

# **Covert human intelligence sources in cartel investigations**

Code of practice

August 2004

This code applies to every authorisation of the use or conduct of covert human intelligence sources by the OFT carried out under Part II of the Regulation of Investigatory Powers Act 2000 beginning from 5 January 2004

OFT739

**Crown copyright**

© Crown copyright 2004

This material may be freely reproduced, except for sale or advertising purposes.

## CONTENTS

<i>Chapter</i>		<i>Page</i>
1	Background	1
2	General rules on authorisations	4
3	Special rules on authorisations	9
4	Authorisation procedures for covert human intelligence sources	13



# 1 BACKGROUND

- 1.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 No. 3171 added the Office of Fair Trading (OFT) to the list of public authorities approved for the purposes of authorising covert human intelligence sources under Part II of the Regulation of Investigatory Powers Act 2000 (the 2000 Act). This code of practice provides guidance on the authorisation of the use or conduct of covert human intelligence sources (a source) by the OFT in cartel investigations under the Enterprise Act 2002 (the Enterprise Act) and the Competition Act 1998 (the Competition Act). This code should be read in conjunction with the Home Office 'Covert Human Intelligence Sources Code of Practice', published pursuant to section 71 of the 2000 Act.
- 1.2 The Enterprise Act makes it a criminal offence for individuals dishonestly to agree with one or more other persons that two or more undertakings will engage in certain prohibited cartel arrangements, such as those that involve price-fixing, market-sharing, limitation of production or supply and bid-rigging. The offence applies in respect of dishonest agreements both to make or implement such arrangements and also to cause such arrangements to be made or implemented. The criminal cartel offence will be committed irrespective of whether the agreement reached is actually implemented by the undertakings. Any individual convicted of the offence may receive a maximum of five years' imprisonment and/or an unlimited fine.
- 1.3 The criminal cartel offence operates alongside the Competition Act regime and the regime by which the OFT can enforce article 81 of the EC Treaty in light of EC Regulation 1/2003. For the purposes of this Code, references to the Competition Act, in terms of the use or conduct of a source and use of the material obtained thereby, should also be taken to refer to the OFT's responsibility to enforce article 81 so far as it relates to cartels. It should be noted that in order for the use or conduct of a source to be authorised in an investigation under article 81, the OFT will need to demonstrate that such an authorisation was necessary in the interests of the economic well-being of the United Kingdom.

- 1.4 The OFT will limit authorisations for the use or conduct of a source in its Enterprise Act investigations to those where it is investigating a suspected cartel agreement to fix prices, limit production or supply, share markets or rig bids. In respect of Competition Act investigations, this definition of a cartel can embrace some vertical price fixing arrangements as well as purely horizontal ones. For example, where a manufacturer enters into separate agreements with a number of retailers that they will not sell the manufacturer's products at below a certain price.
- 1.5 The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the OFT as part of their normal civic duties. Members of the public acting in this way will not generally be regarded as sources.
- 1.6 Neither Part II of the 2000 Act nor this code of practice is intended to affect the practices and procedures surrounding criminal participation of sources.

## **General extent of powers**

- 1.7 Authorisations can be given for the use or conduct of a source both inside and outside the United Kingdom. Authorisations for actions outside the United Kingdom can only validate them for the purposes of criminal proceedings or administrative procedures in the United Kingdom. An authorisation under Part II of the 2000 Act does not take into account the requirements of the country outside the United Kingdom in which the investigation or operation is taking place.

## **Use of material in evidence**

- 1.8 Material obtained from a source may be used as evidence in criminal proceedings in respect of the cartel offence and administrative procedures instituted by the OFT under the Competition Act. The proper authorisation of a source should ensure the suitability of such evidence under the common law, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998. Furthermore, the product obtained by a source described in this code is subject to the ordinary rules

for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996. There are also well-established legal procedures in criminal proceedings that will protect the identity of a source from disclosure. In respect of administrative procedures instituted by the OFT under the Competition Act, it is possible that the product obtained by a source may form part of the OFT's file relating to a proposed infringement decision. The undertakings the subject of the proposed decision will have an opportunity to inspect the OFT file although the file would not include documents to the extent to which they contain confidential information, including those that might give rise to even the slightest possibility that the identity of a source would be revealed. ('Confidential information' in this context is used in a wider sense than the very specific meaning given to the term in Chapter 3 of this code.)

