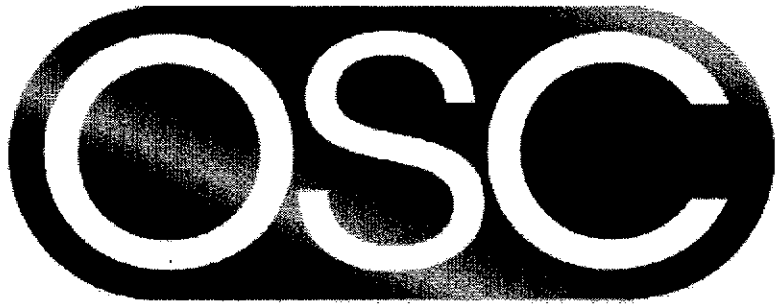

Office of Surveillance Commissioners

PROCEDURES AND GUIDANCE

Oversight arrangements for

covert surveillance and property interference

conducted by public authorities

Issued by the Chief Surveillance Commissioner

The Rt. Hon. Sir Christopher Rose

September 2010

Intentionally blank

The opinions expressed in the Interpretational Guidance Section of this publication are those of the Surveillance Commissioners. They do not purport to state what the law is: they merely indicate the way in which the Commissioners are minded to construe particular statutory provisions. There is no statutory requirement to publish them but they are a response to frequent requests for guidance from public authorities or are matters raised or identified during inspections. In the absence of case law, they are the most reliable indicator of likely judicial interpretation. They are the basis on which inspections will be conducted and performance assessed by the Office of Surveillance Commissioners. Applicants and authorising officers should take note of the interpretations when constructing and considering applications for the use of covert surveillance.

The document is to be properly promoted by and made accessible to all members of each public authority subject to the oversight of the Chief Surveillance Commissioner. Authorising officers are expected to retain a personal copy.

Extracts may be reproduced but notes must be copied in full and without alteration. Any extracts must be attributed as "Note [number] OSC Procedures and Guidance 2010" either immediately following the extract or as a footnote or as an endnote.

This document supersedes the OSC Procedures and Guidance published in December 2008 and all similar publications. The Chief Surveillance Commissioner, Surveillance Commissioners and Assistant Surveillance Commissioners – all of whom have held judicial office – will note its contents but may exercise individual discretion if they are presented with facts which justify expression of an alternative view.

Amendment Sheet

Date	Amendment Number	Amendment	Made by

Contents

PART 1 - PROCEDURES

SECTION 1 – INTRODUCTION

GENERAL

1. This document explains the role of the Office of Surveillance Commissioners and how the Commissioners carry out their statutory functions. It also sets out the requirements of the Chief Surveillance Commissioner with regard to the notification of authorisations for property interference and intrusive surveillance. It takes account of the implementation of the Police Act 1997 ('PA97'), the Regulation of Investigatory Powers Act 2000 ('RIPA'), the Regulation of Investigatory Powers (Scotland) Act 2000 ('RIP(S)A') and amending legislation. It replaces all previous versions of the Procedures and Guidance.

2. The terms 'he' and 'his' are used throughout this document when referring to a Commissioner, an authorising officer and the subjects of covert surveillance. This is simply for ease of reference and does not indicate an assumption that they are male.

ROLE OF THE OFFICE OF SURVEILLANCE COMMISSIONERS (OSC)

3. The OSC is a Non Departmental Public Body (NDPB) which was established to oversee covert surveillance and property interference operations carried out by public authorities. The work of the OSC is led by the Chief Surveillance Commissioner. He reports directly to the Prime Minister and First Minister of Scotland and is supported by Surveillance Commissioners, Assistant Surveillance Commissioners, Inspectors and a Secretariat.

4. The Commissioners are appointed under Part III of PA97 and RIP(S)A to oversee operations carried out under those Acts as well as under Parts II and III of RIPA.

5. The work of the Commissioners is divided into three main categories: first, considering notifications of authorisations for property interference when they are granted, renewed or cancelled; secondly, deciding whether to give or withhold approval for certain operations under PA97 and under RIPA/RIP(S)A before they take place; and thirdly, oversight of the use of powers conferred by the Acts relating to encryption keys.

6. Even if a Commissioner's prior approval is required before an authorisation becomes effective, the responsibility for authorising an operation always remains with the authorising officer within the relevant law enforcement agency. It is the responsibility of each authorising officer to ensure that any necessary approvals are obtained from the Commissioners.

DISCLOSURE OF INSPECTION REPORTS

7. Paragraph 9.7 of the RIPA Covert Human Intelligence Source Code of Practice provides that reports made by the Commissioners concerning the inspection of public authorities and their exercise and performance of powers under RIPA Part II may be made available to the Home Office. Paragraph 9.8 provides that public authorities may publish their inspection reports, in full or in summary, subject to the approval of the OSC at least 10 working days prior to intended publication. These provisions are not made at the request of the Chief Commissioner. The Chief Commissioner does not divulge the content of inspection reports to anyone other than the Chief Officer of the public authority inspected.

HOW TO CONTACT OSC

8. Any queries on interpretational issues or operating practices should be directed to the appropriate regional office in the first instance. If necessary, queries can be referred to the Secretary to OSC. Authorisations for England, Wales and Scotland will be processed by the central office (telephone: 020 7035 0074) and those for Northern Ireland by the Belfast office (telephone 02890 765155 (am) 02890 528170 (pm)).

9. Section 2 of this guidance sets out the procedures to be adopted by law enforcement agencies in notifying Commissioners of authorisations and requesting prior approval where appropriate. These procedures only cover the requirements subsequent to authorisation by an authorising officer. Procedures prior to this remain the responsibility of the relevant law enforcement agency.

SECTION 2 – PROPERTY INTERFERENCE AND INTRUSIVE SURVEILLANCE OPERATIONS

GENERAL

10. Most authorisations, applications for prior approval, renewals and cancellations will be sent to OSC offices by BRENT fax or through CLUSTER. However, there will be occasions outside normal working hours when the authorising officer or his staff need to contact the Commissioners directly. This will apply when a Commissioner's prior approval is required for operations that need to start outside office hours. It applies also to cases where the prior approval of a Commissioner would normally be required, but where, because of the urgency of the case, prior approval has not been sought or obtained (but see 23 below). The OSC will therefore supply force authority bureaux with a rota showing the Duty Commissioners and how they can be contacted.

11. OSC working hours are 9am – 5pm Monday to Friday except for Public Holidays.

TIMESCALES

12. All authorisations, renewals and cancellations should be notified to the OSC within four working hours of being given. Renewals should be submitted to the OSC before the existing authorisation expires. If there are any problems in meeting these targets, the OSC should be notified and the reasons explained.

13. Forces are reminded that, except in urgent cases, requests for prior approval should be sent to the OSC London or Belfast office at least 16 working hours before the surveillance is due to start. Some forces are not following this guidance and are allowing no more than a few hours for Commissioners to consider the papers.

14. For ease of reference the Chief Commissioner's requirements for each type of authorisation are set out below.

NOTIFICATION OF PROPERTY INTERFERENCE AUTHORISATIONS

15. In most cases an authorisation for property interference is notified to a Commissioner for his scrutiny after it has been given but it is effective from the time of signing. This does not apply to a renewal which, if applied for before the existing authorisation expires, takes effect on expiry.

16. BRENT fax the authorisation and all supporting documentation to the appropriate office of the OSC within four working hours of the authorisation being granted.

PRIOR APPROVALS IN INTRUSIVE SURVEILLANCE AND PROPERTY INTERFERENCE CASES

17. In most intrusive surveillance cases and in certain property interference cases, referred to as 'prior approval cases', an authorisation will not take effect until a Commissioner has approved it and the authorising officer has been notified in accordance with the legislation. The property interference cases in which prior approval is required are cases where the person giving the authorisation believes that:

a. any of the property specified in the authorisation is

i. used wholly or mainly as a dwelling or as a bedroom in a hotel or

ii. constitutes office premises; OR

b. the action authorised is likely to result in any person acquiring knowledge of

i. matters subject to legal privilege

ii. confidential personal information (of the limited character specified in section 99 of PA97), or

iii. confidential journalistic material.

Prior approval cases in working hours

18. BRENT fax the authorisation and all supporting documentation to the appropriate office of the OSC within four working hours of the authorisation being granted and, unless the matter is urgent, at least 16 working hours before the approval is needed.

Prior approval cases outside working hours

19. Contact the Duty Commissioner on the number shown on the duty rota to tell him that the authorisation has been granted and when his approval is likely to be required. He will tell you how and when the papers can be submitted to him.

20. If you have problems contacting the Duty Commissioner for your area of the UK you should contact a Commissioner who is on duty for one of the other areas.

21. If possible, contact a Commissioner as soon as you know that his approval is likely to be needed so that there are no avoidable delays once the authorisation is ready for his consideration.

Renewals of prior approvals

22. BRENT fax the authorisation and all supporting documentation to the appropriate office of the OSC within four working hours of the authorisation being renewed and at least 16 working hours

before the current authorisation is due to expire. This allows time for the Commissioner to give his approval so that the renewal can become effective before the initial authorisation expires. In default a fresh application will be required.

Urgent cases where there is not enough time to seek prior approval

23. When the urgency provisions of section 95(1) and 97(3) of PA97 are used and when there is insufficient time to apply for approval (in a case where approval would otherwise be required) an oral authorisation can be granted. The need for prior approval is then dispensed with.

24. Outside working hours contact the Duty Commissioner as soon as practicable after the authorisation is granted (but not between 11pm and 7.30am) and tell him what has been authorised and the grounds for believing that the case was one of urgency. The papers should be sent to the Commissioner (care of OSC) as soon as practicable.

Notifications and renewals of notifications

25. BRENT fax the authorisation and all supporting documentation to the appropriate office of the OSC within four working hours of the authorisation being granted or renewed.

Urgent oral authorisations

26. During working hours, BRENT fax the oral authorisation forms, signed by the applicant and the authorising officer, to the appropriate office of the OSC within four working hours of the authorisation being granted. Otherwise, follow the guidance at paragraph 24. A Commissioner will not expect to be provided with the details of an intelligence case.

Cancellations

27. BRENT fax the cancellation form to the appropriate office of the OSC within four working hours of the authorising officer cancelling the authorisation. It is vital that the cancellation explains: what time the order to cease activity was given; what interference or surveillance was conducted since the authorisation was granted or renewed; the value of the activity and confirmation that all equipment has been recovered.

28. For directed surveillance and CHIS activity which was likely to obtain legally privileged information, the Commissioner will expect to be informed whether legally privileged information has been obtained and, if so, what steps have been taken to deal with it.

