Archived 2002

COVERT HUMAN INTELLIGENCE SOURCES

CODE OF PRACTICE

Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000

Commencement

This code applies to every authorisation of the use or conduct by public authorities of covert human intelligence sources carried out under Part II of the Regulation of Investigatory Powers Act 2000 which begins on or after the day on which this code comes into effect.

Page created 1 August 2002

1 BACKGROUND

1 GENERAL

1.1 In this code the:

- **"1989 Act"** means the Security Service Act 1989;
- **"1994 Act"** means the Intelligence Services Act 1994;
- **"1997 Act"** means the Police Act 1997;
- **"2000 Act"** means the Regulation of Investigatory Powers Act 2000;
- **"RIP(S)A"** means the Regulation of Investigatory Powers (Scotland) Act 2000;

1.2 This code of practice provides guidance on the authorisation of the use or conduct of covert human intelligence sources ("a source") by public authorities under Part II of the 2000 Act.

1.3 The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

1.4 Neither Part II of the 2000 Act or this code of practice is intended to affect the practices and procedures surrounding criminal participation of sources.

1.5 The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of the code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the 2000 Act, or to one of the Commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account.

General extent of powers

1.6 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 proceedings 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.

1.7 Members of foreign law enforcement or other agencies or sources of those agencies may be authorised under the 2000 Act in the UK in support of domestic and international investigations.

1.8 Where the conduct authorised is likely to take place in Scotland, authorisations should be granted under RIP(S)A, unless the authorisation is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000). Additionally, any authorisation granted or renewed for the purposes of national security or the economic well-being of the UK must be made under the 2000 Act. This code of practice is extended to Scotland in relation to authorisations made under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to authorisations made under RIP(S)A.

Use of material in evidence

1.9 Material obtained from a source may be used as evidence in criminal proceedings. 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, where those rules apply to the law enforcement body in question. There are also well-established legal procedures that will protect the identity of a source from disclosure in such circumstances.

2 GENERAL RULES ON AUTHORISATIONS

2.1 An authorisation under Part II of the 2000 Act will provide lawful authority for the use of a source. Responsibility for giving the authorisation will depend on which public authority is responsible for the source.

2.2 Part II of the 2000 Act does not impose a requirement on public authorities 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 a public authority 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 Public authorities are therefore strongly recommended to 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 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 person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 29(3) of the 2000 Act.

2.5 Then, if the use of the source is necessary, the person granting the authorisation must believe 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 should be carefully managed to meet the objective in question and sources must 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 should 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 should 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 should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the use and conduct of a source.

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

2.9 Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the source is being used and of similar activities being undertaken by other public authorities which could impact on the deployment of the source. Consideration should 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, it is recommended that where the authorising officers in the National Criminal Intelligence Service (NCIS), the National Crime Squad (NCS) and HM Customs and Excise (HMCE) consider that conflicts might arise they should consult a senior officer within the police force area in which the source is deployed. Additionally, the authorising officer should 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, and consideration should always be given to seeking advice from the legal adviser within the relevant public authority when such activity is contemplated. 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 must be considered separately. Thus, a police superintendent can authorise the conduct of a source but an authorisation for intrusive surveillance by the police needs the separate authority of a chief constable, and in certain cases the approval of a Surveillance Commissioner will also be necessary. Where an authorisation for the use or conduct of a covert human intelligence source is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State. However, this does not preclude public authorities from obtaining separate authorisations.

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 the approach to them. An authorisation under this code authorising an officer to establish a covert relationship with a potential source could be combined with a directed surveillance authorisation so that both the officer and potential source could be followed. Directed surveillance is defined in section 26(2) of the 2000 Act. See the code of practice on Covert Surveillance.

Central Record of all authorisations

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

2.14 Proper records must be kept of the authorisation and use of a source. Section 29(5) of the 2000 Act provides that an 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. 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.