## 2 GENERAL RULES ON AUTHORISATIONS

- 2.1 An authorisation under Part II of the 2000 Act will provide the OFT with lawful authority for the use of a source. The responsibility for granting such authorisations within the OFT will rest with the Director of Cartel Investigations (the Authorising Officer), although in urgent cases a designated Principal Investigation Officer in the Cartels Investigations Branch may act to grant authorisations (see paragraphs 4.10 and 4.11 below).
- 2.2 Part II of the 2000 Act does not impose a requirement on public authorities such as the OFT to seek or obtain an authorisation where, under the 2000 Act, one is available (see section 80 of the 2000 Act). Nevertheless, where there is an interference by the OFT with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other lawful authority, the consequences of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.
- 2.3 The OFT will therefore always seek an authorisation where the use or conduct of a source is likely to interfere with a person's Article 8 rights to privacy by obtaining information from or about a person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with the law and subject to stringent safeguards against abuse.

### **Necessity and proportionality**

- 2.4 Obtaining an authorisation under the 2000 Act will only ensure that the authorised use or conduct of a source is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for the source to be used. The 2000 Act first requires that the authorising officer believes that the authorisation is necessary in the circumstances of the particular case for the statutory grounds in section 29(3)(b) of the 2000 Act in respect of Enterprise Act investigations and section 29(3)(c) in respect of Competition Act investigations.

2.5 Then, if he believes that the use of the source is necessary, the authorising officer will also decide if he believes that the use of a source is proportionate to what is sought to be achieved by the conduct and use of that source. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. The use of a source will be carefully managed to meet the objective in question and a source will not be used in an arbitrary or unfair way.

### **Collateral intrusion**

2.6 Before authorising the use or conduct of a source, the authorising officer will also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation ('collateral intrusion'). Measures will be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

2.7 An application for an authorisation will include an assessment of the risk of any collateral intrusion. The authorising officer will take this into account when considering the proportionality of the use and conduct of a source.

2.8 Those tasking a source will inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When, in light of this, the original authorisation may not be sufficient, consideration will be given as to whether the authorisation needs to be amended and reauthorised or whether a new authorisation is required.

2.9 Those granting or applying for an authorisation will consider whether there are any particular sensitivities in the local community where the source is being used and whether there are similar activities being undertaken by other public authorities which could impact on the deployment of the source. Consideration will also be given to any adverse

impact on community confidence or safety that may result from the use or conduct of a source or of information obtained from that source. In this regard, the authorising officer may consider it appropriate to consult a senior officer within the police force area in which the source is deployed. Additionally, the authorising officer will make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

- 2.10 In a very limited range of circumstances an authorisation under Part II may, by virtue of sections 26(7) and 27 of the 2000 Act, render lawful conduct which would otherwise be criminal, if it is incidental to any conduct falling within section 26(8) of the 2000 Act which the source is authorised to undertake. This would depend on the circumstances of each individual case. A source that acts beyond the limits recognised by the law will be at risk from prosecution. The need to protect the source cannot alter this principle.

### **Combined authorisations**

- 2.11 A single authorisation may combine two or more different authorisations under Part II of the 2000 Act. For example, a single authorisation may combine authorisations for intrusive surveillance and the conduct of a source. In such cases the provisions applicable to each of the authorisations will be considered separately. Thus, the Director of Cartel Investigations would authorise the conduct of a source but an authorisation for intrusive surveillance by the OFT would need the separate authority of the Chairman of the OFT and the approval of a Surveillance Commissioner.

### **Directed surveillance against a potential source**

- 2.12 It may be necessary to deploy directed surveillance against a potential source as part of the process of assessing their suitability for recruitment, or in planning how best to make an approach to them. An authorisation under this code authorising an officer of the OFT to establish a covert relationship with a potential source could be combined with a directed surveillance authorisation so that both the officer and the potential source could be followed. Directed surveillance is defined in section 26(2) of the 2000 Act (and also in the OFT's Code of Practice on Covert Surveillance).

## Central record of all authorisations

2.13 A centrally retrievable record of all authorisations will be held by the Cartels Investigation Branch of the OFT (the CIB) and regularly updated whenever an authorisation is granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records will be retained for a period of at least three years from the ending of the authorisation.

2.14 Proper records will be kept of the authorisation and use of a source. Section 29(5) of the 2000 Act provides that the authorising officer must not grant an authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source. Therefore, within the CIB, designated Investigation Officers will be responsible for maintaining the relevant records. The Regulation of Investigatory Powers (Source Records) Regulations 2000 SI No: 2725 details the particulars that must be included in the records relating to each source. The CIB will ensure these particulars are included in every case.

