E2

[redacted]

Report of the Intelligence Services Commissioner for 2014

CONFIDENTIAL ANNEX

The Rt Hon Sir Mark Waller

June 2015

Excluded from publication under section 60(5) of the Regulation of Investigatory Powers Act 2000

[redacted]

[redacted]

2. ADDITIONAL 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.

The Prime Minister has now issued three such directions placing all of my oversight on a statutory footing. Two of the directions are set out in my open report:

- the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets including the misuse of data and how this is prevented
- compliance with the Consolidated Guidance..

[redacted]

[redacted]

Section 94

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. During 2014 I continued to oversee GCHQ's use of section 94 directions in a similar way to my oversight of bulk personal data. However, in January 2015 the Interception of Communications Commissioner was asked and has agreed to formally oversee directions under section 94.

[redacted]

[redacted]

8. BULK PERSONAL DATA

On 12 March 2014 the Prime Minister published a direction which put my continued oversight of bulk personal data on a statutory footing.

On 14 October 2010, the Prime Minister wrote to my predecessor, Sir Peter Gibson, setting out 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.

I have set out my oversight of bulk personal data in as much detail as I can in my open report this year.

Statistics

Bulk Personal Datasets	SIS	MI5	GCHQ	Total
Held at the start of 2014	[redacted]	[redacted]	[redacted]	[redacted]
Acquired in year:	[redacted]	[redacted]	[redacted]	[redacted]
Deleted in year	[redacted]	[redacted]	[redacted]	[redacted]
Held at the end of year	[redacted]	[redacted]	[redacted]	[redacted]

Details of my Oversight of Bulk Personal Data

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]

MI5 provided me with a summary of how each of the datasets are used. I had no difficulty with the justification for retention of datasets so I have concentrated on the use of the data.

[redacted]

The Security Service have access to data sets through:

[redacted]

Access is also limited by post so when an officer changes role their access to datasets is likely to change as well.

[redacted] indicate which system(s) they wish to search. RIPA product is also on this system. [redacted] does not supply all information at once so the analyst has to consider if further information is needed. They do not have a justification box or field to complete before they undertake a search of [redacted] but prior to being granted access to the system they must undergo training and they are expected adhere to the code of practice. Individual analysts will record the necessity and proportionality given to them by the investigator. The Security Service relies on the integrity of their staff. MI5 has also a strong monitoring system.

[redacted]

Secret Intelligence Service

For the calendar year 2014:

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

Within SIS most bulk personal data sets are available to users through a system called [redacted]. A few datasets are stored on standalone systems and not available to [redacted] users but can be searched separately. Each data set is authorised separately before input onto [redacted]

[redacted]SIS staff have access to [redacted]

[redacted]

[redacted]

The training explains that users have personal responsibility for any search undertaken. Managers are responsible for ensuring that staff read and sign the code of conduct. This explains that BPD needs to be managed to ensure that the privacy of those whose data is held is respected and that data is held, accessed and disclosed only to the extent necessary for the purpose of the statutory functions and proportionate to those aims.

When undertaking a search SIS must now complete mandatory fields setting out:

- Purpose of the search
- Justification (business need relating back to an intelligence report, sigint etc)
- Free text box

[redacted]

I asked if the justification box required consideration of proportionality. SIS explained that the box has a limited word count (300 characters) but staff are expected to give the operational context and the [redacted] team review what is written. Users also have to comply with the code of practice which explains that users have a responsibility to ensure enquiries are necessary and proportionate.

I enquired if the justification box could be changed – to include a human rights justification setting out if the invasion of privacy is justified. In my view the "justification" box did not accurately reflect the way in which SIS often ensure that intrusion into privacy is justified. That assessment is often done prior to an analyst actually conducting a search. Thus this box needs to reflect either that the analyst is satisfied the assessment has been made or that he ir she has done the assessment themselves.

[redacted]

This muster has highlighted a weakness in the system by which they tracked media around the office and then destroyed it. Also the culture around the handling of classified media was not as strong as it should have been. As a consequence SIS were not able to account for all media in the service. Of the 2730 recorded items in their bulk data registrar, 367 are unaccounted for.[1] [redacted]

[1] SIS wish to make it clear that since this report, enquiries were conducted in respect of the 367 items referred to. The conclusion of those enquiries was that it was likely that the 367 items had been deleted. Furthermore, it became clear that not all the items were BPD. Some items were not BPD but other items of media held by the BPD team.

[redacted]

[redacted]

[redacted]

[redacted]

At the Inspection SIS said that they strongly believe that this missing data is not down to malicious theft – there has been no leak to the media for example. A full search of media is underway with amnesty for any found and registered now.[1]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[1] SIS wish to make it clear that since this report, enquiries were conducted in respect of the 367 items referred to. The conclusion of those enquiries was that it was likely that the 367 items had been deleted. Furthermore, it became clear that not all the items were BPD. Some items were not BPD but other items of media held by the BPD team.

Since this muster SIS have put into place a tracking system with one officer as single point of contact [redacted]

- **Unexploited Datasets**

I asked SIS to chart any datasets acquired but not currently available for exploitation and was provided with two lists which showed that there were:

- [redacted] existing datasets which were also in this category six months ago
- [redacted] datasets which were not in this category at the previous inspection (new acquisitions)

The [redacted] older datasets should all have written justification from a senior officer or legal adviser while they are waiting to be authorised for exploitation into [redacted]. However, SIS could not find authorisations in the permanent record for [redacted] of these datasets and were taking immediate action to rectify this.

I expressed concern that there were [redacted] old and unexploited datasets; some dating back to 2005 and advised that SIS could not justify the necessity for retaining datasets if they have not been exploited within three years. SIS explained that one dataset was retained [redacted] which I accepted as a valid reason.

SIS have set up a project to deal with the old datasets and are aiming

- To authorise any dataset over 12 months for exploitation by May 2015
- To authorise any dataset over 6 months for exploitation by Nov 2015

All unauthorised datasets after this period will be deleted by the Data Review Panel unless an exceptional case for necessity is made. I instructed them to be ruthless in deleting old datasets

SIS agreed to revert to the relevant teams to make their case for retaining the datasets. If they want to retain the older dataset then they will have to prioritise this over newly acquired datasets. In future the relevant business area will take ownership of the datasets and provide the justifications.

SIS consider there to be three main causes for the delay in exploiting or deleting datasets:

1. Difficulties in accessing the data or difficulties in assessing the content of the data.[redacted]
2. The technical complexities for some datasets can cause delays in transforming them into a format that permits exploitation.
3. Delays in the authorisation process which requires six people to approve it.Of the [redacted] datasets, [redacted] fall within this category which may also have been caused by problems in the corporate IT system.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]