2.15 In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

- 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 investigating authority;

- 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 public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person

within the relevant public authority 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 or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

2.18 In the cases of the law enforcement agencies (not including the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

2.19 There is nothing in the 2000 Act which prevents material obtained from properly authorised use of a source being used in other investigations. Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of a source. Authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material.

The Intelligence services, MOD and HM Forces

2.20 The heads of these agencies are responsible for ensuring that arrangements exist to ensure that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

3 SPECIAL RULES ON AUTHORISATIONS

Confidential Information

3.1 The 2000 Act does not provide any special protection for ‘confidential information’. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, 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 is subject to a higher level of authorisation. Annex A lists the authorising officer for each public authority permitted to authorise such use or conduct of a source.

Communications Subject to Legal Privilege

3.3 Section 98 of the 1997 Act describes those matters that are subject to legal privilege in England and Wales. 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. But privilege is not lost 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 The 2000 Act does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and any source which acquires such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8. Legally privileged information obtained by a source is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, 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 should only be made in exceptional and compelling circumstance. Full regard should be had to the particular proportionality issues such a use or conduct of a source raises. The application should 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. The application should 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 authorising officer in deciding whether the proposed use or conduct of a source is necessary and proportionate for a purpose under section 29 of the 2000 Act. The authorising officer may 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 should be reported to the relevant Commissioner or Inspector during his next inspection and the material should 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 should be notified to the relevant Commissioner or Inspector during his next inspection and any material which has been retained should 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, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Similar advice should 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. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should 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 or civil proceedings related to the information. Any dissemination of legally privileged material to an outside body should 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 must 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 should 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.

Vulnerable individuals

3.13 A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances. In these cases, the attached table in Annex A lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a source.

Juvenile sources

3.14 Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. **On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.** In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is **one month** instead of twelve months.

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 may include those referred to as agents, informants and officers working undercover.

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 where he believes that the authorisation is necessary:

- in the interests of national security [1],[2];

- for the purpose of preventing and detecting [3] crime or of preventing disorder;
- in the interests of the economic well-being of the UK;
- In the interests of public safety;
- for the purpose of protecting public health[4];
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for any other purpose prescribed in an order made by the Secretary of State[5].

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 The public authorities entitled to authorise the use or conduct of a source are those listed in Schedule 1 to the 2000 Act. 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. An authorising officer is the person designated under section 29 of the 2000 Act to grant an authorisation for the use or conduct of a source. The Regulation of Investigatory Powers (Prescriptions of Offices, Ranks and Positions) Order 2000; SI No: 2417 designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases. In certain circumstances the Secretary of State will be the authorising officer (see section 30(2) of the 2000 Act).

4.10 The authorising officer must 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. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant as soon as is reasonably practicable.

4.11 A case is 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.

4.12 Authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the source or in tasking the source. However, it is recognised that this is not always possible, especially in the cases of small organisations. Where an authorising officer authorises his own activity the authorisation record (see paragraphs 2.13 - 2.15) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

4.13 The authorising officers within the police, NCIS and NCS may only grant authorisations on application by a member of their own force, Service or Squad. Authorising officers in HMCE may only grant authorisations on application by a customs officer.

Footnote:

[1]One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the United Kingdom, save that, in Northern Ireland, where the lead responsibility for investigating the threat from terrorism related to the affairs of Northern Ireland lies with the Police Service of Northern Ireland. An authorising officer in another public authority should not issue an authorisation under Part II of the 2000 Act where the operation or investigation falls within the responsibilities of the Security Service,as set out above, except where it is to be carried out by a Special Branch or where the Security Service has agreed that another public authority can authorise the use or conduct of a source which would normally fall within the responsibilities of the Security Service.

[2]HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security in support of the Security Service, the Police Service of Northern Ireland or other Civil Powers.

[3]Detecting crime is defined in section 81(5) of the 2000 Act.