NOTIFICATION OF COMMISSIONERS' DECISIONS

29. The Commissioners will seek to return decisions on all notifications of authorisation within 16 working hours, and decisions on applications for their prior approval within eight working hours. If an authorising officer needs an application for prior approval to be considered more quickly, he must make this clear when sending the application to the OSC or Duty Commissioner and they will do their utmost to meet your timescales.

APPEALS AGAINST COMMISSIONERS' DECISIONS

Powers of the Commissioners

30. The Commissioners have the power to quash or cancel any authorisation where they are satisfied that the authorisation criteria were not met at the time the authorisation was given or are no longer met. They can quash authorisations given under the urgency provisions if they are satisfied that, at the time of the grant of the authorisation, there were no reasonable grounds for believing that the case was one of urgency. They also have the power to order the destruction of any material obtained other than that required for pending criminal or civil proceedings.

When appeals can be brought

31. PA97, RIPA and RIP(S)A all provide for the submission by an authorising officer of an appeal to the Chief Surveillance Commissioner against Commissioners' decisions.

32. An authorising officer may appeal to the Chief Surveillance Commissioner within a period of seven days against any decision made by a Commissioner to:

a. refuse to approve an authorisation or its renewal,

b. quash an authorisation or renewal,

c. cancel an authorisation or renewal, or

d. order the destruction of records when cancelling or quashing an authorisation or renewal (other than those required for pending civil or criminal proceedings).

How to appeal

33. All appeals should be sent in the first instance to the Secretary to OSC (by secure BRENT or to OSC, PO Box 29105, London SW1V 1ZU), who will forward them to the Chief Surveillance Commissioner for his consideration.

34. The authorising officer should set out the full reasons for appealing, taking into account the grounds on which the Chief Surveillance Commissioner may allow an appeal as specified in the Acts.

35. The Chief Surveillance Commissioner will give notice of his determination to the authorising officer concerned and to the Commissioner who made the initial decision.

36. Where he dismisses an appeal, the Chief Surveillance Commissioner will make a report of his findings to the Prime Minister.

SECURE COMMUNICATION ARRANGEMENTS

37. In view of the sensitivity of the material being handled, it is imperative that all parties observe strict security arrangements. In particular, the following points should be borne in mind:

a. All telephone calls and fax transmissions to and from the OSC and the Commissioners that involve sensitive material must utilise the BRENT encrypted lines. The generally published telephone lines are not secure. All Commissioners have been provided with mobile

telephones to ease contact outside office hours but law enforcement agencies should have in mind that this form of communication is not secure.

b. When sending protectively marked faxes to the OSC offices or the Commissioners, speak to the OSC or the Commissioner on the BRENT telephone number before sending the fax.

c. Law enforcement agencies will need to ensure that their faxes are connected to BRENT (via a G3FI interface) through the BRENT Data port to enable secure telephone conversations to take place at the same time as a fax is being transmitted.

d. All law enforcement agencies (even those with e-mail links, as out of hours access to Commissioners may still be required) must have BRENT equipment. Separate arrangements are in place for Scottish police forces, where there is greater reliance on CLUSTER.

e. The BRENT fax machines in the Secretariat are not capable of receiving information outside normal office hours, i.e. 9am – 5pm Monday to Friday.

PART 2 – INTERPRETATIONAL GUIDANCE

Each activity should be considered on its merits

100 It is unacceptable to consider whether an authorisation is required based on the description of the surveillance. Test purchase operations conducted by law enforcement agencies (e.g. in drugs operations) are significantly different from those normally conducted by local authorities (e.g. by trading standards). 'Drive-by' surveillance may or may not require an authorisation depending on the circumstances.

101 The application of the legal principles of covert surveillance to particular facts is, ultimately, a matter of judgment: the extent to which judgment can be prescribed is limited; there cannot be a one-size-fits-all catalogue of principles, and it would be misleading if authorising officers, in particular, were to believe that such a chimera exists.

102 A common error when considering whether authorisation is required is to restrict contemplation to the type of tactic rather than the specific facts of the activity. It is unwise to approach RIPA or RIP(S)A from the perspective of labels.

The effect of section 80 RIPA and section 30 RIP(S)A

103 Whilst not an obligation there is an expectation that covert surveillance is authorised. Section 80 RIPA and Section 30 RIP(S)A help a Trial Judge in exercising his discretion regarding the admissibility of evidence and the impact of the way that evidence was obtained on the fairness of a trial. It is inappropriate to cite these sections as justification for a decision not to authorise. It is unwise for a public authority to rely on them as protection from liability if it chooses not to authorise covert surveillance. It is one of the functions of the Office of Surveillance Commissioners to prevent abuse of discretionary powers.

Necessity

104 The authorising officer must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in s.28(3) of RIPA and s.29(3) of RIP(S)A. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. Often missed is an explanation of why it is necessary to use the covert techniques requested.

Proportionality

105 Proportionality is a key concept of RIPA and RIP(S)A. It is often poorly articulated. An authorisation should demonstrate how an authorising officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment

can only properly be reached once all other aspects of an authorisation have been fully considered.

106 A potential model answer would make clear that the four elements of proportionality had been fully considered:

106.1 balancing the size and scope of the operation against the gravity and extent of the perceived mischief,

106.2 explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,

106.3 that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and

106.4 providing evidence of other methods considered and why they were not implemented.

"I am satisfied" and "I believe"

107 The authorising officer should set out, in his own words, why he is satisfied (RIP(S)A) or why he believes (RIPA) the activity is necessary and proportionate. A bare assertion is insufficient.

Record the provenance of the data, information or intelligence on which covert surveillance is based

108 To assist an authorising officer to reach a proper judgment, the provenance of the data, information or intelligence on which the application has been made should be clear. It is considered best practice for law enforcement agencies to utilise standard evaluation nomenclature which grades both the source and the information. While it is not necessary or desirable in the application to spell out in detail the content of intelligence logs, cross-referencing to these enables an authorising officer to check detail. Particular care should be taken when using data or information obtained from open or unevaluated sources such as the Internet or social networks.

109 The law prevents an applicant or authorising officer from referring in writing to intelligence derived from some sensitive sources and this presents significant difficulty when covert surveillance is to be based wholly or in part on that type of intelligence. If it is not possible to construct sanitised intelligence, a cross-reference to the appropriate confidential briefing should suffice. The authorising officer should not be denied knowledge of intelligence if it is relevant to his authorisation.

The impact of UK SI 2003/3171 (restricting local authority grounds to section 28(3)(b) of RIPA)

110 Local authorities (outside Scotland) can no longer seek the protection that the Act affords on the grounds provided by subsections 28(3)(d) and (e) (i.e. in the interests of public safety and for the purpose of protecting public health). In order to conduct covert surveillance with the protection of RIPA, the authorising officer must demonstrate that the proposed activity is necessary for the prevention and detection of crime or prevention of disorder (see RIPA section 81(5)).

All covert activity that is not properly authorised should be reported as soon as it is recognised.

111 Activity which should properly be authorised but which isn't should be reported to the Chief Surveillance Commissioner, in writing, as soon as the error is recognised. This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. It does include activity which should have been authorised but wasn't or which was conducted beyond the directions provided by an authorising officer. All activity which should have been authorised but was not should be recorded and reported to the Inspector(s) at the commencement of an inspection to confirm that any direction provided by the Chief Surveillance Commissioner has been followed.

112 When it is decided to use covert surveillance without the protection of RIPA or RIP(S)A it would be prudent to maintain an auditable record of decisions and actions. Such activity should be regularly reviewed by an authorising officer.

The effect of the Policing and Crime Act 2009

113 The Policing and Crime Act 2009 amends section 93 PA97 and sections 29 and 33 RIPA. It enables law enforcement agencies to enter into written collaboration agreements regarding the provision of support within the operating area of the relevant collaborative units. For a collaboration agreement to take effect, the terms of the agreement must explicitly permit officers of the prescribed rank, grade or office to make applications or authorisations or to have day-to-day responsibility for dealing with a CHIS or to have general oversight of the use made of a CHIS or to have responsibility for maintaining a record of the use made of a CHIS or to be used as a CHIS. The CHIS Code of Practice paragraphs 6.10 to 6.13 provide for the authorised control and handling of a CHIS who benefits more than one authority. The Surveillance and property interference Code of Practice paragraphs 3.20 and 3.21 provide for applications and authorisations for directed and intrusive surveillance and property interference where there is a collaboration agreement.

114 If there is no written collaboration agreement, the arrangements provided at paragraphs 7.12 to 7.13 of the Covert Surveillance and property interference Code of Practice and paragraph 5.9 of the Covert Human Intelligence Source Code of Practice must be followed.

Related authorisations

115 If the action authorised refers to activity under a previous authorisation the Unique Reference Number (URN) and details of that authorisation (e.g. details of a vehicle which has a VTD fitted) should be given to enable the Commissioner to cross-refer. The authorising officer should ensure that what is being granted is not in conflict with previous or other current authorisations. Careful attention must be paid to the relationship between property interference and directed surveillance authorisations to ensure that the subsequent download, interrogation or use of the product from the property interference is clearly spelt out on the associated directed surveillance authorisation. Similarly, authorisations for directed surveillance should only permit the download, interrogation or use of product from interference on the condition that a valid PA97 authorisation exists.

The authorising officer must state explicitly what is being authorised

116 Section 32(5) of RIPA requires the authorising officer to describe and specify what he is granting. This may or may not be the same as requested by the applicant. For the benefit of those operating under the terms of an authorisation, or any person who may subsequently review or inspect an authorisation, it is essential to produce, with clarity, a description of that which is being authorised (i.e. who, what, where, when and how). The authorising officer should as a matter of routine state explicitly and in his own words what is being authorised, and against which subjects, property or location. Mere reference to the terms of the application is inadequate.

Authorisation different from Application

117 If an application fails to include an element in the proposed activity which in the opinion of the authorising officer should have been included (for example, the return of something to the place from which it is to be taken for some specified activity), or which is subsequently requested orally by the applicant, it may be included in the authorisation; if so a note should be added explaining why. Conversely, if an authorising officer does not authorise all that was requested, a note should be added explaining why. This requirement applies equally to intrusive surveillance, property interference, directed surveillance and CHIS authorisations.

Careful use of words

118 The authorising officer must be careful in the use of "or" and "and" in order not to restrict what is intended. For example, do not use "or" when "and" is meant (e.g. "deployment of .... on vehicle A or vehicle B" limits deployment to either vehicle, not both simultaneously or one after the other).

Duration of authorisations and renewals

119 Every authorisation must be for the statutory period, normally three months for surveillance authorisations and twelve months for CHIS authorisations. Thus a surveillance authorisation granted at 14:10 hours on 9 June will expire on 8 September at 23:59 hours. Urgent oral authorisations last for 72 hours. Authorisations for juvenile CHIS last for one month. For all authorisations the time period begins when the authorisation is granted, unless the prior approval of a Commissioner is required. In that case the period begins when written notice of the Commissioner's approval is received by the authorising officer. The fact that the operation to which authorisation relates is only expected to last for a short time cannot affect the authorisation period. An early review can take care of issues of continuing necessity and proportionality.