2.15 In addition, records or copies of the following, as appropriate, will be kept by the CIB:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested
- the reason why the person renewing an authorisation considered it necessary to do so
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent

- any risk assessment made in relation to the source
- the circumstances in which tasks were given to the source
- the value of the source to the OFT
- a record of the results of any reviews of the authorisation
- the reasons, if any, for not renewing an authorisation
- the reasons for cancelling an authorisation.
- the date and time when any instruction was given by the authorising officer to cease using a source.

2.16 The records kept by the CIB will be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There will, at all times on each investigation or operation, be a designated Investigation Officer within the CIB who will have responsibility for maintaining a record of the use made of the source.

### **Retention and destruction of the product**

2.17 Where the product obtained from a source could be relevant to pending or future criminal proceedings under the Enterprise Act or administrative procedures under the Competition Act, it will be retained by the OFT in accordance with the established disclosure requirements for a suitable further period, commensurate to any subsequent review.

2.18 There is nothing in the 2000 Act which prevents material obtained from the properly authorised use of a source being used in other investigations. The OFT will ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of a source. The OFT will also ensure compliance with the appropriate data protection requirements.

### **3 SPECIAL RULES ON AUTHORISATIONS**

#### **Confidential information**

- 3.1 The 2000 Act does not provide any special protection for 'confidential information'. Nevertheless, particular care will be taken by the OFT in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. The term confidential information in this sense refers to information which consists of matters subject to legal privilege, contains confidential personal information or confidential journalistic material
- 3.2 In cases where through the use or conduct of a source it is likely that knowledge of confidential information will be acquired, the deployment of the source will be subject to a higher level of authorisation. Within the OFT, the Chairman of the OFT will authorise the use or conduct of a source in such circumstances. In his absence, a designated deputy will perform the function.

#### **Communications subject to legal privilege**

- 3.3 Section 196 of the Enterprise Act and section 30 of the Competition Act describes those matters that are subject to legal privilege. In Scotland, the relevant description is contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.
- 3.4 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. Privilege is not lost, however, if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

- 3.5 Although the 2000 Act does not provide any special protection for legally privileged information, the OFT will afford such material special protection in all its investigations. Moreover, such information is particularly sensitive and any source which acquires such material may engage Articles 6 and 8 of the ECHR. Legally privileged information obtained by a source is extremely unlikely ever to be admissible as evidence in criminal proceedings or administrative procedures under the Competition Act. The mere fact that use has been made of a source to obtain such information may lead to any related criminal proceedings being stayed as an abuse of process. Accordingly, action which may lead to such information being obtained is subject to additional safeguards under this code.
- 3.6 In general, an application for the use or conduct of a source which is likely to result in the acquisition of legally privileged information will only be made in exceptional and compelling circumstances. Full regard will be given to the particular proportionality issues such use or conduct of a source raises. The application will include, in addition to the reasons why it is considered necessary for the use or conduct of a source to be used, an assessment of how likely it is that information subject to legal privilege will be acquired. Moreover, the application will clearly state whether the purpose (or one of the purposes) of the use or conduct of the source is to obtain legally privileged information.
- 3.7 This assessment will be taken into account by the Chairman of the OFT in deciding whether the proposed use or conduct of a source is necessary and proportionate for a purpose under section 29(3)(b) or 29(3)(c) of the 2000 Act. The Chairman of the OFT may also require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where legally privileged information has been acquired and retained, the matter will be reported to the relevant Commissioner or Inspector during his next inspection and the material will be made available to him if requested.
- 3.8 A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, any case where a lawyer is the subject of an investigation or operation will be notified to the relevant Commissioner or Inspector during his next inspection and any

material which has been retained will be made available to him if requested.

- 3.9 Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, legal advice will be sought as necessary before any further dissemination of the material takes place. Similar advice will also be sought where there is doubt over whether information is not subject to legal privilege due to the 'in furtherance of a criminal purpose' exception (paragraph 3.4 above). The retention of legally privileged information, or its dissemination to an outside body, will be accompanied by a clear warning that it is subject to legal privilege. It will be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known to any person whose possession of it might prejudice any criminal proceedings under the Enterprise Act or administrative procedures under the Competition Act related to the information. Any dissemination of legally privileged material to an outside body will be notified to the relevant Commissioner or Inspector during his next inspection.

