

**Inspections under Part I Chapter II of the  
Regulation of Investigatory Powers Act (RIPA)  
by the Interception of Communications  
Commissioner's Office (IOCCO)**

Name of Public Authority	West Midlands Police
Date/s of Inspection	15 - 17 October 2012
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, Sir Paul Kennedy. IOCCO undertake a revolving programme of inspection visits to all relevant public authorities who are authorised to acquire communications data under Part I Chapter II of the Regulation of Investigatory Powers Act (RIPA), and produce a written report of the findings for the Interception of Communications Commissioner.

The primary objective of the inspection is to ensure that the system in place for acquiring communications data is sufficient for the purposes of the Act 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 (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised.

**Statistics:**

Number of Notices requiring disclosure of communications data within the meaning of each subsection of section 21(4) of the Act during the last 6 months.	[REDACTED]
Number of Authorisations requiring disclosure of communications data within the meaning of each subsection of section 21(4) of the Act during the last 6 months.	[REDACTED]
Number of applications submitted to a Designated Person for a decision to obtain communications data which were rejected after due consideration (during last 6 months).	[REDACTED]
Number of times an urgent Notice has been given orally, or an urgent Authorisation has been granted orally during the last 6 months. If practicable please breakdown figures by the number of Grade 1 and 2 approvals.	[REDACTED]

Staffing:

Senior Responsible Officer (SRO)	[REDACTED]
SPoC Manager	[REDACTED]
Accredited Officers (AOs) (indicate if full time, part time, oncall etc)	[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

Previous Recommendations:

West Midlands Police emerged well from their last inspection which took place in May 2011. 10 recommendations were made to improve the systems and processes. The inspectors were pleased to find that all of the recommendations had been introduced. However, there is still room to improve the quality of the proportionality justifications and this will be revisited in this report.

Summary of Inspection Findings:

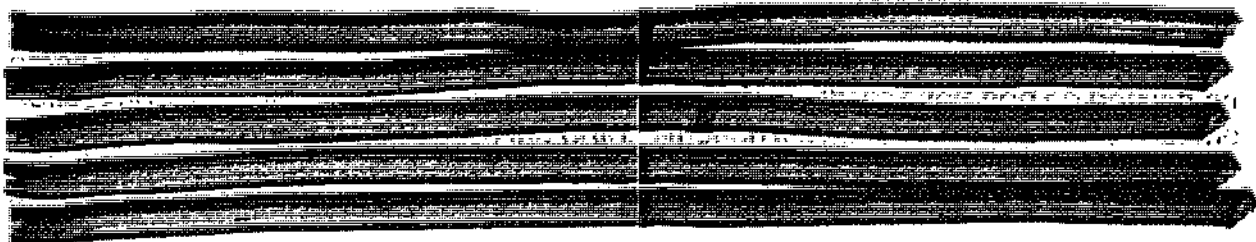
West Midlands Police emerged very well from this inspection and the inspectors were satisfied that the force is acquiring communications data lawfully and for the correct statutory purpose. Overall the public authority has a good level of compliance with the Act and CoP.

A reasonable standard of application is being produced across the board. The inspectors were satisfied that the applications were necessary and proportionate. However there is room to improve the proportionality justifications in two respects. First, all applicants must ensure that they clearly outline what they are trying to achieve from obtaining the data and second, all applicants must ensure they explain the relevance of any date / time periods requested. [REDACTED]

The Accredited Officers (AOs) in the Single Point of Contact (SPoC) are performing their guardian and gatekeeper duties very effectively and are ensuring that West Midlands Police acts in an informed and lawful manner when it is acquiring communications data. It is evident that the SPoC is highly regarded and that communications data continues to play a crucial role in investigations. Since the last inspection the CycComms system has been introduced to manage the communications data applications and a great deal of effort has gone into ensuring a smooth transition.

Overall the Designated Persons (DPs) are discharging their statutory duties responsibly. Their written considerations are generally completed to a good standard, albeit some advice has been provided to ensure that all DPs follow the good practice guidance by tailoring

their considerations to the individual applications.



The Inspectors concluded that the urgent oral process is extremely well managed. There is room to improve the audit trail in relation to the serving of notices and authorisations on the Communication Service Providers (CSPs) and a recommendation has been made to this effect.


The inspection findings are outlined in more detail in the following sections of the report. A number of recommendations arise from the inspection but these are mainly designed to fine tune the systems and procedures to assist the public authority to achieve the best possible level of compliance with the Act and CoP. The recommendations are shown in the last column of the inspection tables. Please note that recommendations are shaded red, amber or green. IOCCO have adapted 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 serious breaches and / or non-compliance with the Act or CoP which could leave the public authority vulnerable to challenge. The amber areas represent non-compliance to a lesser extent. However remedial action must still be taken in these areas as they could potentially lead to breaches. The green areas represent good practice or areas where the efficiency and effectiveness of the process could be improved.