120 Renewals can only be granted before the expiry of the existing authorisation and take effect from the time of that expiry. This applies equally to renewals requiring a Commissioner's prior approval, provided that the authorising officer has received written notice of that approval before that time.

Dates of effectiveness - leaving date boxes blank

121 Because authorisations requiring prior approval will only be effective on receipt by the authorising officer of written notice of the Commissioner's approval, the date boxes should be

left blank until the decision has been received. If, for any reason, the authorising officer does not personally see a Commissioner's Prior Approval (for example, when a Chief Constable is out of the force area), receipt in the office of the authorising officer will suffice as an indication of the authorising officer having received written notice of approval. See paragraph 6.11 of the Covert Surveillance and property interference Code of Practice. The Commissioners require forces which adopt this procedure to notify the authorising officer, by an effective and auditable means, of any comments by the Commissioner when giving approval.

Dates of effectiveness - renewal information required by the OSC

122 The OSC must be notified of the effective to and from dates when the authorisation is renewed. Where a renewal requires a Commissioner's prior approval, the dates of effectiveness should be accompanied by a note from the authorising officer acknowledging that the dates are conditional upon receipt of approval before the expiry of the current authorisation.

The rank of the authorising officer should be provided

123 Every authorisation should show the rank of the person giving it. Designated Deputies must identify themselves as such and say why they are giving the authorisation. ACCs who are not Designated Deputies should state when it would next be reasonably practicable for the authorising officer or Designated Deputy to consider the application. Where a new Chief Constable or Designated Deputy is appointed, the OSC should be notified as soon as possible.

Renewals involving minor changes

124 Commissioners are content to treat as renewals authorisations where minor changes have occurred, e.g. the removal of a person or a vehicle from the investigation or the addition to the authorisation of previously unknown details such as a vehicle registration or a subject's identity, provided that the terms of the original authorisation allowed for such amendment. Where details in authorisations are amended at renewal, the reason for further identification or removing subjects or vehicles must be given.

The scope of an authorisation may not be broadened

125 Reviews and renewals should not broaden the scope of the investigation but can reduce its terms. Where other subjects may unexpectedly come under surveillance, authorisations can anticipate it by using words such as 'suspected of', 'believed to be' or 'this authority is intended to include conversations between any and all of the subjects of this investigation, including those whose identities are not yet known'. When the identities of the other criminal associates and vehicle details become known, they should be identified at review and in the renewal authorisation, so long as this is consistent with the terms of the original authorisation. Otherwise, fresh authorisations are required.

126 When an authorisation includes the phrase "... and other criminal associates..." a review or renewal can only include those associates who are acting in concert with a named subject within the authorisation (a direct associate). It does not enable "associates of associates" to be included, for whom a fresh authorisation is required.

127 Where a person or vehicle can be identified they must be. If, for example, a subject drives two known vehicles but has access to others and the property interference or intrusive surveillance

may take place on or in any of the vehicles, the wording of the authorisation must reflect this and the two known vehicles be specified in the authorisation, as well as a suitable formula to allow for deployment on as yet unidentified vehicles.

128 It is acceptable to authorise surveillance against a group or entity involving more than one individual (for example an organised criminal group where only some identities are known) providing that it is possible to link the individual to the common criminal purpose being investigated. It is essential to make explicit the reasons why it is necessary and proportionate to include persons, vehicles or other details that are unknown at the time of authorisation but once identified they should be added at review (see note 132). The authorising officer should set parameters to limit surveillance and use review to avoid 'mission creep'.

129 It is no longer necessary to notify the OSC in writing of the identification of any vehicle, property or person that could not be identified at the time authorisation was given. However, it is vital that details are recorded at the next review or renewal. It is wise to confirm in writing, at cancellation, the details of all property interfered with and persons subjected to surveillance (see note 141).

Authorising more than has been requested, more than is justifiable in the specific circumstances, or more than it is intended to use

130 Authorisations should state specifically covert activities or techniques likely to be required. It is recognised that it is not always possible, at the outset of an investigation, to foresee how it will progress. However, it is inappropriate to authorise property interference or covert surveillance techniques where they are not demonstrated to be necessary, or clearly not required, or where they would not be used until the investigation is more mature. The authorising officer may not authorise more than can be justified at the time and should demonstrate control and a proper understanding of proportionality, which relates to the method to be used, not only the seriousness of the crime or the convenience of those conducting covert surveillance.

131 The position is different for the tracking of vehicles or surveillance of persons "as yet unknown" (see notes 125 to 129) because in that case the tactic is identified but the precise vehicles are not.

132 Authorisations against a named subject should indicate when, where, and in what circumstances the surveillance is to be carried out.

What must be specified in authorisations (section 32(5) of RIPA and section 6(5) of RIP(S)A)

133 Intrusive surveillance authorisations must specify or describe (a) the type of surveillance, (b) the premises or private vehicle, and (c) the investigation or operation. For example, an authorisation for the use of an audio device could be for 'the monitoring and recording of conversations taking place between x and y at z address in connection with operation w, an investigation into drug trafficking.'

Crime other than specified in authorisation

134 Discussion by subjects of crimes other than such as are specified in an authorisation need not be disregarded.

Absence of authorising officer (section 94(1) of PA97, section 34(2) of RIPA and section 12(2) of RIP(S)A)

135 It is unlikely to be regarded as "not reasonably practicable" (within the meaning of sections of the Acts specified above) for an authorising officer to consider an application, unless he is too ill to give attention, on annual leave, is absent from his office and his home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not to be regarded as rendering it impracticable for an authorising officer to consider an application.

136 Where a designated deputy gives an authorisation the reason for the absence of the authorising officer should be stated.

Authorisations under section 93(3) of PA97: execution by another organisation

137 The absence of a collaboration agreement does not preclude the application seeking authorisation of actions by members of another organisation. This guidance is extended to RIPA and RIP(S)A.

Cancel at the earliest opportunity

138 If, during the currency of an authorisation, the authorising officer is satisfied that the authorisation is no longer necessary, he must cancel it. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. In the case of authorisations for property interference and intrusive surveillance, the authorising officer should, within four working hours of signing the cancellation, give notice to a Commissioner (which in practice means the OSC) that he has done so.

139 Authorisations may be cancelled orally. When and by whom this was done should be endorsed on the cancellation form when it is completed, and recorded on the Central Record of authorisations.

(See also Part 1, paragraph 27).

Cancellation – information required

140 It is not necessary to complete a separate form when it is decided at review or renewal not to continue the authorisation; properly designed forms should enable the recording of relevant details depending on the authorising officer's decision. Nor is it appropriate to simply sign to say that the authorisation is cancelled.

141 Although paragraph 5.18 of the Covert Surveillance and property interference Code of Practice is correct in saying that there is no *requirement* for any further details to be recorded when cancelling a directed surveillance authorisation, the Commissioners considered that it would be sensible to complete the authorisation process in a form similar to other parts of the authorisation where relevant details can be retained together. When cancelling an authorisation, the authorising officer should:

141.1 Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.

141.2 The reason for cancellation.

141.3 Ensure that surveillance equipment has been removed and returned.

141.4 Provide directions for the management of the product.

141.5 Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.

141.6 Record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

The use by one authority of another to conduct surveillance for a crime that it has no capability to prosecute

142 RIPA and RIP(S)A deal not with enforcement powers but the acquisition of information; there is no obligation to do something with the information collected. It is acceptable for one authority to use the services of another even if the requesting authority has no power or intent to use the product providing that the surveillance is necessary and proportionate to what it seeks to achieve. CHIS should not be exposed to unnecessary risk to obtain information that is unlikely to be used.

The use of external partners

143 When a person who is not an employee of the public authority is authorised to conduct covert surveillance, he is an agent of the public authority. This applies to private contractors or members of another public authority. The use and relevant qualifications and experience of a third party must be explicit in the application and authorisation. It is wise, if no collaboration agreement exists, to obtain written acknowledgement that they are an agent of the public authority and will comply with the authorisation. Third parties authorised by a public authority are liable to inspection by the Office of Surveillance Commissioners regarding their conduct in relation to the activity authorised.

Disclosure of techniques

144 A Surveillance Commissioner and an authorising officer can only authorise on the basis of what he has been told. Issues of disclosure should not inhibit the proper construction of applications and authorisations but can be dealt with at the appropriate time using existing procedures. Where necessary, authorisations should cross-refer to the intelligence report.

145 To comply with *R v Sutherland* the authorising officer should clearly set out what activity and surveillance equipment is authorised in order that those conducting the surveillance are clear on what has been sanctioned.

One public authority may not force the terms of an authorisation on another

146 One authority may request another to conduct covert surveillance on its behalf (see note 137) but it may not force those conducting the surveillance to act in a manner that is counter to their

beliefs or where the risk is unacceptable to them. If agreement cannot be reached then the requesting authority will have to find an alternative solution.

Requests to amend data

147 If an overt approach is made to the owner of data to amend data that he holds to prevent the compromise of a covert investigation (for example, amendment to flight manifests or delivery tracking details), property interference authorisation is not necessary. It would be prudent, however, for the request and amendments to be made in an auditable manner so that the data owner is appropriately protected.

The retention of applications with 'wet signatures'

148 The key signature is that of the authorising officer. If information technology is used to construct applications and authorisations, it must be capable of authenticating the user's identity (i.e. it must be protected from alteration and auditable) if hand-written signatures are not used. In the absence of authentication, hand-written (so-called 'wet') signatures are required. Authorisations with wet signatures may be retained by the authorising officer or centrally.

The meaning of Professional Legal Adviser

149 Legal privilege attaches to communications with a professional legal adviser (usually involving a contractual relationship). It would not normally apply to a Trade Union representative but would normally apply to a Barrister, Solicitor, Legal Executive or Solicitor's Clerk.

The design of forms

150 The Commissioners will continue to criticise the use of forms which do not require the authorising officer to fulfil his or her statutory responsibilities. Forms should enable authors to comply with legislation which requires an authorising officer to explain the details required by the legislation (see also notes 107 and 116). There are benefits to the adoption of a common design, but a public authority may amend forms if it encourages precision. The use of pre-scripted assertions is usually inadequate.

(See also 235)

Combined authorisations

151 Although an authorisation combining one or more types of covert activity is within the legislation, such contribution often causes error; for example directed surveillance can only be authorised for three months and a CHIS may only be authorised for 12 months and ensuring synchronised documentation is difficult. It should also be remembered that property interference and intrusive surveillance require separate authorisations because they are the requirements of different Acts. (See also note 191).

