Inspections under Section 94 Telecommunications Act 1984 by the Interception of Communications Commissioner's Office (IOCCO)

Gists are shown in italics and are double-underlined

Name of Public Authority	The Government Communications Headquarters (GCHQ)
Date/s of Inspection	25-26 April 2017
Inspector/s	[REDACTED]

Background to the Inspection: The Interception of Communications Commissioner's Office (IOCCO) is charged with undertaking inspections on behalf of the Interception of Communications Commissioner ("the Commissioner").

IOCCO now undertakes a revolving programme of inspection visits to Mi5 and GCHQ who are authorised to acquire communications data under Chapter 2 of Part I of the Regulation of Investigatory Powers Act (RIPA) and Section 94 of the Telecommunications Act 1984, and produce a written report of the findings for the Commissioner.

In October 2015 IOCCO started its first review of directions issued under section 94 of the Telecommunications Act 1984. The purpose of the review was to identify the extent to which the intelligence agencies use section 94 directions, to assess what a comprehensive oversight and audit function of section 94 directions would look like and to assess whether the systems and procedures in place for section 94 directions are sufficient to comply with the legislation and any relevant policies.

On the 4th November 2015 the agencies published their handling arrangements under section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 ("the handling arrangements") where the section 94 directions relate to the acquisition of bulk communications data (BCD).

Our review report of directions issued under section 94 of the Telecommunications Act 1984 was published on 7 July 2016 ("the review report") and explains the scope of our oversight function.

The primary objectives of the inspection are to:

- Ensure that the system in place for acquiring communications data is sufficient for the purposes of RIPA and the handling arrangements for the acquisition of BCD ("the BCD handling arrangements") and that all relevant records have been kept.
- Ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act, RIPA and its associated Code of Practice (CoP) and the BCD handling arrangements.
- Ensure that the data acquired was necessary and proportionate to the conduct authorised.
- Examine what use has been made of the communications data acquired.
- Ensure that errors are being 'reported' or 'recorded' and that the systems are reviewed and adapted in the light of any exposed weaknesses or faults.

- Ensure that persons engaged in the acquisition of data are adequately trained and are aware of the relevant parts of the legislation.

Statistics:

Number of section 94 directions given by SofS for **BCD**; since January 2016:	**[REDACTED]**
Number of items of **BCD** accessed during 2016:	**[REDACTED]**
Number of intelligence reports produced between 01/01/2016 to 31/07/2016 from accessing **BCD**:	**[REDACTED]**

Staffing:

Senior Responsible Officer (SRO)	[REDACTED] (Deputy Director)
Other staff met during the inspection	[REDACTED] (Head of Warrantry) [REDACTED] (Joint Head of Warrantry & oversight team) [REDACTED] (Policy advisor (RIPA Warrantry)) [REDACTED] Ops Manager [REDACTED] (Internal Audit) [REDACTED] (Internal Audit) Analysts [REDACTED]

Summary of Inspection Findings:

GCHQ emerged very well from this **first** inspection by IOCCO regarding the acquisition of bulk communications data. It was clear that the standards highlighted in review report of section 94 directions had been maintained. The inspectors were satisfied that GCHQ is acquiring bulk communications data lawfully within the permissible parameters of the Telecommunications Act 1984 and for the correct statutory purpose.

A high standard of applications are produced for submission to the Foreign Secretary. GCHQ has taken full account of the recommendations in the IOCCO review report and integrated them into their processes.

The inspection findings are outlined in more detail in the following sections of the report. A number of recommendations have been made for GCHQ to work with IOCCO to explore how GCHQ's development tools and internal audit systems could be modified to enable IOCCO to undertake a more thorough inspection and audit. This would make it easier to assess what BCD has been accessed and the justifications as to why it was necessary and proportionate. This would enhance the oversight given by the Commissioner and his inspectors and would enhance GCHQ's internal audits.

The existence of the published handling arrangements acknowledges the potential for sharing with a partner agency outside of the United Kingdom which will attract questions about what is done with the data, who has access to it (for example, further dissemination by the partner agency to a 3rd party outside their or United Kingdom jurisdiction) and the security safeguards that have been put in place.

