



SCOTTISH EXECUTIVE

COVERT HUMAN INTELLIGENCE SOURCES

CODE OF PRACTICE

This code is issued by the Scottish Ministers under section 24(1) of the Regulation of Investigatory Powers (Scotland) Act 2000 relating to the exercise and performance of the powers and duties that are conferred or imposed by or under the Act.

Commencement

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

CONTENTS

Chapter 1: GENERAL

Chapter 2: RELATIONSHIP WITH THE UK REGULATION OF INVESTIGATORY POWERS ACT 2000

Chapter 3: GENERAL RULES ON AUTHORISATIONS

Chapter 4: SPECIAL RULES ON AUTHORISATIONS

Chapter 5: AUTHORISATION PROCEDURES FOR COVERT HUMAN INTELLIGENCE SOURCES

Chapter 6: OVERSIGHT BY COMMISSIONERS

Chapter 7: COMPLAINTS

Annex A: 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

1 GENERAL

1.1 In this code the:

- “**1997 Act**” means the Police Act 1997;
- “**2000 Act**” means the Regulation of Investigatory Powers Act 2000;
- “**RIP(S) Act**” means the Regulation of Investigatory Powers (Scotland) Act 2000.

1.2 This code of practice (“the code”) provides guidance on the authorisation of the use or conduct of covert human intelligence sources (“a source”) by public authorities listed in section 8(3) of the RIP(S) Act.

1.3 The provisions of the RIP(S) 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 the RIP(S) Act nor this code is intended to affect the practices and procedures surrounding criminal participation of sources (i.e. a covert human intelligence source will not be excused from any criminal conduct simply by virtue of his status, subject to paragraph 3.10 below).

1.5 The RIP(S) Act provides that all codes relating to the RIP(S) 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 RIP(S) Act, it must be taken into account.

Use of material in evidence

1.6 The admissibility of evidence obtained from a source in Scotland depends on whether evidence has been lawfully and fairly obtained. This will be decided in accordance with principles of common law. The product of the surveillance described in this code is subject to both common law provisions relating to disclosure and statutory provisions relating to retention of documents after trials. Specifically in relation to disclosure, the Crown has a duty to disclose any exculpatory evidence in their possession (see *McLeod petitioner* 1988 SLT 233). There is, however, no duty upon the Crown to disclose every document in their possession which may be relevant to the case.

2 RELATIONSHIP WITH THE UK REGULATION OF INVESTIGATORY POWERS ACT 2000

2.1 The 2000 Act is the appropriate legislation for authorisation of a source whose use or conduct:

- a. will mainly take place outwith Scotland; or
- b. will start outwith Scotland; or
- c. is for reserved purposes such as national security or economic well-being.

2.2 Where the conduct authorised is likely to take place in Scotland, authorisation should be granted under the RIP(S) Act, unless the authorisation is being obtained by certain public authorities (see section 46 of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000; SI No. 2418). The RIP(S) Act is the appropriate legislation and should be used by Scottish public authorities for all other use or conduct of covert human intelligence sources. (See paragraphs 5.39 and 5.40 in relation to the recording of telephone or other conversations).

2.3 The 2000 Act contains provisions to allow cross border operations. An authorisation under the RIP(S) Act will allow Scottish public authorities to use or conduct a source anywhere within the UK for a period of up to 3 weeks at a time (see section 76(2) of the 2000 Act). This 3-week period will restart each time the border is crossed by the source, provided it remains within the original validity period of the authorisation.

2.4 The 2000 Act authorises the conduct or use of a source in Scotland by public authorities (listed in Schedule 1 of the 2000 Act) other than those specified in section 8(3) of the RIP(S) Act or designated by an Order under section 8(4).

2.5 Authorisations under the 2000 and RIP(S) Acts can also be given for surveillance outside the United Kingdom. Authorisations for actions outside the United Kingdom can only validate them for the purposes of legal proceedings in the UK. The requirements of the country outside the United Kingdom in which the investigation or operation is taking place will have to be separately addressed.

2.6 A separate code of practice, pursuant to section 71 of the 2000 Act, applies in relation to authorisations made under that Act. That code of practice is extended to Scotland in relation to authorisations made under Part II of the 2000 Act which apply to Scotland.

3 GENERAL RULES ON AUTHORISATIONS

3.1 An authorisation under the RIP(S) 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.

3.2 The RIP(S) Act does not impose a requirement on public authorities to seek or obtain an authorisation where, under the RIP(S) Act, one is available (see section 30 of the RIP(S) 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 RIP(S) Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

3.3 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

3.4 Obtaining an authorisation under the RIP(S) 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 RIP(S) Act first requires that the person granting an authorisation is satisfied that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 7(3) of the RIP(S) Act.