Retention of property

152 The principles of RIPA regarding the retention of property apply equally to PA97 (see Covert Surveillance Code of Practice paragraphs 1.2, 9.4 to 9.6 and 7.33 to 7.34).

The authorising officer should fully understand the capability of surveillance equipment

153 In order to give proper consideration to collateral intrusion, and to comply with *R v Sutherland,* the authorising officer must fully understand the capabilities and sensitivity levels of technical equipment intended to be used, and where and how it is to be deployed. An application which does not assist the authorising officer in this respect should be returned for clarification (see also 293).

154 The Commissioners are aware that some specialist equipment extracts automatically more data than can be justified as necessary or proportionate and may give rise to collateral intrusion. The inability of technology to restrict capability should not dictate the terms of an authorisation. If data is obtained that exceeds the parameters of an authorisation, the authorising officer should immediately review it and make arrangements for its disposal.

Those required to respond to tasking should see the authorisation

155 Where Technical Support Units or other officers are required to respond to tasking, they should see a copy of the authorisation and of any comments by a Surveillance Commissioner or authorising officer. For directed surveillance not involving the installation of devices, it is sufficient for the officer in charge of the surveillance team to see these documents and then to brief the team accordingly while taking care to repeat precisely the form of words used by the authorising officer. In the case of CHIS, the handler should not proceed until the authorisation has been seen. In each case there should be acknowledgement in writing (with date and time) that the authorisation has been seen.

Private information - Review of historical data

156 Section 26(2) RIPA does not differentiate between current and historical surveillance product. Sections 48(2) of RIPA and s.31(2) of RIP(S)A define surveillance as including "monitoring, observing or listening" which all denote present activity; but present monitoring could be of past events. Pending judicial decision on this difficult point the Commissioners' tentative view is that if there is a systematic trawl through recorded data (sometimes referred to as 'data-mining') of the movements of a particular individual with a view to establishing, for example, a lifestyle pattern or relationships, it is processing personal data and therefore capable of being directed surveillance if it contributes to a planned operation or focused research for which the information was not originally obtained.

157 The checking of CCTV cameras or databases simply to establish events leading to an incident or crime is not usually directed surveillance; nor is general analysis of data by intelligence staffs for predictive purposes (e.g. identifying crime hotspots or analysing trends). But research or analysis which is part of focused monitoring or analysis of an individual or group of individuals is capable of being directed surveillance and authorisation may be considered appropriate.

(Covert Surveillance Code of Practice 2.6 refers)

Biographical information does not satisfy the private information test on its own

158 Use of the term 'biographical information' appears to have resulted from the data protection case of *Durant v Financial Services Authority [2003] EWCA Civ 1746*. The Court of Appeal was construing the Data Protection Act 1998, which gave effect to the EC Directive in relation to the protection of personal data and its holding by data controllers. In construing the meaning of 'personal data' in s.1(1) of the Act, the Court held that one of the two notions which may be of assistance is "whether the information is biographical in a significant sense, that is going beyond the recording of the protective data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy would not be said to be compromised". It is important to note about this decision that:

158.1 s.1(1) defines 'personal data' by reference to individuals who can be identified from data: it is therefore obvious that 'personal data' is a different concept from private information;

158.2 it was not concerned with RIPA nor was the Court referred to the Strasbourg decisions in relation to private or family life.

158.3 'Private information' in RIPA s26(10) reflects private life in Article 8. 'Private life' has been broadly defined at Strasbourg to include professional and business activities.

159 It is dangerously misleading to seek to apply a court's tests for construing a term in one statute to the construction of a different term in a different statute, particularly when the statutes have different purposes, as these have. "Biographical information" which identifies a subject may be convenient shorthand for identifying some material which directed surveillance may disclose, but it does not cover, for example, a subject's relationships with others which are part of private and family life.

160 For example, a tracking device which shows a driver visiting his mistress's address, his children's school, his bank, or any other premises unconnected with crime is likely to give rise to a breach of Article 8 even though these details may not be "biographical information" as defined in *Durant*: it should therefore be authorised as directed surveillance if there is to be RIPA protection.

Central Record of authorisations

161 Paragraphs 8.1 to 8.3 of RIPA and paragraphs 3.14 and 3.15 of RIP(S)A Covert Surveillance Codes of Practice and paragraphs 7.1 to 7.6 of RIPA and paragraphs 3.13 to 3.16 of RIP(S)A CHIS Codes of Practice detail the requirements for a centrally retrievable record of all authorisations to be held by each public authority. Some aspects of covert policing are especially sensitive and require strict application of the 'need to know' principle (e.g. investigations into suspected police misconduct by a force Professional Standards Department, anti-corruption investigations and Special Branch operations). Authorisations (i.e. the document that provides the detail of the activity and the signature of the authorising officer) arising from these sensitive matters may be held in separate systems, away from the general run of authorisations, so long as they are centrally retrievable, are accessible to at least the Head of the Central Authorities Bureau (or equivalent unit), in order to ensure proper quality control, and

are made available for examination by the relevant Surveillance Commissioner or OSC Inspector.

162 Full compliance is no mere bureaucratic requirement but will allow the person responsible for the Central Record, at a glance, to exercise effective oversight and quality control. It will enable that person to identify when reviews, renewals and cancellations are due, which authorising officer is directly involved in any of the operations which they authorise, and will draw attention to investigations likely to involve confidential information.

163 There should be a single centrally retrievable record, preferably in a tabular or electronic format, which contains the information required by the legislation. This record must include references to all the covert activities authorised by a prescribed officer of the authority. Any specialist units applying the 'need to know' principle may retain their own authorisations but must record the Unique Reference Number and key details of the authorisation on the single Central Record.

164 It is acceptable to have a Central Record for all CHIS activity (other than those authorised by the Security Service) and a separate Central Record for all other types of covert surveillance. It is also prudent to maintain a record of PA97 authorisations for property interference in the same place as the record for intrusive surveillance.

165 Policing and Crime Act Section 23 collaboration agreements should make explicit provision for the proper keeping of a central record. In principle, the central record should be maintained by the force providing the authorising officer.

The use of template entries

166 Template forms inevitably lead to, or at least give the appearance of, minimal or no consideration of: (a) the nature and extent of the surveillance proposed and the justification for the use of the devices to be employed; (b) necessity; (c) proportionality; (d) collateral intrusion; and (e) what alternative methods have been considered. Template entries are therefore to be avoided or used with great care.

(See notes 100 to 102)

Overseas surveillance - Schengen Convention

167 Cross-border surveillance is now regulated under the Schengen Convention. Article 40.1 allows officers from one contracting party who are carrying out surveillance to continue that surveillance in the territory of another party where the latter has authorised the surveillance in response to a request for assistance. There are administrative provisions dealing with how and to whom requests for assistance should be made, and there is also provision for the surveillance to be entrusted to officers of the party in whose territory it is to be carried out. RIPA and RIP(S)A will apply in such a case in the UK.

168 Article 40.2 permits the officers carrying out surveillance in one territory to continue it across the border of another territory, where "for particularly urgent reasons" prior authorisation cannot be requested. This permission is subject to a number of conditions, including the requirement for officers to carry identification, make reports, etc. Those which seem significant are as follows:

168.1 Article 40.2 requires that the appropriate authority in the territory where the surveillance is being carried out should be notified immediately that the border has been crossed, and that a request for assistance should be submitted immediately, explaining the grounds for crossing the border without prior authorisation.

168.2 Article 40.2 further requires that the surveillance must cease as soon as the contracting party in whose territory it is being carried out so requests or, where no authorisation is obtained in response to the request mentioned above, five hours after the border was crossed.

168.3 Article 40.3.c provides that entry into private homes and places not accessible to the public is prohibited.

168.4 Article 40.3.d provides that the officers carrying out the surveillance may neither challenge nor arrest the person under surveillance.

Surveillance outside the UK (RIPA section 27(3))

169 Although under RIPA section 27(3) conduct may be authorised outside the United Kingdom, the application for such an authorisation calls for the exercise of judgment by the applicant because it could only be relevant in the United Kingdom (see note 192). In case of doubt it is good practice to apply for an authorisation.

Urgent oral authorisation (section 43(1)(a) of RIPA, section 19(1)(a) of RIP(S)A and section 95(1) of PA97)

170 For the purposes of sections 43(1)(a) of RIPA, 19(1)(a) of RIP(S)A and 95(1) of PA97, a case is to be regarded as urgent, so as to permit an authorisation to be given orally, if the time taken to apply in writing would, in the judgment of the person giving the authorisation, be likely to endanger life or to jeopardise the operation for which the authorisation is being given.

Use by officers of covert surveillance devices to confirm at a later date what has been said or done by another person (section 48(2) of RIPA and section 31(2) of RIP(S)A)

171 No matter that the status of the officer is obvious, this would be surveillance under section 48(2)(b) and (c), and covert since the person is unaware that it is taking place: section 26(9)(a). The Commissioners doubt whether section 2.29 of the Covert Surveillance and Property Interference Code of Practice is an accurate statement of law. The individual may well know that what they say has been passed to a public authority but they may not volunteer some information if it were known that what was said was being recorded. If there is no reason to suspect that the individual would object to a recording it should be made with their knowledge. Otherwise, a recording is capable of being construed as covert and should be authorised.

(See also note 263)

Length of applications

172 Applications for covert activity should be concise and should only contain material facts. This applies especially to intelligence cases.

173 The issue is one of balance, the object of OSC observations is not to restrict the information to be provided but to achieve a focus on what is really material and avoid burdening the process with information that is not relevant to the decision which is being made.

174 If it aids clarity and reduces reliance on powers of expression, sketches, annotated maps or photographs may be attached to documentation providing they are properly cross-referenced within the main document. Authorising officers should sign attached documents and ensure that there is adequate information to collate documents if they separate.

Serious crime (section 93(4) of PA97 and section 81(3) of RIPA)

175 An authorisation for property interference cannot be obtained for an operation that does not concern 'serious crime'. If there is uncertainty about whether or not crime is 'serious', it is good practice to seek an authorisation.

Notification signatures

176 Although it is desirable, it is not necessary for a written notification to a Commissioner to be signed. The name of the authorising officer must always be clearly stated.

Collateral Intrusion

177 When notification of property interference is made to a Commissioner, details of any collateral intrusion that may result as part of it or from use of any equipment put in place must be made known to the Commissioner at the same time. Such matters should be included in the application.

Renewals for property interference and intrusive surveillance must specify all actions taken

178 Commissioners do not see review forms so it is important that renewals for property interference and intrusive surveillance summarily specify all actions taken and material discovered since the previous authorisation was granted.

Continuing interference (sections 92 and 93(1)(a) of PA97)

179 The continuing presence of a surveillance device placed on any private property, including dwellings, hotel bedrooms and private or hired vehicles, is to be treated as a continuing interference. The wording of PA97 (and RIPA or RIP(S)A)) authorisations for surveillance equipment must cover its continued presence.