[REDACTION]

Recommendations are shown in the last column of the inspection tables. Please note that recommendations are shaded red, amber or green. IOCCO have adopted this practice to enable public authorities to prioritise the areas where remedial action is necessary. The red areas are of immediate concern as they mainly involve potentially serious breaches and / or non-compliance with RIPA, the CoP or the BCD handling arrangements which either are unlawful or could leave the

public authority vulnerable to legal challenge. The amber areas represent non-compliance to a lesser extent. Remedial action must still be taken in these areas as they could potentially lead to breaches.

Summary of Recommendations: Red - 0; Amber - 2; Green - 0.

Areas Inspected:

1. S.94 directions given by Secretary of State

Section 94 Direction given by Secretary of State to acquire BCD from PECNs			
Each time a section 94 direction is given by a Secretary of State it must be notified to the Commissioner by the agency. In order to enable a reverse audit to be conducted each time a section 94 direction is served on a PECN, the PECN must report the details of that direction to the Commissioner. Review report of section 94 directions – recommendations.	**Yes**	A process is now in place which allows for the secure electronic transfer of copies to our office, from Security Service and GCHQ, of section 94 directions given by a Secretary of State. Since February 2016 GCHQ have made copies available to IOCCO when a section 94 direction has been given by Foreign Secretary. The [REDACT] section 94 directions undertaken in October 2016, that replaced or updated previous directions, were made available for inspection.	
All section 94 directions should indicate the specific communications data that is required to be disclosed by the PECN. When a requirement is amended (i.e. modified) a new direction should be given. Review report of section 94 directions – recommendations.	**Yes**	The [REDACT] extant section 94 directions were examined by the IOCCO inspectors - each made explicit the specific communications data required to be disclosed by the PECN.	
There should be a clear application process for requests for BCD which sets out the requirements to be met. The agencies (in conjunction with the Home Office and Foreign Office) should develop a specimen application form and a specimen section 94 direction in order to ensure a standard and consistent approach. Review report of section 94 directions – recommendations.	**Yes**	In the absence of any codified procedures in or made pursuant to section 94 of the Telecommunications Act 1984, the intelligence agencies developed a process to facilitate the acquisition of BCD and to review and provide operational updates in relation to the use of section 94 directions for bulk communications data. That process is set out in the handling arrangements published by the agencies in November 2015. The process can be broken down into four distinct areas, some of which may be undertaken simultaneously: a) The agency identifies and describes the BCD considered	

		necessary to meet its operational objectives; b) The agency identifies the relevant PECN(s) and consults to assess whether the acquisition of specific communications data in bulk from a PECN is reasonably practical or whether the specific data required is inextricably linked to other data; c) The agency consults further with the PECN and assesses whether the data can be made available by means of a section 94 direction; and d) The agency determines whether the bulk acquisition of communications data is appropriate under a section 94 direction and, if so, prepares a detailed submission for consideration by the Secretary of State. The submissions to the Foreign Secretary were highly detailed, made explicit why the acquisition of BCD was required in the interests of national security, and the intelligence requirement or gap they were seeking to address. The submissions provided extensive detail as to how the BCD would address the operational requirement, the expected value of the intelligence to derive from the BCD, and why there was no appropriate or suitable alternative to the proposed conduct under the section 94 direction. A refined application process has been developed and takes account of the requirements of the Investigatory Powers Act 2016. Each of the submissions outlined reasons why the Foreign Secretary might decide not to lay the particular section 94 direction in Parliament because disclosure was determined to be against the interests of national security. There were also issues highlighted in relation to how disclosure might damage the standing of the PECN involved. The submissions also	