Summary of Recommendations: Red - 0; Amber - 2; Green - 4.

**Areas Inspected:**

**1. Application Process**

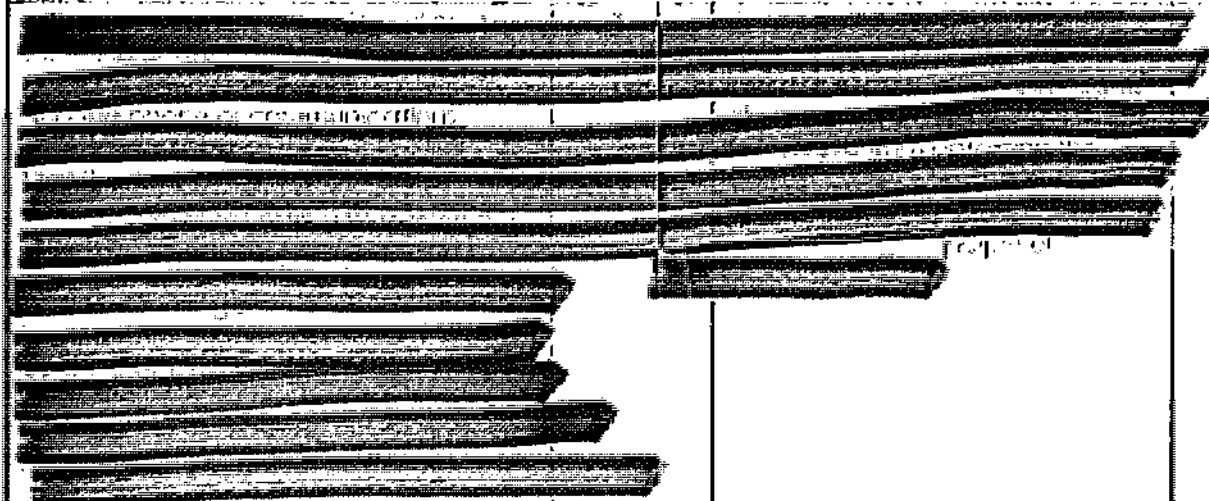
Acquisition of communications data under the Act involves four roles within a relevant public authority; the Applicant, the Designated Person (DP), the Single Point of Contact (SPoC) and the Senior Responsible Officer (SRO). The Act provides for two alternative means for acquiring communications data, by way of an Authorisation under Section 22(3) or a Notice under Section 22(4).

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
<b>Random Sampling &amp; Auditing Information from the Communication Service Providers (CSPs)</b>			
IOCCO obtained information from various CSPs outlining the requests for disclosure of data which the public authority had made during the last twelve months. These records were randomly checked against the application forms to verify that documentation was available to support the acquisition of the communications data from the CSPs. The inspection team also randomly examined a number of applications submitted by various	Yes	 In all cases the inspectors were satisfied that the correct process had been applied and that the data had been obtained lawfully, with the approval of a Designated Person (DP).  Overall the applications are completed to a satisfactory	


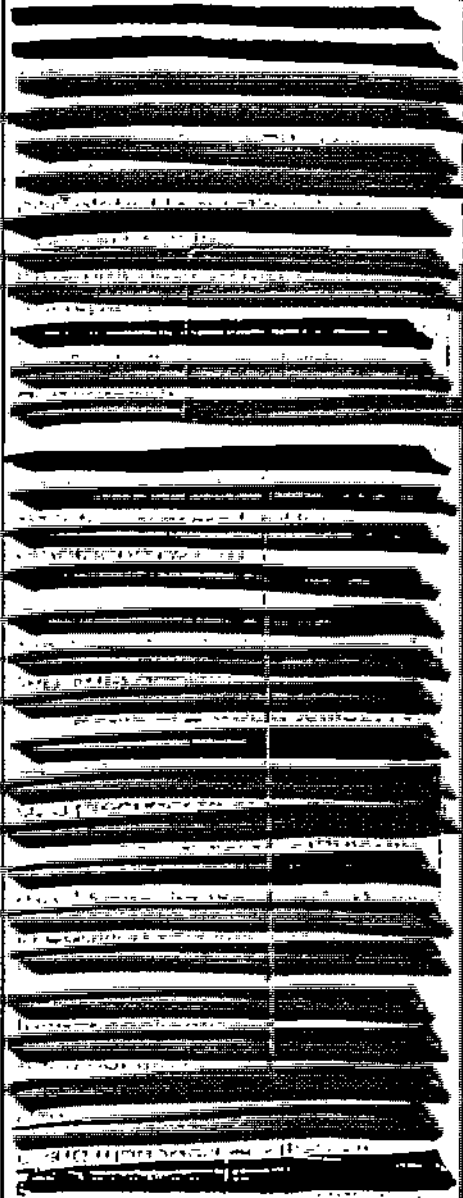
<p>divisions and departments in the force.</p>		<p>standard. The inspectors were also given an overview of one investigation by operational staff to ascertain what use had been made of the communications data acquired. A more detailed summary of this operation is appended to the report (Annex A).</p>	
--	--	---	--