180 In the event that surveillance equipment is considered to be *lost*, and if all attempts to locate the equipment have been exhausted, the existing property interference authorisation and any associated authorisation may be cancelled. The Chief Surveillance Commissioner should be informed immediately in writing. Should the equipment's location subsequently be identified, a new property interference authorisation should be granted to enable the removal of the equipment as soon as its location is known and the Chief Surveillance Commissioner informed.

181 In the event that equipment is *irretrievable* a property interference authorisation should remain extant until its recovery is possible and any other surveillance authorisation should be cancelled. In extraordinary circumstances, when recovery is unlikely within a reasonable period, the Chief Surveillance Commissioner should be informed in writing detailing the circumstances and requesting permission to cancel the property interference authorisation. In this circumstance, interference continues but the equipment is not being authorised for the purpose of surveillance. If an opportunity to recover the item appears, a new property interference authorisation should be granted. As soon as the equipment is recovered the Chief Surveillance Commissioner should be informed in writing.

Property details (Paragraphs 7.6 and 7.7 Covert Surveillance and Property Interference Code of Practice)

182 Interference is 'properly authorised' when all property that may be interfered with is identified. It is important that any entry to surrounding property needed to achieve the objective is defined as clearly and as narrowly as possible. A Commissioner will not regard anything that is not specifically mentioned in the authorisation as being authorised.

183 When describing land to be entered, care should be taken to provide Commissioners with sufficient detail to permit the land to be clearly identified (e.g. O.S. grid references with plans showing them and the relevant land).

The effect of section 48(3)(c) RIPA

184 Surveillance is defined to exclude the product from the interference with property. Searching a vehicle or baggage or placing a device in or on property is interference with it but is not itself surveillance. There is a difference between activity which a trial judge may consider *'de minimis'* and continuing interference which may provide a profile over time. The use of product from interference may be surveillance and should be separately authorised.

(See also 202).

Specify the interference

185 Property interference authorisations must specify the interference. For example, a search would be authorised as 'entry into x address and the recording or copying of any contents believed to be relevant to the investigation into the murder of y'.

186 Interference relates to the deed and is not confined to the purpose. Therefore, there is an expectation of authorisation when property is interfered with during feasibility studies or reconnaissance.

Property interference outside designated operational areas of responsibility when no written collaboration agreement exists

187 All that can be authorised outside a force area is the maintenance and retrieval of equipment. Entry on private land is not covered. Removal of a Tracking Device to replace its batteries or redeployment of identical equipment amounts to maintenance of the equipment, rather than replacement, and so can take place outside the authorising officer's force area, provided that the maintenance was authorised originally. If a property interference authorisation is intended

to cover maintenance and retrieval outside the authorising force area, the authorising officer must specify this: see PA97 (as amended) section 93(1)(a). This only extends to entry onto public land to carry out these actions. If entry onto private land outside the authorising officer's force area is required, the authorising officer of the force area within whose area the land lies must give the authorisation.

188 Any other interference with property or any entry on to private land cannot be authorised outside the force's own area. Any such authorisation has to be sought from the authorising officer of the area concerned. Authorisations from outside forces, in particular when property interference is sought, should be accompanied by the supporting directed surveillance authorisation, technical feasibility reports and a comprehensive map indicating where deployment is to take place.

The use of tracking devices

189 Attaching or placing a tracking device onto, or remotely obtaining information about the location of, property without the consent of the owner and when the property is not owned by the investigating authority is interference with property. The usual need to relate the location data obtained by the device to other information causes a potential and foreseeable invasion of privacy even if the location data is historical. In these circumstances it is necessary to obtain a property interference authorisation (to interfere with the property) and usually a directed surveillance authorisation (to make effective use of the product).

(See also note 184)

Tracking devices and surveillance equipment within public authority vehicles

190 Placing tracking devices or surveillance equipment in or on vehicles owned by the public authority entails no property interference by the authority. The activity is unlikely to be regarded as covert if the staff using the vehicle are appropriately notified that they are in place for the purpose of recording vehicle movements and may also be used for evidential purposes should the need arise. If tracking devices, or equipment capable of being used for surveillance purposes (including the remote activation of public authority owned equipment), are used for a purpose not notified to the vehicle occupants this use is covert and an appropriate authorisation should be sought.

Separate authorisations for each property interfered with

191 Separate authorisations are normally required for each property entered or interfered with in order to ensure that full consideration is given to whether each interference is warranted. The only exceptions are:

191.1 where all the properties concerned are owned by the main subject under investigation and it makes administrative sense to combine them. This may cover searches of rubbish at more than one address, if the main subject frequently moves home, or entry on property in order the carry out a feasibility study and subsequently or at the same time deploy technical equipment. However it is not good practice to combine authorisations where part may require cancellation whilst part continues to be needed. Thus a private dwelling and a vehicle, even if belonging to the same person, would require separate authorisations.

191.2 where a subject has access to more than one vehicle, in which case the application can cover as many vehicles as is necessary, if such a wide authorisation is shown to be needed. Such authorisations will normally only cover one subject unless more than one subject uses the same vehicles. All vehicles must be identified whenever it is possible to do so.

191.3 where an operation requires entry on or interference with more than one property in order to achieve the main objective, for example when officers need to cross various pieces of land to reach the property they wish to enter or interfere with, or where there is a need to enter private land to attach a tracking device.

191.4 where a subject is expected to book into one of two or more hotel rooms or two subjects are likely to book into different rooms in the same hotel.

191.5 where persons are suspected of joint involvement in a criminal enterprise, unless it is foreseen that an authorisation in respect of one suspect may need to be cancelled before that in respect of another.

(See also note 151).

Overseas surveillance - subject nationality

192 An authorisation under RIPA is required whenever surveillance is carried out overseas by law enforcement agencies either directly or by others on their behalf. But where a subject is neither a UK national nor likely to be the subject of criminal proceedings in this country, and the conduct under investigation would neither affect a UK national nor give rise to material likely to be used in evidence before a UK court, such authorisation is not required.

Overseas deployment of Vehicle Tracking Devices

193 If a vehicle is expected to be travelling through several countries, it is sufficient for the authorisation to state that the deployment has the approval of the host countries without need for an authorisation for each country. If maintenance or retrieval of surveillance equipment whilst the vehicle is overseas is foreseen then the authorisation should enable this action to be taken.

Extra-territorial offences

194 In relation to offences committed abroad, any actions under the provisions of Part III of PA97 may be undertaken in the United Kingdom only where the serious crime, in the prevention or detection of which such surveillance is likely to be of substantial value, consists of conspiracy to commit offences outside the United Kingdom [see sections 5, 6 and 7 of the Criminal Justice (Terrorism and Conspiracy) Act 1998].

195 Section 27(3) of RIPA provides that the conduct which may be authorised under Part II includes conduct outside the UK. A request for authorisation for surveillance in a Convention State would therefore be competent in terms of UK legislation. However, Article 40 of the Schengen Convention clearly restricts surveillance in the territory of any Convention State and Article 40.3.c, in particular, restricts intrusive surveillance. If any request for authorisation for surveillance in such a State which is party to the relevant provisions of the Convention is made,

it should make clear how the surveillance is to be carried out consistently with the Convention, and what steps are being taken to request assistance from the State in question.

Urgent prior approval cases

196 A case is to be regarded as one of urgency within the meaning of the statutory provisions where either (a) the time taken to apply for the approval of a Commissioner, or (b) the further delay following at least one unsuccessful attempt to communicate with a Commissioner, or (c) inability to communicate securely with a Commissioner on account of mechanical failure, would in the judgment of the authorising officer, be likely to endanger life or jeopardise the operation in connection with which the surveillance is to be undertaken. A decision to give an authorisation under these circumstances must be notified to a Commissioner as soon as practicable after it is taken even if this is outside normal working hours (but not between 11pm and 7.30am).

Urgent oral authorisations – recording

197 Paragraph 5.9 of the Covert Surveillance and Property Interference Code of Practice extends RIPA to include the requirement for the authorising officer as well as the applicant, when using the urgency provisions, to record the details set out in that paragraph. The Covert Human Intelligence Source Code of Practice (paragraphs 5.11 and 5.12) requires less information to be required and then only by the applicant. The Commissioners advise that, in addition to the details set out in the codes of practice, the key issues of necessity, proportionality, collateral intrusion and explicitly what has been authorised should be recorded by both parties.

198 Both codes require an urgent oral authorisation to be recorded when "reasonably practicable". The Commissioners advise that notes are made contemporaneously. If, at a later stage, the oral authorisation is recorded in another form (e.g. electronically) care should be taken to copy the contemporaneous notes precisely and not refer to the decision in the past tense. The same considerations apply to the notes and formal records completed by the applicant.

What constitutes 'property' and 'interference' (section 92 of PA97): keys, shoes, baggage searches and computer passwords

199 'Property' includes personal property such as keys and mobile phones.

200 If a computer is set up to work with a password, interference with the password requires an authorisation for property interference. An authorisation under Part III RIPA will be necessary if the owner is required to disclose the password.

201 Taking shoes away for prints is interference, unless authorised under another enactment, whereas taking impressions left after a person has trodden on a mat would not be, provided, of course, that access to the mat was lawful.

202 Deliberately holding up other people's baggage in order to avoid the suspicion of the subject as part of the operational plan to search his luggage constitutes interference. The activity may be considered *'de minimis'* by a Trial Judge but it should be referred to in authorisations.

203 If software is installed in the computers in an internet café with the consent of the owner in order to determine when a known password is entered, an authorisation for property

interference is not required, as the persons using the consoles do not have ownership of this property.

Interference (section 97(2)(a) of PA97)

204 Touching or pushing a door or a window, or putting a probe into a lock of a dwelling, office or hotel bedroom constitutes interference with that property and requires a Commissioner's prior approval before being undertaken.

Multiple vehicles

205 An authorisation may be expressed to permit interference with any vehicle which the subject may use and any vehicle into which the goods targeted may be transhipped. But such a formula should not be used except in relation to vehicles that cannot be further particularised.

(See also 125 to 129)

Boats

206 Where it is possible that crew members of a boat may change, it is only necessary to name the owner in an authorisation relating to it.

Placing a device in a vessel (section 97(2)(a) of PA97)

207 Where devices are located on parts of a vessel which, arguably, are not used as a dwelling, (such as the engine room) the safer course is nevertheless to seek prior approval.

Covert search of residential premises or a private vehicle and of items found therein (section 26(3) of RIPA and section 1(3) of RIP(S)A)

208 When a covert search of a residential premise or private vehicle is authorised under PA97 Part III a separate authorisation for intrusive surveillance may be required. Taking property out of those locations simply for the purpose of obtaining information or data before returning them is to conduct surveillance *in relation to* activity which has taken place in those locations.