[4]This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

[5]This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

Information to be provided in applications for authorisation

4.14 In application for authorisation for the use or conduct of a source should be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in section 29(3) 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 an organised serious crime, espionage, a series of racially motivated crimes etc);
- where a specific investigation or operation is involved, 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.

4.15 Additionally, in urgent cases, the authorisation should 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.

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

Duration of authorisations

4.17 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.

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

Reviews

4.19 Regular reviews of authorisations should be undertaken to assess the need for the use of a source to continue. The review should 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 should be recorded on the authorisation record (see paragraphs 2.13 - 2.15). Particular attention is drawn to the need to review authorisations frequently where the use of a source provides access to confidential information or involves collateral intrusion.

4.20 In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Renewals

4.21 Before an authorising officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a source as outlined in paragraph 4.19.

4.22 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 may renew it in writing for a further period of **twelve months**. Renewals may also be granted orally in urgent cases and last for a period of **seventy-two hours**.

4.23 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 should not be made until shortly before the authorisation period is drawing to an end. Any person 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 should be kept/recorded as part of the authorisation record (see paragraphs 2.13 - 2.15).

4.24 All applications for the renewal of an authorisation should 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 4.14;
- 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

4.25 The authorising officer who granted or renewed the authorisation must 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 on the person who has taken over the role of authorising officer or the person who is acting as authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794). Where necessary, the safety and welfare of the source should continue to be taken into account after the authorisation has been cancelled.

MANAGEMENT OF SOURCES

Tasking

4.26 Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. 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.

4.27 The person referred to in section 29(5)(a) of the 2000 Act will have day to day responsibility for:

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

4.28 The person referred to in section 29(5)(b) of the 2000 Act will be responsible for the general oversight of the use of the source.

4.29 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. Alternatively, a trading standards officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may require authorisation.

4.30 It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.

4.31 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 must be recorded as soon as practicable after the event and, if the existing

authorisation is insufficient it should either be updated and reauthorised (for minor amendments only) or it should cancelled and a new authorisation should be obtained before any further such action is carried out.

4.32 Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

4.33 Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each source.

4.34 The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.
In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

4.36 Any public authority deploying a source should 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 should 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, should also be considered at the outset.

4.37 The person defined at section 29(5)(a) of the 2000 Act is responsible for bringing to the attention of the person defined at section 29(5)(b) of the 2000 Act 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.

4.38 Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

ADDITIONAL RULES

Recording of telephone conversations

4.39 Subject to paragraph 4.40 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.

4.40 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, 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 Covert Surveillance code of practice).

Use of covert human intelligence source with technical equipment

4.41 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 may be obtained in the usual way.

4.42 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 should be obtained.

5 OVERSIGHT BY COMMISSIONERS

5.1 The 2000 Act requires the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police and the Ministry of Defence Police and the British Transport Police), NCIS, NCS, HMCE and of the 2000 Act the other public authorities listed in Schedule 1 and in Northern Ireland officials of the Ministry of Defence and HM Forces

5.2 The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within Part II of the 2000 Act by the Security Service, Secret Intelligence Service (SIS), the Governments Communication Headquarters (GCHQ) and the Ministry of Defence and HM Forces (excluding the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police, and in Northern Ireland officials of the Ministry of Defence HM Forces).

5.3 This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

5.4 References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other members of staff to whom such functions have been delegated.

COMPLAINTS

6.1 The 2000 Act establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

6.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

☎ 020 7273 4514

Authorisation levels when knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a source

- **Government Department / Public Authority**	**Authorisation level for when knowledge of Confidential Information is likely to be acquired**	**Authorisation level for when a vulnerable individual or a Juvenile is to be used as a source**