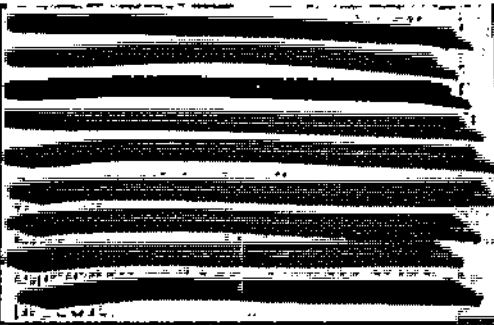
**Applicant**

<p>The applicant should complete an application form, setting out for consideration by the designated person (DP), the necessity and proportionality of a specific requirement for acquiring communications data, (Para 3.3 CoP). Applications must include all of the requirements specified in Paragraphs 3.5 and 3.6 of the CoP. The Home Office and ACPO Data Communications Group (DCG) have produced a template application form.</p>	<p><b>Yes</b></p>	<p><b>Application / System used:</b> West Midlands Police introduced the CycComms System in February 2012.</p>	
---	-------------------	--	--



<p>Proportionality: Applicants should outline what is expected to be achieved from obtaining the data and how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. The specific date/time periods requested should be justified i.e. how these are proportionate. An explanation as to how the data will be used, once acquired, and how this will benefit the investigation will assist the justification. (See Home Office and ACPO DCG application guidance document).</p>	<p><b>Partly</b></p>	<p>It was not always clear what the applicant was trying to achieve from obtaining the data and this is a key part of the proportionality test. On a number of occasions applicants had also failed to provide an explanation as to how the date periods requested were proportionate to the offence/s under investigation and this is also a key part of the proportionality test. It is recommended that in future all applicants should sufficiently justify the principle of proportionality by outlining what they are trying to achieve from obtaining the data and by explaining the relevance of any date / time periods requested. The SPoC must provide a more robust guardian and gatekeeper role in this respect and provide</p>	
--	----------------------	--	--

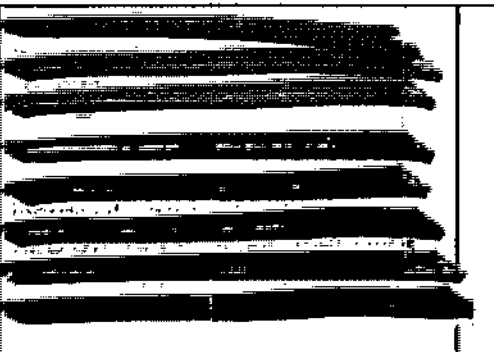
		applicants with appropriate training / advice where this principle is not sufficiently justified.	
<p>Collateral Intrusion: Applicants should consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstance. Applicants should be aware that that there will only ever be minimal collateral intrusion in relation to subscriber data or that none will be identified at the time the application is made. (See Home Office and ACPO DCG application guidance document).</p>	<p>Yes</p>		
	<p>No</p>	<p>No special arrangements are in place. All applications are submitted on the CycComms system.</p> 	