The use of surveillance devices on police property, in places of detention or custody and places of business of a professional legal adviser

209 Covert surveillance carried out in relation to anything taking place on so much of any premises specified in paragraph 4.18 of the Covert Surveillance Code of Practice as is, at any time during the surveillance, used for the purposes of legal consultation, shall be processed in the same way as intrusive surveillance and requires the prior approval of a Surveillance Commissioner. Surveillance carried out in these places when they are unlikely to be used for the purpose of legal consultation, should be authorised as directed surveillance.

210 Ordinarily a subject should have been interviewed before there is any recourse to listening devices, unless the authorising officer believes that further interview(s) will not progress the investigation.

211 When approval is sought for the deployment of surveillance equipment in a room on police premises that has been allocated exclusively to another party for their permanent use (e.g. a solicitors' room), it may be expedient to seek a property interference authorisation and a directed surveillance authorisation.

Police cells and prison cells (section 97(2)(a) of PA97)

212 No authorisation for property interference is needed for the placing of an audio or video device in a police or prison cell, provided that verifiable consent has been given by the Chief Constable of the appropriate force or by the officer in charge of the cell area.

Items seized under PACE

213 Items seized under PACE should not be covertly opened or searched without a property interference authorisation, because seizure does not make a package the property of the arresting officers. A separate authorisation for directed surveillance will usually be required.

Examination of mobile telephones

214 Section 32(9)(b) of PACE, which does not apply to persons not arrested, allows a constable to retain anything not subject to legal privilege if he has reasonable grounds to believe that it is "evidence of an offence or has been obtained in consequence of the commission of an offence". This provision relates to offences already committed. It cannot extend to anything believed to reveal useful intelligence, the gathering of which will usually be at least part of the purpose of the examination. Section 54(5) of PACE requires that where anything is seized, the person from whom it is seized shall (except in two specified circumstances) be told the reason for the seizure. Ordinarily the purpose will be considerably wider than officers would want the suspect to be told. The examination of any mobile telephone will generally be likely to lead to the acquisition of at least some private information. For these reasons, before examining a mobile telephone covertly it is prudent to obtain authorisations for both property interference and directed surveillance. The authorising officer must be explicit when completing the authorisation regarding what is allowed (e.g. view or extract) and what is to happen in specified circumstances (e.g. when texts or voicemail arrive). Simple references to "examination" or "interrogation" are insufficient. The Commissioners' view is that authorisations cannot in general authorise the opening of unread messages or texts.

215 The Commissioners are aware that technology is capable of automatically downloading data even though there is no requirement for that data. If it is not possible to control what is downloaded, the use of such equipment should be avoided or the authorising officer should restrict the use of product obtained.

(See also 154)

Refuse in dustbins (section 92 of PA97)

216 Refuse made available by the occupier of premises for collection by the local authority in dustbins or disposable bags or any other container, whether on private property or in the street, is to be regarded as having been abandoned by the occupier only in favour of the local authority, and it accordingly remains "property" within the meaning of the section.

Items or samples discarded in a public place

217 Where a subject discards an item belonging to him that the police may wish to retrieve in a public place (e.g. for DNA analysis) an authorisation for property interference is not required if the proper inference is that it has been abandoned. However, if a DNA sample is to be taken from property owned by another (for example a glass in a public house) it would be prudent to obtain the consent of the owner of the glass or seek authorisation if such an event could reasonably have been foreseen.

Surveillance devices installed in moveable property

218 Where a surveillance device installed within moveable property (e.g. a parcel or a briefcase) is to be taken into private property or a private vehicle, an authorisation for the 'entry' of the device into those premises or the vehicle should be obtained. If the premises are either a dwelling or a hotel bedroom, prior approval of a Commissioner will be required. If the device is to be put into movable property without the property owner's consent, then an authorisation for the installation of the device should also be obtained.

219 An authorisation for intrusive surveillance need not be obtained just in case a device contained within movable property (e.g. a parcel or a briefcase) ends up in residential premises or a private vehicle. The possibility of a surveillance device being introduced into either of these places must be considered at the outset of the operation and a realistic view taken about the need for such authorisation. If the device is purely for the tracking of an asset (e.g. a drugs parcel) in order not to lose 'sight' of it, and the data is not going to be used for evidence or to assist in the construction of intelligence, an authorisation may not be required.

Substantial financial gain (section 93(4)(a) of PA97)

220 "Substantial financial gain" is not defined in either of the Acts. Had Parliament intended this to be a fixed amount for every case it would have said so. In each case it is a matter of judgment by the authorising officer whether, taking into account all of the circumstances, the resulting gain is substantial.

221 What is to be considered is belief about resulting gain, not resulting profit. A drug supplier who buys drugs for £500 and sells them for £1,000 gains £1,000 from his supplying. The view may be reasonably taken that a burglar who steals jewellery valued at £1,000 gains £1,000, whether or not he then sells it for £100 or throws it away and whether or not what he throws away is recovered and returned to the loser.

222 In most cases the gain will be that of the offender(s), but gain to others criminally involved is material if it is believed to result from the conduct in question.

Victim communicators

223 When victim communicators or couriers are used in a kidnap or extortion situation, and surveillance equipment is deployed, a RIPA/RIP(S)A authorisation may not be required but, as so much depends on whether or not a crime is in fact being committed and on the scope of the surveillance being proposed, it would, in most cases, be prudent to obtain the appropriate RIPA/RIP(S)A authorisation.

Dwelling (section 97(2)(a) of PA97) and residential premises (section 48(1) of RIPA and section 31(1) of RIP(S)A)

224 PA97 concerns dwellings; RIPA and RIP(S)A concern residential premises. In both cases authorisation for property interference is required and, in the case of dwellings, prior approval of a Commissioner is necessary. The Acts are concerned with use at the time, not permanence.

224.1 Dwelling. Prior approval is necessary where any of the property specified is used wholly or mainly as a dwelling (i.e. as a place of abode). Authorisation is therefore necessary for caravans, houseboats, yachts, railway arches, walkers' hides, tents and anywhere else believed to be used as a place to live. An integrated house garage should be regarded as a dwelling. The parts of the premises subject to interference should be specifically identified in the authorisation.

224.2 Residential Premises. Authorisation for intrusive surveillance is necessary for activity on residential premises involving the presence of an individual or a surveillance device. Hospital wards and police cells are likely to be residential premises but gardens and driveways are not. The parts of the premises subject to interference should be specifically identified and this will determine whether authorisation for intrusive or directed surveillance is appropriate. A lorry with sleeping accommodation should be regarded as residential premises requiring authorisation for intrusive surveillance. Absent any sleeping accommodation, authorisation for directed surveillance will usually suffice for a lorry.

Hotel bedrooms (section 97(2)(a) of PA97)

225 Property interference authorisation should be given and the prior approval of a Commissioner obtained for any interference with or entry into a hotel bedroom, whether devices are installed before or after allocation, signing the register or entering the room. Even if a device is fitted with the consent of the hotel owner or manager prior to the subject(s) taking occupancy, a property interference authorisation and the prior approval of a Commissioner are still required for the continued presence of the device and any servicing or retrieval of it whilst the room is allocated to the subject.

Interference with leased premises

226 Property leased to a public authority by tenancy agreement does not make the public authority the owner. Without the consent of the owner, the fabric of such property may only be interfered with (for example by way of installing a listening device or drilling a hole to insert a probe to monitor neighbouring property) after authorisation for property interference and an associated intrusive or directed surveillance authorisation.

Repeat burglary victims and vulnerable pensioners

227 While the consent of the owner to the installation of a surveillance device on his premises avoids the need for a property interference authorisation, the authorising officer should consider whether it is likely that the privacy of another person lawfully on the premises may be invaded. Any visitor who is not made aware of it is subject to covert surveillance. This is a technical breach of the visitor's Article 8 rights, although in such circumstances any complaint may be regarded as unlikely.

228 The surveillance is intrusive because it is carried out in relation to things taking place on residential premises: s.26(3)(a). But if the crime apprehended is not "serious", intrusive surveillance cannot be authorised: cf s.32(3)(b). On the other hand, the surveillance is not directed, because it is intrusive: s.26(2).

229 The fact that particular conduct may not be authorised under RIPA or RIP(S)A does not necessarily mean that the actions proposed cannot lawfully be undertaken, even though without the protection that an authorisation under the Acts would afford.

Binoculars and cameras (section 26(5) of RIPA and section 1(5) of RIP(S)A)

230 If binoculars or cameras are used in relation to anything taking place on any residential premises or in any private vehicle the surveillance can be intrusive even if the use is only fleeting. It will be intrusive "if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle". The quality of the image obtained rather than the duration of the observation is what is determinative.

Stolen vehicles (section 48(1) of RIPA and section 31(1) of RIP(S)A)

231 A stolen vehicle is not a 'private vehicle' for purposes of the Acts because a private vehicle is defined by these provisions by reference to use by the owner or person who has the right to use it.

Automated Number Plate Recognition and CCTV

232 The 'private life' of a car driver is not interfered with because the registration number of his vehicle is recorded by ANPR while he is travelling on a public road. That is because the registration plate is a publicly displayed object. But it is not adequate to say that this is so because the occupants of the car are in a public place: they are, but they are ignorant of the technology which is capable of identifying them and their movements or the extent to which the data may be retained and used. Because ANPR is now capable of producing clear images of the occupants of a car, as well as of its registration number, private life may be interfered with. If the occupant is in a private vehicle it may constitute intrusive surveillance if data that is recorded for potential later use is capable of identifying the occupants.

233 Tracking the movements of a specific vehicle or person (persistently or intermittently) over a protracted period or distance, when no action is taken to stop the vehicle or individual when first sighted, is capable of being directed surveillance and an authorisation should be obtained. If the details of persons or vehicles are placed on a list requiring that an investigating officer be notified or a record is made of the location or movements of the person or vehicle, or that vehicle or person is subjected to focused monitoring to build up a picture of the movements of the vehicle or person, an authorisation would be expected.

Premises set up to monitor traders covertly

234 Premises set up solely for surveillance purposes and not occupied or in current use for residential purposes are not residential premises within s.26(3)(a) of RIPA and surveillance carried out there is therefore not intrusive but may require authorisation for directed

surveillance. The position would be otherwise if a variety of defects were deliberately set up in premises which continued to be occupied for residential purposes (sometimes referred to as a 'house of horrors'). In some cases a CHIS authorisation may afford protection and merits consideration depending on the facts.

Authorisation for Undercover Officers (section 29(4)(b) of RIPA and section 7(5)(b) of RIP(S)A)

235 More than one Undercover Officer, Test Purchase Operative or Covert Internet Investigator or other person within the definition of a CHIS (i.e. s26(8)) can be included in a single CHIS authorisation, provided they are individually identified by pseudonym or otherwise from the outset. If their identity is not yet known, they cannot be included at this initial stage.