### **Communications involving confidential personal information and confidential journalistic material**

- 3.10 Similar consideration will also be given to authorisations that involve confidential personal information and confidential journalistic material. In those cases where confidential personal information and confidential journalistic material has been acquired and retained, the matter will be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

- 3.11 Spiritual counselling means conversations between an individual and a Minister of Religion acting in his official capacity, where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.
- 3.12 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

## **4 AUTHORISATION PROCEDURES FOR COVERT HUMAN INTELLIGENCE SOURCES**

- 4.1 Under section 26(8) of the 2000 Act a person is a source if:
- a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c)
  - b) he covertly uses such a relationship to obtain information or to provide access to any information to another person or
  - c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
- 4.2 A source, as used by the OFT, will usually include those referred to as informants or whistle-blowers.
- 4.3 By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.
- 4.4 By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as mentioned in paragraph 4.1(c) above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.
- 4.5 The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.
- 4.6 The conduct of a source is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

## Authorisation procedures

- 4.7 Under section 29(3) of the 2000 Act an authorisation for the use or conduct of a source may be granted by the authorising officer only where he believes that the authorisation is necessary:
- for the purpose of preventing and detecting crime<sup>1</sup> (in respect of Enterprise Act investigations) or
  - in the interests of the economic well-being of the UK (in respect of Competition Act investigations).
- 4.8 The authorising officer must also believe that the authorised use or conduct of a source is proportionate to what is sought to be achieved by that use or conduct.
- 4.9 Responsibility for authorising the use or conduct of a source rests with the authorising officer and all authorisations require the personal authority of the authorising officer.
- 4.10 The authorising officer will give authorisations in writing, except that in urgent cases, they may be given orally by the authorising officer or the officer entitled to act in urgent cases. The officers entitled to act in urgent cases will be designated Principal Investigation Officers within the CIB. In such cases, a statement that the authorising officer has expressly authorised the action will be recorded in writing by the applicant as soon as is reasonably practicable.
- 4.11 A case will not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making.

---

<sup>1</sup> This is defined in section 81(5) of the 2000 Act.

4.12 The authorising officer, including the authorising officer acting in urgent cases, will not be responsible for tasking a source or acting as a source.

### **Information to be provided in applications for authorisation**

4.13 An application for authorisation for the use or conduct of a source will be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds as listed in either section 29(3)(b) or 29(3)(c) of the 2000 Act
- the reasons why the authorisation is considered proportionate to what it seeks to achieve
- the purpose for which the source will be tasked or deployed (e.g. in relation to the investigation of a suspected criminal cartel offence)
- where a specific investigation or operation is involved, the nature of that investigation or operation
- the nature of what the source will be tasked to do
- the level of authority required (or recommended, where that is different)
- the details of any potential collateral intrusion and why the intrusion is justified
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

4.14 Additionally, in urgent cases, the authorisation will record (as the case may be):

- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given and/or
- the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

4.15 Where the authorisation is oral, the detail referred to above will be recorded in writing by the applicant as soon as reasonably practicable.

### Duration of authorisations

4.16 A written authorisation will, unless renewed, cease to have effect at the end of a period of **twelve months** beginning with the day on which it took effect.

4.17 Urgent oral authorisations or authorisations granted or renewed by the person who is entitled to act only in urgent cases (paragraph 4.10) will, unless renewed, cease to have effect after **seventy-two hours**, beginning with the time when the authorisation was granted or renewed.

### Reviews

4.18 Regular reviews of authorisations will be undertaken to assess the need for the use of a source to continue. The review will include the use made of the source during the period authorised, the tasks given to the source and the information obtained from the source. The results of a review will be recorded on the authorisation record (see paragraphs 2.13 - 2.16). The authorising officer will be mindful of the need to review authorisations more frequently where the use of a source provides access to confidential information or involves collateral intrusion.

4.19 In each case the authorising officer will determine how often a review should take place. This will be as frequently as the authorising officer considers to be necessary and practicable.