		contained an assessment of the risks that would need addressing if disclosure was undertaken. As a consequence, none of the extant section 94 directions had been laid in Parliament due to the secrecy provisions relating to national security.	
Where a PECN changes its company name or merges with another PECN, any section 94 direction should be amended to reflect the position. Review report of section 94 directions – recommendations.	**Yes**	GCHQ have historically taken the approach to undertake new section 94 directions where a PECN changes its company name or merges with another PECN. The IOCCO inspectors confirmed all the extant section 94 directions take account of this on-going consideration.	
There should be a clear process for the review, cancellation or modification of any section 94 directions for BCD. The agencies (in conjunction with the Home Office and Foreign Office) should develop specimen review, cancellation and modification templates to ensure a standard and consistent approach. Review report of section 94 directions – recommendations.	**Yes**	GCHQ undertake reviews every 6 months as to whether the acquisition of BCD remains necessary and proportionate. The reviews were examined and are detailed and give updated outcomes. Either way, the review and its recommendation to keep the direction in place, modify or cease its use is submitted to the Foreign Secretary. The reviews are conducted in three parts: • an audit of all current Directions; • a quantitative assessment of the contribution to GCHQ operations of the data provided under these Directions; • a qualitative check on the value from data sources for which traceability to GCHQ outcomes is more difficult. The last completed review covered the period 01/01/2016 to 31/07/2016. During that period, GCHQ issued at least [REDACT] reports containing data provided under section 94 directions by at least one PECN. Over [REDACT] items of data provided by PECNs were used in those reports. In April 2017 GCHQ undertook a review and submission to the Foreign Secretary concerning their collection of BCD under several existing section 94 directions. [REDACTED].	

		The Foreign Secretary confirmed he was content that GCHQ continue to access this data within the BCD data sets.	

2. Access to BCD

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
Random Sampling and/or Sampling from Query Based Searches			
The IOCCO inspectors will examine a random sample of applications and/or where an application workflow system is in operation the IOCCO inspectors will seek to run query based searches to identify the applications to be examined. The query based searches that were conducted will be described against the relevant baseline. The objective of this part of the inspection is twofold. First, it is to ensure that the overall system in place for accessing BCD is sufficient for the purposes of the BCD handling arrangements. Second, the IOCCO inspectors will be seeking to ensure that the individual requests for communications data were necessary and proportionate to the task in hand. See also and para 4.1.3, 4.1.4 and 4.3.3 (2nd indentation) of BCD handling arrangements.	**Yes**	The IOCCO inspectors interviewed those in charge of intelligence operations, those senior managers facilitating access, analysts within operational teams and those who manage and undertake audits of the access. Within GCHQ, all operational data gathered from a variety of different sources is treated in the same manner. Where there is an operational requirement to gain access to operational data (which will include BCD), an *analyst* is required to justify why the access and examination of the data are necessary and proportionate. This is a three-stage process covering: • why the search is necessary for one of the authorised purposes, for example, *"in the interests of national security"*; • an internal cross-reference number which equates to the specific intelligence requirement and priority for the search. [REDACTED] • a justification of the necessity and proportionality to access the data. GCHQ undertakes robust retrospective audit checks. The senior managers interviewed by the IOCCO inspectors as part of our inspection explained and demonstrated in detail how the audit processes work and the function of GCHQ's Internal Compliance Team who carry out *ex-post facto* random audit	**1.**

		checks of the analysts' justifications for the selection of BCD. In addition, GCHQ's IT Security Team conducts technical audits to identify and further investigate any possible unauthorised use. However, the two internal audits do not have access to the full detail of the ECHR justifications completed by the analyst and the data they sought access to. During 2016 [REDACTED] items of BCD accessed were included within [REDACTED] intelligence reports. The IOCCO inspectors were particularly impressed with the work undertaken by GCHQ to improve and develop the [REDACTED] system. The inspectors met with Analyst [REDACTED]. They concluded there is an opportunity to undertake development that would benefit GCHQ's internal compliance / audit processes and assist IOCCO and the Commissioner in their oversight inspections. **It is recommended GCHQ work with IOCCO to explore how GCHQ's development tools and current audit systems may be modified to enable a more thorough inspection and audit to be undertaken by IOCCO. In particular, to assess what BCD was accessed and the justifications as to why it was necessary and proportionate. Such a development will enhance the oversight given by the Commissioner.**	
Retention and security of BCD			
Access to BCD must be strictly limited with the following protective security measures: • Physical security to protect any premises where the information may be accessed; • IT security to minimise the risk of unauthorised access to IT systems; • A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.	**Yes**	The IOCCO review report of directions given under section 94 of the Telecommunications Act 1984 describes (paras 8.54 to 8.57) our findings in relation to this baseline which is based on the handling arrangements published in November 2015. Each of these elements was discussed and the arrangements remain current.	