		
--	--	--

**Single Point of Contact (SPoC)**

<p>The SPoC should promote efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. The SPoC should provide a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner. (Para 3.16 CoP).</p>	<p><b>Yes</b></p>	<p>The SPoC is ensuring that the public authority acts in an informed and lawful manner when acquiring communications data. The SPoC is working very efficiently and ensuring that the data is acquired and disclosed in a timely fashion. A recommendation has already been made in this report to ensure that the SPoC provides a more robust guardian and gatekeeper function in future in relation to the principle of proportionality.</p>
<p>The SPoC should provide objective judgement and advice to both the applicant and the DP (Para 3.16 CoP). The SPoC should engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations. (Para 3.17 CoP).</p>	<p><b>Yes</b></p>	<p>The inspectors saw numerous examples of the AOs offering excellent guidance and advice to both applicants and DPs.</p>
<p>The SPoC should be in a position to fulfil the additional responsibilities outlined in Para 3.17 CoP. There should be a full audit trail of all of the actions taken by the SPoC.</p>	<p><b>Yes</b></p>	<p>The AOs are in regular contact with investigation teams to assist the staff to develop strategies to use communications data effectively in support of operations. There is a good audit trail on the CycComms system.</p>
<p>The SPoC may be an individual who is also a DP. The SPoC may be an individual who is also an applicant. The same person should never be an applicant, a DP and a SPoC. Equally the same person should never be both the applicant and the DP. (Para 3.19 CoP).</p>	<p><b>N/A</b></p>	

**Designated Persons (DPs)**

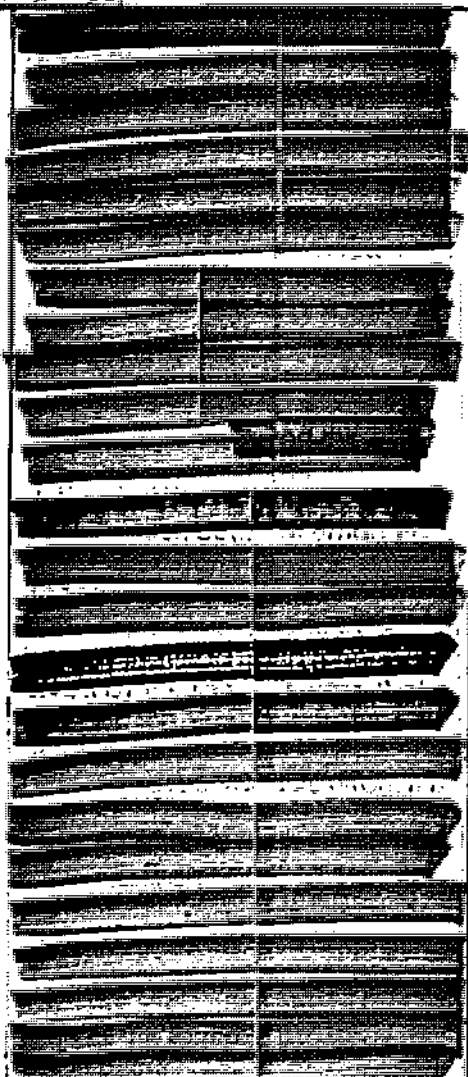
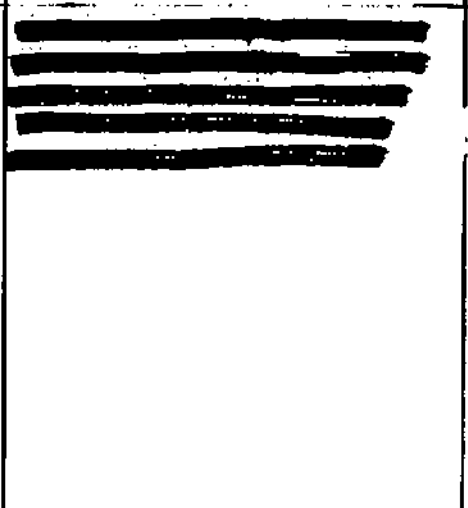
<p>A DP shall not grant an authorisation or give notice unless they believe that obtaining the data in question by the conduct authorised is proportionate to what is sought to be achieved by obtaining the data. (Section 22(5) Act). A DP must consider the application and record his considerations at the time (or as soon as is reasonably practicable) in writing or electronically. (Para 3.7 CoP). The DP shall assess the necessity for any</p>	<p><b>Yes</b></p>	
--	-------------------	--

<p>conduct to acquire or obtain data taking account of any advice provided by the SPoC. (Para 3.10 CoP).</p>		<p>The Inspectors were satisfied that the DPs are discharging their statutory duties responsibly.</p> <p>The DPs are completing their written considerations to a satisfactory standard.</p>	
<p>IOCCO recommends that DPs should tailor their written considerations to the individual applications to provide evidence that they have been given due consideration.</p>	<p>Partly</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>
<p>DPs must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a DP of their office, rank or position in the relevant public authority may grant or give. (Para 3.9 CoP).</p>	<p>Yes</p>		
<p>DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons. Where a DP is directly involved in the investigation or operation their involvement and their justification for undertaking the role of DP must be</p>	<p>Yes</p>	<p>A good level of independence exists in the process. The Inspectors examined one application that was approved by a DP who was directly involved in the investigation. This was undertaken for reasons of security and the [REDACTED] DP had complied with Para 3.11 by providing their justification for undertaking the role.</p>	

