



# **COVERT SURVEILLANCE**

## **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 and Part III of the Police Act 1997 insofar as relating to a police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967.

### **Commencement**

This code applies to every authorisation of covert surveillance carried out under the Regulation of Investigatory Powers (Scotland) Act 2000 or Part III of the Police Act 1997 which begins on or after the day on which this codes 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 DIRECTED SURVEILLANCE**

**Chapter 6: AUTHORISATION PROCEDURES FOR INTRUSIVE SURVEILLANCE**

**Chapter 7: AUTHORISATION PROCEDURES FOR ENTRY ON AND INTERFERENCE WITH PROPERTY OR WIRELESS TELEGRAPHY**

**Chapter 8: OVERSIGHT BY COMMISSIONERS**

**Chapter 9: COMPLAINTS**

**Annex A: AUTHORISATION LEVELS WHEN KNOWLEDGE OF CONFIDENTIAL INFORMATION IS LIKELY TO BE ACQUIRED**

# 1 GENERAL

1.1 In this code the:

- “**1967 Act**” means the Police (Scotland) Act 1967
- “**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 use of covert surveillance by public authorities under the RIP(S) Act and on entry on or interference with property (or wireless telegraphy) under Part III of the 1997 Act. This code replaces the code of practice issued in 1999 pursuant to section 101(3) of the 1997 Act.

1.3 General observation forms part of the duties of many law enforcement officers and other public authorities and is not usually regulated by the RIP(S) Act. For example, police officers will be on patrol to prevent and detect crime, maintain public safety and prevent disorder. Trading standards officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

1.4 Although the provisions of the RIP(S) Act or of this code do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for intrusive or directed surveillance may be necessary.

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 through covert surveillance 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.

### **Directed surveillance, intrusive surveillance and entry on or interference with property or with wireless telegraphy**

1.7 Directed surveillance is defined in section 1(2) of the RIP(S) Act as surveillance, which is covert but not intrusive, and undertaken:

- a. for the purposes of a specific investigation or specific operation;
- b. in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- c. otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under the RIP(S) Act to be sought for the carrying out of the surveillance.

1.8 Directed surveillance investigations or operations can only be carried out by those public authorities that are listed in or added to section 8(3) of the RIP(S) Act.

1.9 Intrusive surveillance is defined in section 1(3) of the RIP(S) Act as covert surveillance that:

- a. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

1.10 Applications to a Surveillance Commissioner for approval of a grant of authorisation to carry out intrusive surveillance can only be made by the senior authorising officer, which means the Chief Constable of a police force or by their designated deputy.

1.11 Applications to enter on or interfere with property or with wireless telegraphy can only be made by the authorising officers of those public authorities listed in or added to section 93(5) of the 1997 Act.

## **2 RELATIONSHIP WITH THE UK REGULATION OF INVESTIGATORY POWERS ACT 2000**

2.1 The 2000 Act is the appropriate legislation for the authorisation of surveillance which:

- 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, authorisations 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 surveillance (see paragraphs 5.29 - 5.31 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 conduct surveillance 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, provided it remains within the original validity period of the authorisation.

2.4 The 2000 Act authorises surveillance operations 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 the 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 a public authority to carry out covert surveillance. Responsibility for authorising surveillance operations will vary, depending on whether the authorisation is for intrusive surveillance or directed surveillance, and which public authority is involved. For the purposes of Chapter 3 and 4 of this code the authorising officer, senior authorising officer or the person who makes an application to the Scottish Ministers will be referred to as an 'authorising officer'.

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 source of lawful authority, the consequence 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 surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that 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 and the 1997 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. 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 6(3) of the RIP(S) Act for directed surveillance and in section 10(2)(a) of the RIP(S) Act for intrusive surveillance.

3.5 Then, if the activities are necessary, the person granting the authorisation must be satisfied that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity 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. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

#### **Collateral Intrusion**

3.6 Before authorising surveillance 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 investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

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 surveillance.

3.8 Those carrying out the surveillance 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 particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. In this regard, it is recommended that where authorising officers consider that conflicts might arise they should consult a senior officer within the police force area in which the investigation or operation takes place.

3.10 The matters in paragraphs 3.1 – 3.9 above must also be taken into account when applying for authorisations or warrants for entry on or interference with property or with wireless telegraphy. In particular they must be necessary in the circumstances of the particular case for the statutory ground listed in section 93(2)(a) of the 1997 Act, proportionate and when exercised steps should be taken to minimise collateral intrusion.

### **Combined authorisations**

3.11 A single authorisation may combine:

- two or more different authorisations under the RIP(S) Act;
- an authorisation under the RIP(S) Act and an authorisation under Part III of the 1997 Act.

