and their own family name. The response to the justification request raised some concerns and further investigation identified additional unnecessary queries with no justifiable business reason. The individual was referred to the Service's Disciplinary process, where

		the panel determined the incident to be gross misconduct. A final written warning was issued.

9.2.3 SECURITY BREACHES

	Detail	Assessment
	SERIOUS BREACHES	
1	Search on family member when refreshing understanding of the application.	No operational requirement for the information. No further unnecessary queries identified.
2	Search on family member when demonstrating application capabilities to a new user.	No operational requirement for the information. No further unnecessary queries identified.
3	Search on family member when refreshing understanding of the application.	No operational requirement for the information. No further unnecessary queries identified.
4	Search on ex Agent ([redacted] to demonstrate application capabilities to a colleague.	No operational requirement for the information at that time. No further unnecessary queries identified.
5	Search on staff details for a pass application.	No operational requirement for the information. Bulk data is not an administrative support tool and the information can be obtained via less intrusive sources. No further unnecessary queries identified.
6	Search on a telephone number to identify source of a 'missed call'.	No operational requirement for the information; bulk data stores are not provided as an administrative support tool. No further unnecessary queries identified.
7	Self search when refreshing understanding of the application, in preparation for training new users.	No operational requirement for the information; training scripts already exist. No further unnecessary queries identified.
	MODERATE BREACHES	
8	Search to identify colleague telephone number (for welfare contact) and passport number (operational flight booking).	General Business requirement for the information, but information can be obtained by less intrusive methods.
9	Search on family member to identify bio details for Security Tracing Purposes.	General Business requirement for the information, but information can be obtained by less intrusive methods.
	MINOR BREACHES	
10	Search on family member to	Operational requirement for the

	Detail	Assessment
	identify bio details for a diplomatic visa application.	information, but information can be obtained by less intrusive methods.
11	Failure to demonstrate specific operational requirement for search.	Associated paperwork suggests operationally related, user made substantial efforts to identify appropriate reference, but no definitive justification.
12	Search on family member to identify bio details for a diplomatic passport application.	Operational requirement for the information, but information can be obtained by less intrusive methods.
13	Search to identify colleague's passport information for urgent flight booking.	Operational requirement for the information, but query was too broad with non proportionate intrusion on staff family.
14	Search on family member to identify bio details for a diplomatic visa application.	Operational requirement for the information, but information can be obtained by less intrusive methods.

9.3 Government Communications Headquarters

Bulk personal data comprises only a small proportion of the operational data held by GCHQ and is often held in databases alongside data from other sources. Access to these databases is restricted to individuals that have demonstrated an operational requirement to use the data. GCHQ therefore uses the same methods to manage and protectively monitor access to its bulk personal data as those applied to all of its operational data with increasingly sophisticated computer monitoring providing tip-offs for investigation(for example to detect self-referential searches) . It continues to seek ever better means of detecting potential instances of abusive access to operational data. New technical ideas are tried and tested (and sometimes discarded). The internal processes and linkages between the various areas of the Department – IT Services, Mission Policy, Security and HR – that work closely together to deliver this monitoring and investigation are constantly reviewed and refined.

Upon completion of an investigation, an incident is assessed for its actual or potential damage or level of non-compliance, together with the degree of culpability and/or negligence in evidence on the part of those involved. Incidents are categorised as either Minor or Major and in both cases there are consequences for those involved. The incident is recorded on their personnel security file and they and at least their line manager are notified accordingly. Incidents recorded against an individual in this way contribute towards their overall security profile, can affect their suitability for certain posts, and may lead to formal disciplinary proceedings.

The way that bulk personal data is stored in GCHQ and the way that GCHQ IT systems record security incidents means I have been told that it is very difficult and