See BCD handling arrangements.			
Disclosure of BCD in its entirety or as a subset outside of the intelligence services may only be authorised by a senior official (for example, the equivalent of a senior civil servant) or the Secretary of State (for example, Foreign Secretary). The sharing of BCD in its entirety or as a subset outside of the intelligence services does not include instances when information is included in an intelligence report i.e. the information does not give itself away as being derived directly from a section 94 direction or the handling arrangements associated to it. See paragraphs 4.4.1 to 4.4.6 of the handling arrangements.	**Yes**	[REDACTED]	**2.**
Destruction of BCD.	**Yes**	GCHQ's policy is to retain BCD within its systems for a maximum of 1 year. [REDACTION] The BCD is subject to automated deletion in line with the retention policy which occurs on a daily basis.	

3. Communications Data Involving Certain Professions

Special consideration must be given to the degree of interference with an individual's rights and freedoms where the data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information. In cases where communications data is sought to determine a journalist's source judicial approval must be obtained.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
The degree of interference with an individual's rights and freedoms may be higher where the data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist. (Para 3.73 CoP Chapter 2 Part 1 RIPA and para 4.3.3 (4th indentation) of BCD handling arrangements). Such situations do not preclude an application being made. However, applicants, giving special consideration to necessity and proportionality, must	**Yes**	The inspectors examined instances recorded within the system relating to data acquired in relation to sensitive professions [REDACTED]	

draw attention to any such circumstances that might lead to an usual degree of intrusion of infringement of rights and freedoms. Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions. Particular care must be taken by DPs when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application. (Para 3.74 CoP Chapter 2 Part 1 RIPA and para 4.3.3 (5th and 6th indentations) of BCD handling arrangements). That such an application has been made must be recorded and such applications should be flagged to the Commissioner during inspections. (Para 3.75 CoP).			
Issues surrounding the infringement of right to freedom of expression may arise where a request is made for the communications data of a journalist. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Where an application is intended to determine the source of journalistic information, there must therefore be an overriding requirement in the public interest and the applicant must consider properly whether the conduct is criminal and of a sufficiently serious nature for rights to freedom of expression to be interfered with. In cases where the data is required to determine the source of journalistic information a judicial process must be followed (see the guidance at Paragraphs 3.78 to 3.84 of the CoP Chapter 2 Part 1 RIPA) unless there is believed to be an immediate threat of loss of human life. See also and para 4.3.3 (7th indentation) of BCD handling arrangements. Where the application is for communications data of a journalist, but is not intended to determine the source of journalistic information (for example, where the journalist is a victim of crime or is suspected of committing a crime	**Yes**	[REDACTED]	

unrelated to their occupation), an application under RIPA may be justified. Particular care must be taken to ensure that the intrusion is justified in such cases. (Paragraphs 3.77, 3.84 CoP Chapter 2 Part 1 RIPA and para 4.3.3 (5th and 6th indentations) of BCD handling arrangements).			

4. Training and guidance

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
Users must be trained on their professional and legal responsibilities, and refresher training and/or updated must be provided when systems or policies are updated. Para 4.3.3 (8th indentations) of BCD handling arrangements).	Yes	The arrangements made to internally train staff were to standard: • Any analyst wishing access to any operational data must take training in UK legalities and pass a test every 2 years. • Databases apply access controls. Analysts only gain access to tools they need. • All databases have an agreed data retention limit in accordance with GCHQ's Data Retention Policy.	
Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution. Para 4.3.3 (11th indentations) of BCD handling arrangements).	Yes	On logging on to a database analysts are presented with a reminder of their HRA responsibilities and the consequences of unauthorised access and use.	