3.5 Then, if the use of the source is necessary, the person granting the authorisation must be satisfied 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

3.6 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 or investigation.

3.7 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.

3.8 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 a new authorisation is required.

3.9 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 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.

3.10 In a very limited range of circumstances an authorisation under the RIP(S) Act may, by virtue of sections 1(7) and 5 of RIP(S) Act, render lawful conduct which would otherwise be unlawful, if it is incidental to any conduct falling within section 1(8) of the RIP(S) 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. Consideration should also be given to consultation with the Procurator Fiscal. 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

3.11 A single authorisation may combine two or more different authorisations under the RIP(S) 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. Reference should also be made to paragraph 5.41 of this code which deals with the use of a covert human intelligence source with technical equipment.

Directed surveillance against a potential source

3.12 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 1(2) of the RIP(S) Act. See the code of practice on Covert Surveillance.

Central record of all authorisations

3.13 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.

3.14 Proper records must be kept of the authorisation and use of a source. Section 7(6) of the RIP(S) 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) (Scotland) Regulations 2002; SSI No. 205 details the particulars that must be included in the records relating to each source.

3.15 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; and
- the date and time when any instruction was given by the authorising officer to cease using a source.

3.16 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

3.17 Where the product obtained from a source could be relevant to pending or future criminal or civil proceedings, it should be retained for a suitable further period and its retention reviewed at a future date.

3.18 There is nothing in the RIP(S) 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.

4 SPECIAL RULES ON AUTHORISATIONS

Confidential information

4.1 The RIP(S) 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 includes matters subject to legal privilege, confidential personal information and confidential journalistic material.

4.2 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

4.3 In Scotland, the law relating to legal privilege rests on common law principles. In general communications between professional legal advisers and their clients will be subject to legal privilege unless they are intended for the purpose of furthering a criminal act or to obtain advice thereon.

4.4 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, for example, 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.

4.5 The RIP(S) 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. In criminal proceedings, the admissibility of legally privileged material obtained from a source will require to be determined by the courts. Accordingly, action which may lead to such information being obtained is subject to additional safeguards under this code.

4.6 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 circumstances. 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. In addition, 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.

4.7 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 under section 7 of the RIP(S) 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.

4.8 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.

4.9 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. These arrangements are without prejudice to the role of the Procurator Fiscal in the investigation of crime and the role of the courts to determine the admissibility of any evidence for which privilege is claimed.

Communications involving confidential personal information and confidential journalistic material

4.10 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.

4.11 Confidential personal information is information held in confidence relating to the physical or mental health. 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.

4.12 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. Journalists have a restricted right not to disclose a source of information which is regulated by section 10 of the Contempt of Court Act 1981. The journalist's right is restricted by the fact that such disclosure can be ordered by the court if it is satisfied that it is necessary in the interests of justice, or national security or for the prevention of disorder or crime.

Vulnerable individuals

4.13 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

4.14 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) (Scotland) Order 2002; SSI No. 206 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.

5 AUTHORISATION PROCEDURES FOR COVERT HUMAN INTELLIGENCE SOURCES

- 5.1 Under section 1(7) of the RIP(S) Act a person is a source if the person:
- a. 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. covertly uses such a relationship to obtain information or to provide access to any information to another person; or
 - c. covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

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

5.3 By virtue of section 1(8)(b) of the RIP(S) 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.

5.4 By virtue of section 1(8)(c) of the RIP(S) Act a relationship is used covertly, and information obtained as mentioned in paragraph 5.1(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.

5.5 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.

5.6 The conduct of a source is any conduct falling within section 7(5) of the RIP(S) Act, or which is incidental to anything falling within section 7(5) of the RIP(S) Act.

Authorisation procedures

5.7 Under section 7(3) of the RIP(S) Act an authorisation for the use or conduct of a source may be granted by the authorising officer where that person is satisfied that the authorisation is necessary:

- for the purpose of preventing or detecting crime¹ or of preventing disorder;

¹ Detecting crime is defined in section 31(8) of RIP(S) Act.

- in the interests of public safety;
- for the purpose of protecting public health²;
- for any other purpose prescribed in an order made by the Scottish Ministers³.

5.8 The authorising officer must also be satisfied that the authorised use or conduct of a source is proportionate to what is sought to be achieved by that use or conduct.

5.9 The public authorities entitled to authorise the use or conduct of a source are those listed in section 8(3) of the RIP(S) 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 7 of the RIP(S) Act to grant an authorisation for the use or conduct of a source. The Regulation of Investigatory Powers (Prescriptions of Offices, Ranks and Positions) (Scotland) Order 2000; SSI No. 343 designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases. In certain circumstances the Scottish Ministers will be the authorising officer (see section 8(2) of RIP(S) Act).