235.1 A risk assessment must be completed, pertinent to each individual, which takes into account all the circumstances of the environment in which each is to be deployed and the relevant experience of each operative.

235.2 In all incrementally phased operations where multiple operatives have been authorised at the outset, the authorising officer should be notified by way of review and an up-dated risk assessment carried out when each individual CHIS enters the operational arena.

235.3 Where it is not possible at the outset to identify further officers who are to be deployed, or where an additional unanticipated CHIS(s) is later to take part, they must be subject to an individual risk assessment and must be authorised for twelve months from the time they are deployed. Public authorities can choose to run individual CHIS authorisations in tandem with the original authorisation, paying particular attention to the requirements of separate review and renewal periods or, can cancel the original authorisation and start with a fresh twelve month authorisation. The new authorisation can then incorporate all CHIS operatives who have been identified and deployed.

235.4 The authorisation for the use or conduct of each operative included within a single generic authorisation will cease at the time the use or conduct of the individual operative is no longer necessary and proportionate. This should be reflected in the review process. Cancellation of the original authorisation for all operatives should in any event take place at the end of the statutory twelve month period, irrespective of the time an operative is engaged in the operation as a CHIS. Should an operative(s) be the subject of a renewal authorisation and be specifically identified for this purpose, this should be reflected within the cancellation of the original authorisation.

Risk assessments should be completed for each CHIS

236 If the authorising officer is properly to consider risk, this should reflect all other covert activities in which that officer has been engaged and the level of experience and training the officer has received. This is particularly relevant if the CHIS comes from a different force, public authority or third party. Police collaboration agreements should make arrangement for these details to be made available.

(See also note 237).

Recording Undercover Officer details

237 It is important that the authorisation makes it clear that it is authorising one or more CHIS and that there should be some way of referring to them that does not compromise the Undercover Officer. The use of a pseudonym should suffice but the authorising officer should be able to link the pseudonym to an identifiable individual so that he can make a proper risk assessment.

Use of directed surveillance for a prospective CHIS

238 An assessment of suitability is not usually an investigation of crime under PA97 or any of the other reasons cited in RIPA s.28(3) or 29(3) and the Scottish equivalent. Although the use by a police force of covert surveillance to assess the suitability of a person to act as a CHIS cannot usually be authorised under RIPA or RIP(S)A, it should be capable of being justified under Article 8.2 of ECHR.

Pre-authorisation meetings with prospective CHIS

239 Historical debriefing may not normally require an authorisation but any tasking to establish or maintain a relationship for a covert purpose in order to test reliability may and should be kept under review by an authorising officer with appropriate log entries. In principle, it may be better to authorise early and then cancel, if it is later decided not to progress with the CHIS use and conduct, than it is to jeopardise the admissibility of evidence because an authorisation was not obtained. This should not be confused with the assessment of CHIS suitability where no tasking is involved (see also note 238).

240 'Historical debriefing' in this sense means setting out to obtain information which it is believed is already known by the person before initial contact. If the person, as a result of discussion with a public authority, obtains information, as a result of a relationship, which he knows or perceives to be of interest to the public authority, may require authorisation.

241 When an individual is rewarded for, or an intelligence report is submitted relating to, information which is used or disclosed in a manner calculated to ensure that the person(s) being reported on are unaware of the use or disclosure in question, the need for authorisation should be seriously considered.

Adult CHIS (including Undercover Officers and those authorised to participate in crime) require a full 12 months' authorisation

242 All written authorisations for CHIS, of whatever kind, should be of 12 months' duration: cf. section 43(3) of RIPA and s.19(1(b)) of RIP(S)A. Reviews, on the other hand, may be conducted at whatever frequency the authorising officer deems appropriate (juvenile CHIS require one month authorisation).

Participating CHIS - level of authorisation

243 The legislation prescribes the minimum rank or grade for an authorising officer granting the use of a CHIS. Some public authorities, in a desire to supervise this type of CHIS more closely, have stipulated a higher rank or grade officer. The legislation enables this but it does not enable an adjustment to the length of an authorisation and the authorising officer may not delegate all or part of his or her statutory responsibilities. In other words there can only be one

authorising officer per CHIS at the same time and that person must be responsible for all aspects of use and/or conduct until that specified conduct (i.e. participation) is cancelled.

244 The Commissioners will not criticise an arrangement that retains the rank or grade of an authorising officer at the minimum prescribed level but which requires the authorising officer to inform a more senior officer of the necessity and proportionality of the use of the CHIS in this way. This will enable the senior officer to consider the corporate risk to the organisation (not the risk to the CHIS or the tactics involved) which will enable the authorising officer to make an informed risk assessment. It is imperative that the senior officer does not interfere with the authorising officer's statutory responsibilities by providing direction regarding authorisation.

CHIS – sub-sources and conduits

245 Where the identity of a sub-source is unknown and information said to have been obtained from him/her is passed on to a public authority by a conduit, without the knowledge of the sub-source, the conduit is maintaining a covert relationship with the sub-source and should be treated as a CHIS.

Covert Internet Investigations - e-trading

246 CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage.

CHIS should not be dual authorised

247 The Covert Human Intelligence Source Code of Practice paragraph 2.8 refers to the potential that a single CHIS "may be subject of different use and conduct authorisations obtained by one of more public authorities" and that "such authorisations should not conflict."

248 A public authority is not entitled to regard a CHIS as its own agent unless it has authorised him or her. For authorisation to be proper it must be given by an organisation with a single system of management. Put another way, there cannot properly be dual authorisation of an individual using more than one authorising officer or more than one authorisation for use: the risk of overlap and confusion is obvious and to be avoided. It is possible for an individual to be subject to different conduct authorisations proposed by different public authorities, but a wise authorising officer will endeavour to keep the number of simultaneous authorisations to a minimum by way of review (cancelling and combining conduct authorisations when appropriate).

249 The principle of minimising the number of authorising officers and authorisations for a single operation or investigation also applies to authorisations to interfere with property, directed surveillance authorisations and section 49 notices.

250 Covert Internet Investigators may establish or maintain a relationship with more than one individual in relation to different investigations. If it is not possible to construct a single authorisation to cover all of the relationships (because the persons with whom relationships are established are not known in advance) it will be necessary to construct for each person with whom a relationship has been established a separate authorisation each of 12 months duration. It is important that the same authorising officer considers each authorisation to ensure

that operational conflict and risks do not develop, and to monitor the security and welfare of the CHIS. When appropriate, reviews should be combined to establish whether separate authorisations can be combined into a single authorisation to reduce bureaucracy and error.

Test Purchase of sales to juveniles

251 When a young person, pursuant to an arrangement with an officer of a public authority, carries out a test purchase at a shop, he may be a CHIS (see paragraph 2.12 of the CHIS Code of Practice). It does not follow that there must be a CHIS authorisation because designated public authorities are empowered but not obliged to authorise a CHIS and it may be useful to keep the young person out of the direct evidential chain. But if the same individual is used to conduct a test purchase in the same establishment repeatedly, a CHIS authorisation should be obtained. If covert technical equipment is worn by the test purchaser, or an adult is observing the test purchase, it will be desirable to obtain an authorisation for directed surveillance unless the authorising officer is certain that private information is not likely to be obtained about any person subject to surveillance (see also note 269 and Surveillance Code of Practice paragraphs 2.5 and 2.6) and such authorisation must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person and desirable in relation to an adult.

252 When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises.

253 There is a difference between test purchases to establish whether juveniles are sold goods illegally and a test purchase conducted by a law enforcement officer for the sale of drugs or stolen items. The latter is more likely to require authorisation for the use and conduct of a CHIS. The authorisation always relates to the CHIS relationship and not the operation.

Handlers and Controllers must be from the same investigating authority as the authorising officer if no joint working agreement exists.

254 Paragraphs 6.10 to 6.13 of the RIPA CHIS Code of Practice relate to authorisations for the use or conduct of a CHIS whose activities benefit more than a single public authority. In circumstances where a single public authority is the beneficiary of the product obtained from a CHIS, the persons prescribed at section 29(5) of RIPA and section 7(6) of RIP(S)A (usually referred to as the controller and the handler) must be from the same investigating authority as the authorising officer unless, in the case of specified law enforcement agencies, an agreement exists under section 23 of the Policing and Crime Act 2010 which enables alternative arrangements.

255 The authorising officer should carefully consider whether the simple passing of information resulting from a CHIS report is benefiting after the event or whether the benefit is contemplated at the time of authorisation. The Commissioners caution against the term 'beneficiary' being used as a convenience to share resources.

256 If a Test Purchase Officer or Undercover Officer is accompanied by a cover/welfare officer the latter cannot fulfil the obligations under s.29(5)(a) if there is no written collaboration agreement enabling it.

Joint Working – CHIS authorisations

257 The principles of authorisations subject to a collaboration agreement set out in paragraph 3.16 of the RIPA Directed Surveillance and Property Interference Code of Practice should be considered applicable to an authorisation for the use and conduct of a CHIS.

Local Authority CHIS

258 A local authority may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed (see CHIS Code of Practice 6.12). In the absence of such an agreement the local authority must be capable of fulfilling its statutory responsibilities.

259 Elected members and Senior Responsible Officers (see paragraphs 3.26 and 9.2 of the CHIS Code of Practice) are required to ensure that policies are fit for purpose and that authorising officers are competent. An elected member has no need to know the identity of a CHIS nor have access to the product of the use of a CHIS nor know the detail of conduct authorisations. Chief Executives should usually provide elected members with a copy of OSC inspection reports, redacted if necessary.

260 Some local authorities may not wish to use CHIS and may in practice avoid authorising CHIS. However, all such local authorities should recognise that the occasion may arise when a CHIS appears unexpectedly and has to be authorised and managed. Consequently all local authorities must be equipped with a policy and the awareness training to recognise status drift and to manage anyone who has become a CHIS. It is the responsibility of the Senior Responsible Officer to ensure competent officers exist for such purposes (see CHIS Code of Practice 9.1).

The use of terms other than CHIS

261 The legislation does not envisage a different management regime for different types of CHIS. The term 'Tasked Witness' is sometimes used to identify a particular type of CHIS who is willing to testify in court and police officers are variously undercover, test purchase, decoy or covert internet investigators. All types are entitled to all the safeguards afforded a CHIS and the public authority must provide them, including proper considerations for, and completion of, authorisations and risk assessments although some of the factors for consideration, for example when making a risk assessment, may differ as between a CHIS who is an employee of a public authority and one who is a member of the public.