Police Forces - Any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London).	Chief Constable	Assistant Chief Constable
Police Forces - Any police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967	Chief Constable	Assistant Chief Constable
The Metropolitan police force	Assistant Commissioner	Commander
The City of London police force	Commissioner	Commander
The Police Service of Northern Ireland	Deputy Chief Constable	Assistant Chief Constable
The Royal Navy Regulating Branch **Royal Military Police** **Royal Air Force Police**	Provost Marshal Provost Marshal Provost Marshal	Provost Marshal Provost Marshal Provost Marshal
National Criminal Intelligence Service (NCIS)	Director General	Assistant Chief Constable or Assistant Chief Investigation Officer
National Crime Squad (NCS)	Director General or Deputy Director General	Assistant Chief Constable
Serious Fraud Office	Director or Assistant Director	Director or Assistant Director
The Intelligence Services: Government Communications Headquarters Security Service Secret Intelligence Service	 A Director of GCHQ Deputy Director General A Director of the Secret Intelligence Service	A Director of GCHQ Deputy Director General A member of the Secret Intelligence Service not below the equivalent rank to that of a Grade 5 in the Home Civil Service)
HM Forces: Royal Navy Army Royal Air Force	 Rear Admiral Major General Air-Vice Marshall	 Rear Admiral Major General Air-Vice Marshall
HM Customs and Excise	Director Investigation or Regional Heads of Investigation	Band 11 (Intelligence)
Inland Revenue	Deputy Chairman of Inland Revenue	Head of Special Compliance Office

Department for the Environment, Food and Rural Affairs:	Immediate Senior Officer of Head of DEFRA Prosecution Division	Head of DEFRA Prosecution Division
DEFRA Investigation Branch	Immediate Senior Officer of Head of DEFRA Prosecution Division	No
Horticultural Marketing Inspectorate	Immediate Senior Officer of Head of DEFRA Prosecution Division	No
Plant Health and Seed Inspectorate	Immediate Senior Officer of Head of DEFRA Prosecution Division	No
Egg Marketing Inspectorate	Immediate Senior Officer of Head of DEFRA Prosecution Division	No
Sea Fisheries Inspectorate (SFI)	Immediate Senior Officer of Head of DEFRA Prosecution Division	Head of DEFRA Prosecution Division
Centre for Environment, Fisheries & Aquaculture Science (CEFAS)		
Ministry of Defence		
Department for Transport, Local Government and the Regions:		
Vehicle Inspectorate	No	No
Transport Security (Transec)	Director of Transport Security	Deputy Director of Transport Security
Department of Health:		
Medical Devices Agency	Chief Executive	No
Medicine Control Agency	Chief Executive	Head of Division for Inspection and Enforcement
Welfare Foods Policy Unit	Deputy Chief Medical Officer	No
Directorate of Counter Fraud Services (DFCS)	Director of Counter Fraud	Director of Counter Fraud
Home Office:		
HM Prison Service	Deputy Director General	Area Managers
Immigration Service	Chief Inspector	Director

Department of Work and Pensions: Benefits Agency	Chief Executive	Head of Fraud Investigation
Department of Trade and Industry: Radiocommunications Agency British Trade International Coal Health Claims Unit Companies Investigation Branch Legal Services Directorate D	No No Director of Coal Health Claims unit The Inspector of Companies The Director of Legal Service D	No No No The Inspector of Companies The Director of Legal Service D
National Assembly for Wales	Health - Director, NHS Wales Agriculture - Head, National Assembly for Wales Agriculture Department	Health - Director, NHS Wales Agriculture - Head, National Assembly for Wales Agriculture Department
Local Authorities	The Head of Paid Service or (in his absence) a Chief Officer	The Head of Paid Service or (in his absence) a Chief Officer
Environment Agency	Chief Executive	Executive Managers
Financial Services Authority	Chairman	Chairman
Food Standards Agency	Head of Group, Deputy Chief Executive and Chief Executive	Head of Group, Deputy Chief Executive and Chief Executive
The Intervention Board for Agricultural Produce	Chief Executive	Legal Director
Personal Investment Authority	Chairman	Chairman
Post Office	Director of Security	Head of Corporate Security/Head of Security for the Royal Mail/Head of Security for Counter Business

Page created 1 August 2002