5.10 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.

5.11 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.

5.12 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 authorising officers authorise their own activity the authorisation record (see paragraphs 3.13 – 3.16) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

² This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

³ This could only be for a purpose which satisfies the criteria set out in Article 8(2) of ECHR.

5.13 The authorising officers within the police and the SDEA may only grant authorisations on application by a member of their own force or Agency.

Information to be provided in applications for authorisation

5.14 An 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 7(3) of the RIP(S) 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.

5.15 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.

5.16 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

5.17 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.

5.18 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

5.19 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 3.13 – 3.16). 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.

5.20 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

5.21 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 5.19.

5.22 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**.

5.23 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 3.13 - 3.16).

5.24 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 5.14;
- 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

5.25 The authorising officer who granted or renewed the authorisation must cancel it if the authorising officer 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) (Scotland) Order 2002; SSI No. 207). 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

5.26 Tasking is the assignment given to the source by the persons defined at sections 7(6)(a) and (b) of the RIP(S) 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.

5.27 The person referred to in section 7(6)(a) of the RIP(S) 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.

5.28 The person referred to in section 7(6)(b) of the RIP(S) Act will be responsible for the general oversight of the use of the source.

5.29 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.

5.30 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.

5.31 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 be cancelled and a new authorisation should be obtained before any further such action is carried out.

5.32 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 7(6)(a) or (b) of the RIP(S) 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

5.33 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 7(6)(a) and (b) of the RIP(S) Act for each source.

5.34 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.

5.35 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

5.36 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.

5.37 The person defined at section 7(6)(a) of the RIP(S) Act is responsible for bringing to the attention of the person defined at section 7(6)(b) of the RIP(S) 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.

5.38 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

5.39 Subject to paragraph 5.40 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 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.

5.40 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 5 of the Covert Surveillance code of practice).

Use of covert human intelligence source with technical equipment

5.41 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.

5.42 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.

6 OVERSIGHT BY COMMISSIONERS

6.1 The 1997, RIP(S) and 2000 Acts require 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 the RIP(S) Act by the police and the SDEA, and under the RIP(S) Act the other public authorities listed in section 8(3).

6.2 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 the Commissioner requires for the purpose of enabling him to carry out his functions.


6.3 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.

7 COMPLAINTS

7.1 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, including cases to which the RIP(S) Act applies.

7.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaint 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

<u>Relevant Public Authorities</u>	<u>Authorisation level for when knowledge of Confidential Information is likely to be acquired</u>	<u>Authorisation level for when a vulnerable individual or a Juvenile is to be used as a source</u>
Police Forces - Any police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967.	Chief Constable	Assistant Chief Constable
Scottish Drug Enforcement Agency (SDEA)	Chief Constable for the area in which the proposed activity is to be undertaken	Director
The Scottish Executive Environment and Rural Affairs Department		
Agricultural Staff	Chief or Assistant Chief Agricultural Officer	Assistant Chief Agricultural Officer
Scottish Agricultural Science Agency	Director or Deputy Director	Deputy Director
Scottish Fisheries Protection Agency	Chief Executive or Director, Corporate Strategy	Chief Executive or Director, Corporate Strategy
The Scottish Executive Health Department		
Welfare Foods	Member of the Senior Civil Service	Member of the Senior Civil Service
The Scottish Executive Justice Department		
Accountant in Bankruptcy	Accountant in Bankruptcy	Accountant in Bankruptcy
Scottish Prison Service (including contracted out prisons)	Chief Executive or Director of Operations	
The Scottish Executive Enterprise and Lifelong Learning Department		
Innovation and Support	Member of the Senior Civil Service	Member of the Senior Civil Service
A Council constituted under section 2 of the Local Government etc. (Scotland) Act 1994	Chief Executive or (in their absence) a Chief Officer	Chief Executive or (in their absence) a Chief Officer
NHS Bodies in Scotland:		
The Common Services Agency for the Scottish Health Service	Chief Executive	Chief Executive
A Health Board	Chief Executive	Chief Executive
A Special Health Board	Chief Executive	Chief Executive
A National Health Service Trust established under section 12A of the National Health Service (Scotland) Act 1978	Chief Executive	Chief Executive

<u>Relevant Public Authorities</u>	<u>Authorisation level for when knowledge of Confidential Information is likely to be acquired</u>	<u>Authorisation level for when a vulnerable individual or a Juvenile is to be used as a source</u>
The Scottish Environment Protection Agency	Chief Executive	Chief Executive