<p>[REDACTED]</p>	<p>Partly</p>	<p>[REDACTED]</p>	<p>[REDACTED]</p>
-------------------	---------------	-------------------	-------------------

<p><b>Content of Section 22(3) Authorisations and Section 22(4) Notices</b></p>			
<p>An authorisation must comply with all of the requirements outlined in Section 23(1) of the Act and Paragraphs 3.28, 3.43 &amp; 3.44 of the Code of Practice.</p>	<p>Yes</p>	<p>Authorisations on CycComms compliant. Home Office and ACPO DCG application and authorisation template [REDACTED]</p>	<p>[REDACTED]</p>
<p>A notice must comply with all of the requirements outlined in Section 23(2) of the Act and Paragraphs 3.37, 3.43 &amp; 3.44 of the Code of Practice.</p>	<p>Yes</p>	<p>Home Office and ACPO DCG template in use.</p>	<p>[REDACTED]</p>
<p>The 'giving of a notice' means at the point at which a DP determines that a notice should be given to a CSP (Para 3.35 CoP). A notice should emanate from the DP and be endorsed in a clear and auditable manner.</p>	<p>Partly</p>	<p>The DPs issue the Notices at the same time as they approve the related applications on the CycComms system.</p> <p>[REDACTED]</p>	<p>5</p>



			
<p>SPOCs should be mindful when drafting authorisations and notices to ensure the description of the required data corresponds with the way in which the CSP processes, retains and retrieves its data for lawful disclosure. A notice must not place a CSP under a duty to do anything which is not reasonably practicable for the CSP to do. (Section 22(7) Act, Para's 3.29 &amp; 3.38 CoP)</p>	<p>Yes</p>		
<p>A DP may grant an authorisation for persons holding offices, ranks or positions with the same public authority as the DP to engage in any conduct to which Part I Chapter II applies. A notice shall not require the disclosure of data to any person other than the person giving the notice or such other person as may be specified in the notice so long as that person holds an office, rank or position within the same relevant public authority as the DP. (Sections 22(3) &amp; 23(3) Act, Para's 3.24 &amp; 3.39 CoP). The exception to this is where a public authority enters into a formal collaboration agreement under Sections 5 and 7 of the Policing and</p>	<p>Yes</p>		

Crime Act 2009.			
<b>Duration, Renewal &amp; Cancellation of Section 22(3) Authorisations and Section 22(4) Notices</b>			
<p>Relevant to all authorisations and notices is the date upon which authorisation is granted or notice given. From that date, when the authorisation or notice becomes valid, it has a validity of a maximum of one month (see footnote 57 CoP). This means the conduct authorised should have been commenced or the notice served within that month. (Para 3.42 CoP).</p>	Yes		
<p>Any valid authorisation or notice may be renewed at any time <u>before</u> the end of the period of one month applying to that authorisation or notice, for a period of up to one month by the grant of a further authorisation or the giving of a further notice. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing. (Sections 23(5), 23(6) &amp; 23(7) Act, Para 3.46 CoP).</p>	Yes	<p>In general the AOs manage the process efficiently and as a result renewals are rarely needed.</p> <p>The renewal process had only been invoked on four occasions on the CycComms system. On three of the four instances the DP had granted the new Section 22(3) Authorisation after the original Authorisation had expired which is not permitted. Fortunately on these occasions the AOs did not need to acquire any further data and therefore no breach occurred.</p> <p>However the system should not allow the DP to renew in such instances. During the inspection the SPaC Manager contacted GSA Ltd who acknowledged there was a problem in this respect and that the issue would be fixed in the next release. Until then the AOs are aware of the problem and will ensure that any renewals are appropriately granted.</p>	
<p>Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out in an addendum to the application. Where a DP is granting a further authorisation or giving a further notice they should have considered why it is necessary and proportionate to continue with the acquisition of the data and record the date, and when appropriate, the time of the renewal. (Para 3.47 &amp; 3.48 CoP).</p>	Yes		
<p>Where a DP is satisfied that it is no longer necessary or proportionate to acquire the communications data he shall cancel the notice or withdraw the authorisation. (Section 23(8) Act, Para's 3.49, 3.50, 3.52 &amp; 3.53 CoP). Reporting of</p>	Yes		