3.12 For example, a single authorisation may combine authorisations for directed surveillance and intrusive surveillance. The provisions applicable in the case of each of the authorisations must be considered separately. Thus, a police superintendent can authorise directed surveillance but the intrusive surveillance needs the separate authority of a Chief Constable, and in certain cases the approval of a Surveillance Commissioner will also be necessary.

3.13 In cases where one agency is acting on behalf of another, it is normally for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by the Armed Forces on behalf of the police, authorisations would be sought by the police and granted by the appropriate authorising officer. However, in cases where the Security Service is acting in

support of the police or other law enforcement agencies in the field of serious crime, authorisations would normally be sought by the Security Service.

### **Central record of all authorisations**

3.14 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 and should contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorisation was cancelled.

3.15 In all cases, the relevant authority should maintain the following documentation which need not form part of the centrally retrievable record:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

- the date and time when any instruction was given by the authorising officer.

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

3.16 Where the product of surveillance 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.

3.17 There is nothing in the RIP(S) Act which prevents material obtained from properly authorised surveillance from 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 covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

## 4 SPECIAL RULES ON AUTHORISATIONS

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 or confidential journalistic material.

4.2 In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. Annex A lists the authorising officer for each public authority permitted to authorise such surveillance.

### **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 surveillance 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 by surveillance will require to be determined by the courts. Accordingly, action which may lead to such information being acquired is subject to additional safeguards under this code.

4.6 In general, an application for surveillance 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 surveillance raises. The application should include, in addition to the reasons why it is considered necessary for the surveillance to take place, 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 surveillance is to obtain legally privileged information.

4.7 This assessment will be taken into account by the authorising officer in deciding whether the proposed surveillance is necessary and proportionate under

section 6 of the RIP(S) Act for directed surveillance and under section 10 for intrusive surveillance. 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 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.

## **5 AUTHORISATION PROCEDURES FOR DIRECTED SURVEILLANCE**

5.1 Directed surveillance is defined in section 1(2) of the RIP(S) Act as surveillance which is covert, but not intrusive (as defined in section 1(3) of the RIP(S) Act), and is undertaken:

- a. for the purposes of a specific investigation or specific operation;
- b. in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- c. otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under the Act to be sought for the carrying out of the surveillance.

5.2 Covert surveillance is defined in section 1(8)(a) of the RIP(S) Act as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

5.3 Private information is defined in section 1(9) of the RIP(S) Act as including any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. Family life should be treated as extending beyond the formal relationships created by marriage.

5.4 Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that the officer came across in the course of a patrol.

5.5 By virtue of section 48(4) of the 2000 Act, surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication (as the case may be). For further details see paragraphs 5.29 - 5.31 of this code.

5.6 Surveillance in residential premises or in private vehicles is defined as intrusive surveillance in section 1(3) of the RIP(S) Act and is dealt with in Chapter 6 of this code. However, where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is classed as directed surveillance and should be authorised accordingly.

5.7 Directed surveillance does not include entry on or interference with property or with wireless telegraphy. These activities are subject to a separate regime of authorisation as set out in Chapter 7 of this code.

5.8 Directed surveillance includes covert surveillance within office premises, (as defined in paragraph 7.31 of this code). Authorising officers are reminded that confidential information should be afforded an enhanced level of protection. Chapter 4 of this code provides that in cases where the likely consequence of surveillance is to acquire confidential information, the authorisation should be given at a higher level.

### **Authorisation procedures**

5.9 Under section 6(3) of the RIP(S) Act an authorisation for directed surveillance may be granted by an authorising officer where the authorising officer is satisfied that the authorisation is necessary in the circumstances of the particular case:

- for the purpose of preventing or detecting<sup>1</sup> crime or of preventing disorder;
- in the interests of public safety;
- for the purpose of protecting public health<sup>2</sup>.

5.10 The authorising officer must also believe that the surveillance is proportionate to what it seeks to achieve.

5.11 The public authorities entitled to authorise directed surveillance are listed in section 8(3) of the RIP(S) Act. Responsibility for authorising the carrying out of directed surveillance rests with the authorising officer and requires the personal authority of the authorising officer. The Regulation of Investigatory Powers (Prescriptions of Offices, Ranks and Positions) (Scotland) Order 2000; SI No. 343 (as amended) designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases.

5.12 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.

5.13 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 investigation or operation for which the authorisation was being given.

---

<sup>1</sup> Detecting crime is defined in section 31(8) of the RIP(S) Act and is applied to the 1997 Act by section 134 of that Act (as amended).

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

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.