CHIS- remote contact

262 Other than in exceptional and explained circumstances, it is important that regular face-to-face meetings form the primary method for meeting a CHIS rather than remote contact (for example by telephone, text messages or email). The authorising officer should question, on review and renewal, why reasonably frequent face-to-face meetings are not being conducted.

Monitoring of CHIS meetings

263 If it is deemed necessary and proportionate covertly to record meetings with a CHIS an authorisation should be obtained.

264 Overt recording of meetings with a CHIS may be made but the product should be properly recorded, cross-referenced and retained. The authorising officer should assess and manage the risk of disclosure of audio recordings which may result in the compromise of the identity of the CHIS.

Undercover Officer - legend construction

265 During the construction of a legend an officer may establish or maintain a relationship with another person who is not the subject of an operation. The nature of that relationship may be for a covert purpose. It will be covert if it is not clear to the other person that the officer is not who he claims to be. The purpose may be to facilitate access to the subject of an operation or to facilitate *bona fide* checks later. If the relationship is for a covert purpose, and the activity relates to a current operation, an authorisation should be obtained. Where the legend is being prepared for possible later use an authorisation may not be necessary. Appropriate arrangements should be in place to manage 'status drift'.

Repeat voluntary supply of information

266 Some individuals provide information but do not wish to be registered as a CHIS; others repeatedly provide information that has not been sought or where the authority does not wish to authorise the individual as a CHIS (e.g. because there is evidence of unreliability). If the information being provided is recorded as potentially useful or actionable, there is a potential duty of care to the individual and the onus is on the authority to manage human sources properly. The legislation is silent regarding consent but sensible procedures should exist to monitor for status drift and to provide the trial judge with a verifiable procedure. Authorising officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose as described in paragraphs 2.9 to 2.22 of the CHIS Code of Practice.

Separate CHIS use and conduct authorisations

267 It is the practice of some authorities to separate the use and conduct authorisations; there is nothing in the legislation to prevent this but it can lead to error. The principle is that there should be a minimum number of authorisations for a CHIS and each authorisation should stand on its own. Conduct authorisations should not conflict and care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant reviews, renewals and cancellations are correctly performed.

CHIS interference with property

268 Although it is not encouraged, it is permissible for CHIS to interfere with property (for example, by photocopying documents should an opportunity arise), provided that the terms of the

authorisation contemplated this type of conduct. If property interference is foreseen, it would be prudent also to obtain an authorisation for property interference.

Extent of directed surveillance (sections 26 and 48(2) of RIPA and sections 1(2) and 31(2) of RIP(S)A)

269 Directed surveillance is covert surveillance that is carried out for the purposes of a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person, whether or not he is a subject of the action. It includes the activity of monitoring, observing, listening and recording by or with the assistance of surveillance equipment. It need not be subject specific. A search for an identified person in a public place will not amount to directed surveillance, unless it includes covert activity that may elicit private information about that person or any other person. Any processing of data (e.g. taking a photograph to put on record) is an invasion of privacy.

(See also 233)

Subject or operation specific (section 26(2)(a) of RIPA and section 1(2)(a) of RIP(S)A)

270 Whether a fresh authorisation is required if new subjects emerge depends on the terms of the original authorisation. But in principle these provisions put the emphasis on the operation as being the purpose of the surveillance.

Immediate response (section 26(2) of RIPA and section 1(2)(c) of RIP(S)A)

271 These provisions explain the expression "an immediate response to events or circumstances" by saying "the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance." In short, it relates to events or circumstances that occur extemporarily. A response is not to be regarded as "immediate" where the need for an authorisation is neglected until it is too late to apply for it. See also RIPA Covert Surveillance and Property Interference Code of Practice paragraph 2.23.

Crime in progress: private information (section 26(10) of RIPA and section 1(9) of RIP(S)A)

272 As a general principle, if it is clear that a crime is in progress, the offender can have no expectation of privacy and no authorisation for directed surveillance will be required.

273 It is important to differentiate between a crime in progress and a criminal situation which is believed to exist but where evidence may be lacking. In the latter case it would be prudent to obtain an authorisation if time permits.

Describe the operation

274 Authorisations against a named subject should indicate when, where, and in what circumstances the surveillance is to be carried out.

275 Authorisations should specify only the specific covert activities or techniques likely to be required.

Pre-emptive directed surveillance authorisations

276 When high grade intelligence is received which enables the production of a plan involving covert surveillance, but where the exact details of the location are not known, it is permissible to prepare an authorisation in order properly to brief those conducting the surveillance. But it must be subject to an immediate review once the missing details are known. It is unwise to act on an incomplete authorisation and this guidance should not be construed as enabling authorisations to be regularly prepared in anticipation of events. The difference between this guidance and use of the urgency provisions is that the urgency provisions may only be used when events could not be anticipated and when there is a threat to life or the operation would be otherwise jeopardised.

Electronic surveillance across the Scottish/English border

277 There is no difference between the method of surveillance (electronic or non-electronic) and the same rules apply to each.

'Drive by' surveillance

278 'Drive by' surveillance may or may not need an authorisation and it is not acceptable to prescribe a minimum number of passes before an authorisation is required.

Use of noise monitoring equipment

279 Where possible, the intention to monitor noise should be notified to the owner and occupier. Where notice is not possible or has not been effective, covert monitoring may be considered necessary and proportionate. So long as what is recorded is only that which could be heard by the unaided ear the perpetrator has probably forfeited any claim to privacy and an authorisation may not be necessary. The authorising officer should consider whether the surveillance equipment is capable of measuring volume only or whether it can identify the perpetrators, mindful that the more sensitive the equipment the greater the potential for intrusive surveillance.

(See also note 104 and Covert Surveillance and Property Interference Code of Practice 2.29)

CCTV systems - the need for a unified protocol for use

280 It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

Urgent oral authorisations - essential information to be provided to local authority CCTV managers

281 When an urgent oral authorisation has been issued, the local authority (or any other entity acting on the authorisation) should be provided with the details (including contact information)

of the authorising officer, the start and expiry date and time and a written summary of what has been authorised (copy of contemporaneous notes taken by the applicant).

Surveillance of persons wearing electronic tags

282 If surveillance against a person wearing an electronic tag is done in a manner not made clear to him, that surveillance is covert and an authorisation should be obtained.

Recording of telephone calls - one party consent

283 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, a telephone conversation may be recorded and authorised as directed surveillance providing that the consent of one of the parties is obtained (see paragraph 2.9 of the RIPA Covert Surveillance and Property Interference Code of Practice). Providing that the original terms of a CHIS authorisation enables it, an additional authorisation for directed surveillance is not required if a CHIS sets out to overhear a telephone conversation or records a telephone conversation (see paragraph 2.29 of the RIPA Covert Surveillance and Property Interference Code of Practice). If there is doubt, it would be prudent to obtain a directed surveillance authorisation. There is no equivalent provision in RIP(S)A.

Closed visits in prison (section 48(7)(b) of RIPA)

284 In prisons closed visits take place in a common area in which booths are set up in such a way as to prevent contact between the inmate and visitor, or in which cubicles are provided in order to afford a limited degree of privacy primarily in relation to other inmates. But whatever form surveillance may take, such a visiting booth or cubicle is not a space being used for residential purposes or otherwise as living accommodation, so does not amount to intrusive surveillance. If the surveillance is likely to obtain information subject to legal privilege it is directed surveillance but is authorised using intrusive surveillance processes.

285 Provided that notices are displayed within visiting areas advertising the fact that CCTV is in operation, a directed surveillance authorisation is not needed for visual monitoring of prisoners during open prison visits, as they will be aware that they are under surveillance. But when CCTV is concentrated on a particular visit or visits as part of a pre-planned operation, and private information is likely to be obtained, an authorisation should be applied for.

Crime hotspots (section 26(2) of RIPA and section 1(4) of RIP(S)A)

286 The statutory provisions apply to the obtaining of information about a person whether or not one specifically identified for the purposes of the investigation. It is not restricted to an intention to gain private information because the subsections refer to covert surveillance carried out "in such a manner as is likely to result in the obtaining of private information".

287 Surveillance of persons while they are actually engaged in crime in a public place is not likely to result in the obtaining of information about them which is properly to be regarded as 'private'. But surveillance of persons who are not, or who turn out not to be, engaged in crime is much more likely to result in the obtaining of private information about them.

288 An authorisation for directed surveillance is required whenever it is believed that there is a real possibility that the manner in which it is proposed to carry out particular surveillance will result

in the obtaining of private information about any person, whether or not that person is or becomes a subject of the operation.

Drivers using mobile telephones

289 It is currently unwise to act covertly without authorisation to acquire evidence of drivers using mobile telephones whilst in private vehicles because it might be considered to be intrusive surveillance and would need to meet the appropriate necessity, proportionality and serious crime tests and require the prior approval of a Commissioner. (See also note 232).

Police use of grounds of national security (cf RIPA ss 28(3)(a) and 29(3)(a))

290 RIPA enables a Chief Constable (using his Special Branch) to conduct activity on the grounds of National Security. The Commissioners acknowledge the Security Service's primacy and would expect a law enforcement agency to offer that Service the opportunity to take the lead (i.e. to authorise). If this offer is rejected, the Chief Constable should not be constrained from investigating using his own resources providing that the grounds of proportionality and necessity are met. If he decides to authorise a CHIS on these grounds, without 'concurrence', the CHIS should be managed in accordance with the legislation, Codes of Practice *and* OSC guidelines.

Surveillance equipment should be under central management

291 All surveillance equipment owned by the public authority should be under central management, since, whatever the object, covert use could be made of most devices. It is considered best practice to cross-reference equipment deployment records with the Unique Reference Number of the relevant authorisation. Where surveillance equipment is shared (e.g. partnership arrangements) there should be auditable processes to prevent unauthorised use of surveillance equipment.

The availability of resources

292 Whilst there may be a public expectation that public authorities will monitor offenders, an authorising officer should not grant an activity when he knows there to be insufficient covert surveillance resources do conduct it.

Technical feasibility studies

293 Feasibility studies should be conducted before the application is submitted to the authorising officer. Without it the authorising officer is unable to know the objectives can be achieved or to accurately assess proportionality or collateral intrusion. It is unacceptable to deny knowledge of technical capability from the authorising officer.

Copying property

294 To copy the owner's key would require a PA97 authorisation; to obtain duplicate keys from a manufacturer would not require an authorisation for interference with property but the use of them would require an RIPA authorisation.

Surveillance of disqualified drivers

295 RIPA does not forbid the continuance of surveillance if it is known that the driver is disqualified from driving.

INDEX SHOWING PAGE NUMBERS

A

B

C

J

K

L

M

N

O

P

Intentionally blank

Office of Surveillance Commissioners

Additional copies available from:

The Secretary
Office of Surveillance Commissioners
PO Box 29105
London SW1V 1ZU

Email: oscmailbox@osc.gsi.gov.uk