Keeping of Records

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
Records to be kept			
Applications, section 94 directions, copies of directions, reviews and related briefings to the Secretary of State, must be retained by the intelligence agency in written or electronic form.	Yes	Printed signed copies of section 94 directions, reviews and related briefings were retained in a series of folders. All [REDACTED] of the current sections 94 directions were present for examination.	
The agencies must keep a central record of all section 94 directions that relate to their organisations. The central record must include the date the direction was given; the name of the Secretary of State giving the direction; the PECN the direction relates to and the date the direction was served on the PECN; a description of the data required to be	Yes	GCHQ keeps a central record of section 94 directions given by the Home Secretary or Foreign Secretary, respectively, on their behalf. The central record includes the date the direction was given; the name of the Secretary of State giving the direction; the PECN to which the direction relates and	

disclosed and; the date the direction was withdrawn or cancelled. The central record must be available for inspection purposes.		the date the direction was served on the PECN; a description of the conduct required to be undertaken. The record was made available for inspection by IOCCO.	
Errors			
There should be a clear process in place for the reporting of section 94 direction errors. That process should distinguish between errors that occur in the giving of, and conduct complying with, a section 94 direction and errors that occur when an agency is accessing data that has been retained.	**Yes**	There is no statutory requirement under section 94 of the Telecommunications Act 1984 to report an error when: a) undertaking the acquisition of BCD by means of a section 94 direction, or b) when accessing data already retained as a consequence. <u>Acquisition errors</u> No errors have been identified when undertaking the acquisition of BCD by means of a section 94 direction. GCHQ has a good review process that seeks to identify circumstances when the BCD collected may be outside GCHQ's remit [REDACTION] <u>Access errors</u> As stated in IOCCO's review report of section 94 directions, GCHQ in the main merges the communications data obtained under a section 94 direction with other datasets containing communications data (for example, related communications data obtained as a consequence of an interception warrant). GCHQ have a mechanism for reporting interception errors to the IOCCO, but cannot easily differentiate the source from which the data is derived without compounding any potential intrusion (for example, by re-running the erroneous query). However, it may be the case the Commissioner determines the position adopted by GCHQ that it is not practicable to differentiate between the sources of data is unsustainable. That being the case it is hoped that work by GCHQ and IOCCO	

		to explore how GCHQ's development tools and current audit systems may be modified to enable a more thorough inspection and audit may help identify cases were data, once lawfully acquired, is then accessed in error. No errors have been reported to IOCCO that relate specifically to data obtained under a section 94 direction.	
Excess Data			
Where conduct authorised by a section 94 direction results in the potential acquisition of excess data, or its disclosure by a PECN in order to comply with the requirements of a direction, assess the measures in place to minimise the disclosure of data not specified in the direction.	**Yes**	GCHQ has a good level of compliance in this area of work. This is achieved in two ways: 1. There are mechanisms in place to continually review the data disclosed and then filter out data not covered by the section 94 direction or falling outside GCHQ's remit so that it is not made available within the agency's data sets; and 2. If data or target behaviour is identified as causing a concern in relation to GCHQ's compliance a review is undertaken and appropriate action taken (for example, the recent review submitted to the Foreign Secretary[REDACTED]).	

5. Senior Responsible Officer (SRO)

Within every relevant public authority a Senior Responsible Officer (SRO) must be responsible for the integrity of the process within the public authority to acquire communications data and compliance with RIPA and the CoP.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
The SRO is responsible for engaging with the IOCCO inspectors during the inspection.	**Yes**	[REDACTED] (Deputy Director) and [REDACTED] (Joint Head of Warrantry & Oversight Team) were present during the course of the inspection and debrief.	
The SRO is responsible for the integrity of the process to acquire communications data and compliance with RIPA and the CoP; overseeing the reporting of errors to IOCCO; and, the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.	**Yes**	There is a history of good compliance by GCHQ albeit the inspection and oversight of section 94 directions is new.	
The SRO is responsible for the oversight of the implementation of post-inspection action plans.	**Yes**		

Conclusion & Requirement for Action:

IOCCO are extremely grateful for the excellent assistance and cooperation received during this inspection. The recommendations from this inspection are appended to the report in a schedule. It would be appreciated if you would ensure that the Senior Responsible Officer (SRO) oversees the implementation of the recommendations and ensures the schedule is completed and returned electronically to [REDACTED] IOCCO [REDACTED] by 13th November 2017.

Date report issued: 14th September 2017