5.14 Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently. Where an authorising officer authorises such an investigation or operation the central record of authorisations (see paragraphs 3.14 - 3.15) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

5.15 Authorising officers within the police may only grant authorisations on applications by a member of their own force (except in the case of applications for intrusive surveillance which may be granted by authorising officers to officers seconded to the Scottish Drug Enforcement Agency (the successor organisation to the Scottish Crime Squad) as specified in section 9 of the RIP(S) Act).

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

5.16 A written application for authorisation for directed surveillance should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- 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 6(3) of the RIP(S) Act;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- 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 surveillance;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

5.17 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.

5.18 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**

5.19 A written authorisation granted by an authorising officer will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

5.20 Urgent oral authorisations or written authorisations granted 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**

5.21 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations (see paragraphs 3.14 - 3.15). Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

5.22 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**

5.23 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, the authorisation may be renewed in writing for a further period of **three months**. Renewals may also be granted orally in urgent cases and last for a period of **seventy-two hours**.

5.24 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, provided they continue to meet the criteria for authorisation.

5.25 All applications for the renewal of an authorisation for directed surveillance 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 5.16;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

5.26 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations (see paragraphs 3.14 - 3.15).

### **Cancellations**

5.27 The authorising officer who granted or last renewed the authorisation must cancel it if the authorising officer is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. 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) Regulations 2000; SSI No. 207).

### **Ceasing of surveillance activity**

5.28 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central record of authorisations (see paragraphs 3.14 - 3.15) and the notification of cancellation where relevant.

## **ADDITIONAL RULES**

### **Recording of telephone conversations**

5.29 Subject to paragraph 5.30 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.

5.30 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.

5.31 The use of a surveillance device should not be ruled out simply because it may incidentally pick up one or both ends of a telephone conversation, and any such product can be treated as having been lawfully obtained. However, its use would not be appropriate where the sole purpose is to overhear speech which, at the time of monitoring, is being transmitted by a telecommunications system. In such cases an application should be made for an interception of communication warrant under section 5 of the 2000 Act.

## **6 AUTHORISATION PROCEDURES FOR INTRUSIVE SURVEILLANCE**

6.1 Intrusive surveillance is defined in section 1(3) of the RIP(S) Act as covert surveillance that:

- a. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

6.2 Covert surveillance is defined in section 1(8)(a) of the RIP(S) Act as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

6.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises would not be considered as intrusive surveillance.

6.4 Residential premises are defined in section 31(1) of the RIP(S) Act. The definition includes hotel rooms, bedrooms in barracks, and police and prison cells but not any common area to which a person is allowed access in connection with his occupation of such accommodation e.g. a hotel lounge.

6.5 A private vehicle is defined in section 31(1) of the RIP(S) Act as any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it. A person does not have a right to use a motor vehicle if his right to use it derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey.

6.6 In many cases, a surveillance operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. In such cases, both activities need authorisation. This can be done as a combined authorisation (see paragraph 3.11).

6.7 An authorisation for intrusive surveillance may be issued by a Chief Constable. All authorisations require the personal authority of the Chief Constable and, under section 10(2) of the RIP(S) Act a Chief Constable may not authorise intrusive surveillance unless that Chief Constable is satisfied that:

- a. the authorisation is necessary for the purpose of preventing or detecting serious crime; and

- b. the surveillance is proportionate to what is sought to be achieved by carrying it out.

6.8 A factor which must be taken into account in deciding whether an authorisation is necessary and proportionate is whether the information which it is thought necessary to obtain by means of the intrusive surveillance could reasonably be obtained by other less intrusive means.

### **Authorisation procedures**

6.9 The Chief Constable should generally give authorisations in writing. However, in urgent cases, they may be given orally. In an urgent oral case, a statement that the Chief Constable has expressly authorised the conduct should be recorded in writing by the applicant as soon as is reasonably practicable.

6.10 If the Chief Constable is absent then as provided for in section 5(4) of the Police (Scotland) Act 1967, an authorisation can be given in writing or, in urgent cases, orally by the designated deputy.

6.11 In an urgent case, where it is not reasonably practicable having regard to the urgency of the case for the designated deputy to consider the application, a written authorisation may be granted by an Assistant Chief Constable entitled to act under section 12(4) of the RIP(S) Act.

6.12 A case is not normally to be regarded as urgent unless the time that would elapse before the Chief Constable was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation 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.

6.13 The consideration of an authorisation by the Chief Constable is only to be regarded as not reasonably practicable (within the meaning of section 12(2) of the RIP(S) Act) if the Chief Constable is on annual leave, is absent from the office and home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not normally to be regarded as rendering it impracticable for a Chief Constable to consider an application. Where a designated deputy gives an authorisation this should be made clear and the reason for the absence of the Chief Constable given.