<p>a cancellation to a CSP may be undertaken on a DP's behalf by the SPoC, but in such cases the DP must confirm the decision in writing or in a manner that produces a record of the notice or authorisation having been cancelled or withdrawn by the DP.</p>			
<p>A cancellation notice must include the details outlined in Paragraph 3.51 of the Code of Practice. A withdrawal of an authorisation must include the details outlined in Paragraph 3.54 of the Code of Practice.</p>	<p>Yes</p>		
<p><b>National Priority Grading System (NPGS)</b></p>			
<p>Where relevant, the Data Communications Group (DCG) NPGS should be applied to requests for communications data correctly and fairly. [See Footnote 40 of the CoP]. The emphasis within Grade 1 and Grade 2 is that the urgent provision of the specific communications data will have an immediate and positive impact on the investigation.</p>	<p>Yes</p>	<p>The vast majority of applications were appropriately graded [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]</p>	
<p><b>Streamlining Procedures</b></p>			
<p>The streamlining procedure outlined in Paragraph 3.30 of the Code of Practice should be used to reduce unnecessary bureaucracy and speed up the collection of the data when acquiring subscriber data under Section 2(4)(c). This procedure assists with number porting issues and enables the AOs to be more proactive when acquiring subscriber information by widening the data capture. In these instances it may be pertinent to acquire the data in stages. Furthermore, it is often good practice to check with the applicant before the data capture is widened because the direction of the investigation may have changed since the application was submitted or the user of the phone or communications address may have been identified through some other means.</p>	<p>Yes</p>	<p>Good use continues to be made of this procedure to widen the data capture and when dealing with number porting.</p>	
<p>The streamlining procedure outlined in Paragraphs 3.31 and 3.32 of the Code of Practice which enable a DP to pre-authorise future subscriber checks at the same time as he or she is approving an application for service use or traffic data under Sections 2(4)(a) or (b) of RIPA, should be used to reduce unnecessary bureaucracy and speed up the collection of the data.</p>	<p>Yes</p>	<p>Good use is being made of this procedure. [REDACTED] [REDACTED] [REDACTED]</p>	
<p>The applicant must outline why it is necessary and proportionate to either widen the data capture under Section</p>	<p>Yes</p>	<p>The CycComms system contains a question in relation to the consequential subscriber data</p>	

<p>21(4)(c), or obtain the consequential 'future' subscribers in their application. In the latter case they should outline what analytical work they intend to conduct on the service use / traffic data to identify the relevant numbers. It is important that the SPoC gives appropriate advice to the DP and that the DP fully understands what he or she is approving in the application form.</p>		<p>and this is drawn to the attention of the DP. The AOs are providing the DPs with good advice in relation to the use of these procedures. Some of the DPs are also referring to the fact that they are approving consequential subscriber data in their considerations which is regarded as good practice.</p>	
<p>The AOs should spot check the schedules to assure the integrity of the process, i.e. to check that the communications addresses derive from the original service use / traffic data requests and that secure open source checks have been conducted. This should provide a good safety net. Furthermore if an AO finds evidence that applicants or analysts are not following the correct procedures then this should be brought to the attention of the SRC.</p>	<p>Yes</p>	<p><b>Have any breaches been identified by the AOs: No.</b></p> <p><b>Schedules checked by Inspectors:</b> Yes - Random checks were conducted against a number of the schedules and the Inspectors verified that the communications addresses derived from the original data requests.</p> <p>CycComms prevents the submission of a schedule if the authorisation has expired.</p>	

## 2. Urgent Oral Process

In exceptionally urgent circumstances, application for the giving of a notice or the grant of an authorisation may be made by an applicant, approved by a DP and either notice given to a CSP or an authorisation granted orally.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
<p>Circumstances in which an oral notice or authorisation may be appropriate are outlined in full in Paragraph 3.56 of the Code of Practice. Briefly the process may be used for the following circumstances; an immediate threat to life; an exceptionally urgent operational requirement where the data will directly assist the prevention or detection of a serious crime and the making of arrests or the seizure of illicit material; a credible and immediate threat to national security. Applicants must demonstrate how the opportunity will be lost if the application procedure were undertaken in writing from the outset.</p>	<p>Yes</p>	<p>The Inspectors concluded that the urgent oral process is extremely well managed.</p> <p>A new electronic process has been introduced since the last inspection and this is more efficient.</p>	
<p>The use of the urgent oral process must be justified for each application within an investigation. The fact that any part of an investigation is undertaken urgently must not be taken to mean that all requirements to obtain communications data in connection with that investigation be undertaken using the urgent oral process.</p>	<p>Yes</p>	<p>The requests examined were justified and there was no evidence found of unnecessary or continued use of the urgent grades once the period of urgency had ended.</p>	