## Renewals

- 4.20 Before the authorising officer renews an authorisation, he will satisfy himself that a review has been carried out of the use of a source as outlined in paragraph 4.18.
- 4.21 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he will renew it in writing for a further period of **twelve months**. Renewals may also be granted orally in urgent cases and will last for a period of **seventy-two hours**.
- 4.22 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal will not be made until shortly before the authorisation period is drawing to an end. Only the authorising officer who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. The renewal will be kept/recorded as part of the authorisation record (see paragraphs 2.13 - 2.16).
- 4.23 All applications for the renewal of an authorisation will record:
- whether this is the first renewal or every occasion on which the authorisation has been renewed previously
  - any significant changes to the information in paragraph 4.13
  - the reasons why it is necessary to continue to use the source
  - the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation
  - the tasks given to the source during that period and the information obtained from the conduct or use of the source
  - the results of regular reviews of the use of the source.

## **Cancellations**

4.24 The authorising officer who granted or renewed the authorisation will cancel it if he is satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that satisfactory arrangements for the source's case no longer exist. Where the authorising officer is no longer available, this duty will fall to the person who has taken over the role of authorising officer or the person who is acting as authorising officer. Where necessary, the safety and welfare of the source will continue to be taken into account after the authorisation has been cancelled.

## **Management of sources**

### **Tasking**

4.25 Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) ('the source handler') and 29(5)(b) ('the oversight officer') of the 2000 Act. Tasking may include asking the source to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the OFT. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

4.26 The source handler will have day to day responsibility for

- dealing with the source on behalf of the OFT
- directing the day to day activities of the source
- recording the information supplied by the source and
- monitoring the source's security and welfare.

4.27 The source handlers will be designated Officers from within the CIB. There will always be two source handlers dealing with each source in all

cartel investigations. The oversight officer will be a G7 Officer from within the CIB and will be responsible for the general oversight of the use of the source. The oversight officer will not act as a source handler in the same investigation.

- 4.28 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a source may be tasked with finding out purely factual information about the layout of commercial premises. In such cases, it will be for the authorising officer to determine where, and in what circumstances, such activity may require authorisation.
- 4.29 Authorisations will not be drawn so narrowly that a separate authorisation will be required each time the source is tasked. Rather, an authorisation will cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation will be sought, as necessary and appropriate.
- 4.30 It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence will be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it will either be updated and reauthorised (for minor amendments only) or it will be cancelled and a new authorisation will be obtained before any further such action is carried out.
- 4.31 Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the source handler and oversight officer will refer the proposed tasking to the authorising officer, who will consider whether a separate authorisation is required. This will be done in advance of any tasking and the details of such referrals will be recorded.

## **Management responsibility**

- 4.32 The Director of Cartel Investigations will ensure that arrangements are in place for the proper oversight and management of sources and that

individual Officers (as appropriate) from within the CIB are appointed in accordance with section 29(5)(a), and (b) for each source.

- 4.33 In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority (e.g. the OFT and the Serious Fraud Office), the OFT will assume responsibility for the management and oversight of that source.

## **Security and welfare**

- 4.34 When deploying a source the OFT will take into account the safety and welfare of that source when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising officer will ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, will also be considered from the outset.

- 4.35 The source handler is responsible for bringing to the attention of the oversight officer any concerns about the personal circumstances of the source, insofar as they might affect:

- the validity of the risk assessment
- the conduct of the source, and
- the safety and welfare of the source.

- 4.36 Where appropriate, the authorising officer will consider concerns about such matters, and will decide whether or not to allow the authorisation to continue.

## **ADDITIONAL RULES**

### **Recording of telephone conversations**

- 4.37 Subject to paragraph 4.38 below, the interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be authorised only by the Secretary of State, in accordance with the terms of Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.
- 4.38 Part I of the 2000 Act provides certain exceptions to the rule that interception of telephone conversations must be warranted under that Part. This includes where one party to the communication consents to the interception in which case it may be authorised in accordance with section 48(4) of the 2000 Act provided that there is no interception warrant authorising the interception. In such cases, the interception is treated as directed surveillance (see chapter 4 of the OFT's Covert Surveillance code of practice).

### **Use of covert human intelligence source with technical equipment**

- 4.39 A source, whether or not wearing or carrying a surveillance device and invited into residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or vehicle which take place in his presence. This also applies to the recording of telephone conversations other than by interception which takes place in the source's presence. Authorisation for the use or conduct of that source will be obtained in the usual way.
- 4.40 However, if a surveillance device is to be used, other than in the presence of the source, an intrusive surveillance authorisation and, if applicable, an authorisation for interference with property will be obtained (see chapters 5 and 6 of the OFT Covert Surveillance Code of Practice).