<p>After the period of urgency a written process must be completed demonstrating the consideration given to the circumstances and the decisions taken. The applicant or the SPoC shall collate details or copies of contemporaneous records of the considerations given to the acquisition of data, decisions made by the DP and the actions taken in respect of the decisions. [Para's 3.61 &amp; 3.62 CoP]</p>	<p><b>Yes</b></p>	<p><b>Urgent oral SPoC log sheet:</b> Yes</p> <p><b>Full audit trail of process:</b> Yes - the SPoC logs are consistently maintained to an exceptionally high standard. There was a full audit trail in place of the decisions made and actions taken. The DPs are also being given the opportunity to endorse their considerations by email after the period of urgency.</p>	
<p>Written notice (or assurances of authorisations) must be given to the CSP retrospectively within one working day [see footnote 67 of CoP] of the oral notice being given. Failure to do so will constitute an error which may be reported to the Commissioner by the CSP and must be recorded by the public authority. [Para 3.60 CoP].</p>	<p><b>Partly</b></p>	<p>[REDACTED]</p>	
<p>When in a matter of urgency a DP decides that the oral giving of a notice or grant of an authorisation is appropriate, that notice should be given or the authorised conduct undertaken as soon as practicable after the making of that decision.</p>	<p><b>Yes</b></p>		

### 3. Training

It is important for all persons involved in the process to receive training and guidance to ensure that communications data is acquired lawfully in accordance with the Act and Code of Practice and used effectively in support of investigations.

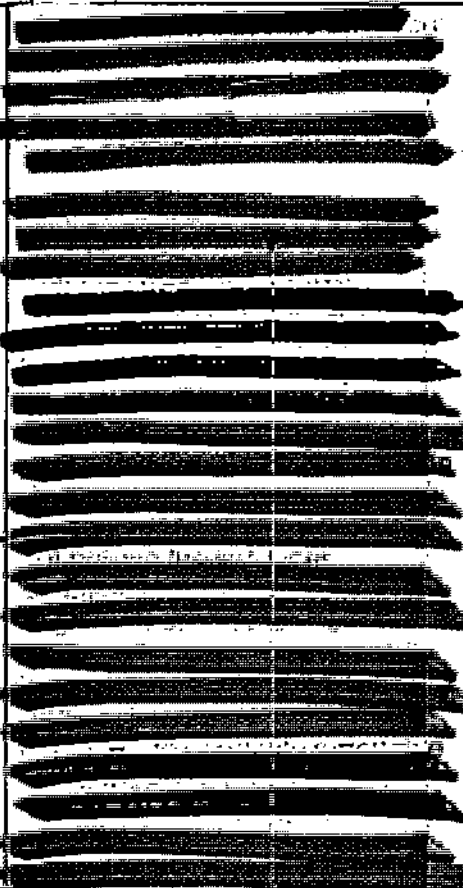
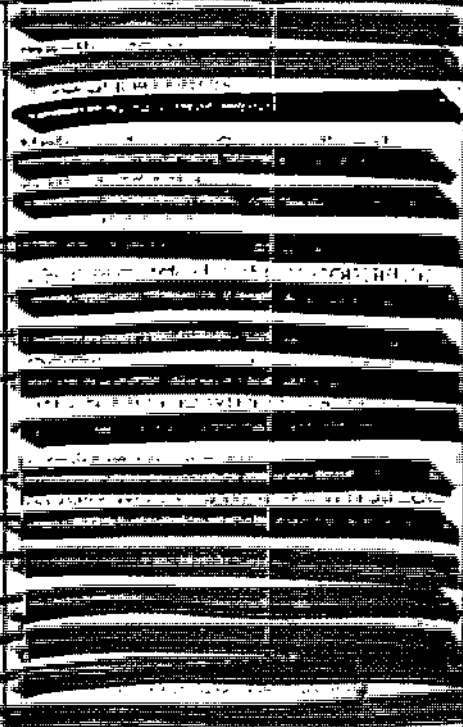
Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
<p>The SPoC is either an accredited officer [AO] or group of AOs trained to facilitate lawful acquisition of communications data. All AOs must complete a course of training and have been issued a SPoC PIN number. [Para 3.15 CoP]. When an AO leaves the SPoC their PIN number should be removed from the list of approved AOs.</p>	<p><b>Yes</b></p>	<p><b>PIN list checked:</b> Yes - The SPoC Manager added the new SRO to the PIN list during the inspection. All AOs have attended accreditation training, refresher training and various tradecraft events. There is greater attendance at tradecraft events now they are regionally delivered.</p>	
<p>DPs must have current working knowledge of human rights principles, specifically those of necessity and</p>	<p><b>Yes</b></p>	<p>Training is provided by the SPoC Supervisor to all newly promoted Inspectors and Superintendents,</p>	

<p>proportionality, and how they apply to the acquisition of communications data under Chapter II of Part I RIPA and its associated CoP. (Para 3.8 CoP).</p>		<p>There is also online learning and advice in relation to the CycComms system.</p>	
<p>SPoCs should make efforts to ensure applicants are appropriately trained in the acquisition of communications data.</p>	<p><b>Yes</b></p>	<p>A great deal of effort has gone into the delivery of the CycComms system. A regular newsletter is issued to provide applicants with correct and up to date advice.</p> <p>The SPoC Manager and her team have introduced and trained Digital Media Co-ordinators across the force. The Co-ordinators are embedded in various investigation teams and have assisted to provide more focus to the communications data requests and reduce the overall level of applications. This appears to have been a major success.</p>	

**4. Keeping of Records**

There are clear rules which must be followed in relation to the keeping of records and these procedures include the recording and reporting of errors. See Chapter 6 of the Code of Practice [CoP] for further information.

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
<b>Records to be kept</b>			
<p>Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellation of notices, must be retained by the public authority in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The public authority should also keep a record of the date, and where appropriate the time, when each notice or authorisation is given or granted, renewed or cancelled. [Para 6.1 CoP].</p>	<p><b>Yes</b></p>	<p>The CycComms system meets the requirements set out in the CoP.</p>	
<p>Records kept by the public authority must be held centrally by the SPoC or in accordance with arrangements previously agreed with the Commissioner. These records must be available for inspection by the Commissioner [Para's 6.1 &amp; 6.2 CoP].</p>	<p><b>Yes</b></p>		
<b>Errors</b>			
<p>Where communications data is acquired or disclosed wrongly a report must be made to the Senior Responsible Officer (SRO) and then to the Commissioner</p>	<p><b>Partly</b></p>	<p>[REDACTED]</p>	

<p>["reportable error"] using the Error Reporting Form within no more than five working days of the error being discovered. (Para's 6.13 &amp; 6.17 CoP). The error report must contain all of the details outlined in Para 6.18 of the CoP.</p>			
<p>In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences ["recordable error"]. These records must be available for inspection by the Commissioner (Para 6.14 CoP). The records must include the details outlined in Para 6.20 of the CoP.</p>	<p>Yes</p>		
<p>Where material is disclosed by a CSP in error which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, the material and any copy of it should be destroyed as soon as the report to the Commissioner has been made. (Para 6.21 CoP).</p>	<p>Yes</p>		
<p>Excess Data</p>			

Restricted (when completed)

<p>Where authorised conduct by a public authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a notice, all the data acquired or disclosed should be retained by the public authority, if having reviewed the excess data it is intended to make use of it in the course of the investigation an applicant must set out the reason(s) for needing to use that material in an addendum to the original application. The DP will then consider the reason(s) and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation. (Para's 6.23 to 6.25 CoP).</p>	<p>Yes</p>	<p>AOs are aware of the procedure to be followed.</p>	
---	------------	---	--

5. Confidential Unit

Baseline	Achieved (Yes / No / Partly)	Description of Procedures & Action Required (if applicable)	Rec No.
[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	
[REDACTED]	[REDACTED]	[REDACTED]	

Restricted (when completed)



		<p>[REDACTED]</p>	
<p>[REDACTED]</p>	<p>May</p>	<p>[REDACTED]</p>	
<p>[REDACTED]</p>		<p>[REDACTED]</p>	
<p>[REDACTED]</p>		<p>[REDACTED]</p>	
<p>[REDACTED]</p>		<p>[REDACTED]</p>	
<p>[REDACTED]</p>	<p>Yes</p>	<p>[REDACTED]</p>	

[REDACTED]

[REDACTED]

**Freedom of Information Act (FOIA)**

IOCCO is not a "public authority" for the purpose of the FOIA. It is therefore outside the reach of the Act, but it is appreciated that police forces are not and that they may receive requests for disclosure of our reports. In the first instance the SRO should follow the procedure which is outlined in Paragraph 8.5 of the Code of Practice (Part I Chapter II of RIPA) and also bring the matter to the attention of the ACPO FOI Central Referral Unit ([acpo.advice@foi.police.pnn.uk](mailto:acpo.advice@foi.police.pnn.uk)). No disclosure should take place until both parties have been fully consulted as it is very important that requests under the FOIA are dealt with in a consistent manner.

**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] by 27<sup>th</sup> January 2013. In light of the good level of compliance it will not be necessary to conduct a further inspection for at least 18 months.