6.14 Applications to the Chief Constable for authorisation must be made in writing by a member of that officer's own force or by a constable seconded to the Scottish Drug Enforcement Agency (or a successor organisation as specified in section 9 of the RIP(S) Act). Where the surveillance is carried out in relation to any residential premises, the authorisation cannot be granted unless the residential premises are within the area of operation of that police force.

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

6.15 Applications should be in writing and describe the conduct to be authorised and the purpose of the investigation or operation. The application should specify:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purposes of preventing or detecting serious crime) listed in section 10(2) of the RIP(S) Act;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the residential premises or private vehicle in relation to which the surveillance will take place;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential material that is likely to be obtained as a result of the surveillance; and
- a subsequent record should be made of whether authority was given or refused, by whom and the time and date.

6.16 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the Chief Constable or designated deputy 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 Chief Constable or the designated deputy.

6.17 Where the application is oral, the detail referred to above should be recorded in writing as soon as reasonably practicable.

## **Approval of Surveillance Commissioners**

6.18 Except in urgent cases, an authorisation granted for intrusive surveillance will not take effect until it has been approved by a Surveillance Commissioner and written notice of the Commissioner's decision has been given to the person who granted the authorisation (see section 14(1) of the RIP(S) Act). This means that the

approval will not take effect until the notice has been received in the office of the person who granted the authorisation within the relevant force.

6.19 When the authorisation is urgent, it will take effect from the time it is granted provided notice is given to the Surveillance Commissioner in accordance with section 13(4)(b) (see section 14(2) of the RIP(S) Act).

6.20 There may be cases that become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the authorising officer should notify the Surveillance Commissioner that the case is now urgent (pointing out that it has become urgent since the notification). In these cases, the authorisation will take effect immediately.

### **Notifications to Surveillance Commissioners**

6.21 Where a person grants, renews or cancels an authorisation, that person must, as soon as is reasonably practicable, give notice of it in writing to a Surveillance Commissioner, in accordance with whatever arrangements have been made by the Chief Surveillance Commissioner.

6.22 In urgent cases, the notification must specify the grounds on which the case is believed to be one of urgency. The urgency provisions should not be used routinely. If the Surveillance Commissioner is satisfied that there were no grounds for believing the case to be one of urgency, he has the power to quash the authorisation.

6.23 The information to be included in the notification to the Surveillance Commissioner is set out in the Regulation of Investigatory Powers (Notification of Authorisations etc.) (Scotland) Order 2000; SSI No. 340.

### **Duration of authorisations**

6.24 A written authorisation granted by a Chief Constable or a designated deputy will cease to have effect (unless renewed) at the end of a period of **three** months, beginning with the day on which it took effect.

6.25 Oral authorisations given in urgent cases by Chief Constables or their designated deputies will cease to have effect (unless renewed) at the end of the period of **seventy-two** hours beginning with the time when they took effect.

### **Renewals**

6.26 If at any time before an authorisation expires the Chief Constable or, in his/her absence, the designated deputy considers the authorisation should continue to have effect for the purpose for which it was issued, he/she may renew it in writing for a further period of **three months**.

6.27 As with the initial authorisation, the Chief Constable must (unless it is a case to which the urgency procedure applies) seek the approval of a Surveillance Commissioner. This means that the renewal will not take effect until the notice of it has been received in the office of the person who granted the authorisation (but not

before the day on which the authorisation would have otherwise ceased to have effect). In urgent cases, a renewal can take effect immediately (provided this is not before the day on which the authorisation would have otherwise ceased to have effect). See sections 13 and 14 of the RIP(S) Act and The Regulation of Investigatory Powers (Notification of Authorisations etc.) (Scotland) Order 2000 SSI No: 340).

6.28 All applications for a 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 listed in paragraph 6.15 ;
- the reasons why it is necessary to continue with the intrusive surveillance;
- the content and value to the investigation or operation of the product so far obtained by the surveillance; and
- the results of regular reviews of the investigation or operation.

## **Reviews**

6.29 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisation record (see paragraphs 3.14-3.15). Particular attention is drawn to the need to review authorisations frequently where the intrusive surveillance provides access to confidential material or involves collateral intrusion.

6.30 The senior authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

## **Cancellations**

6.31 The senior authorising officer who granted or last renewed the authorisation must cancel it if that officer is satisfied that the surveillance no longer meets the criteria upon which it was authorised. Where the senior authorising officer is no longer available, this duty will fall on the person who has taken over the role of senior authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) (Scotland) Regulations 2002; SSI No. 207).

6.32 Surveillance Commissioners must be notified where authorisations are cancelled (see The Regulation of Investigatory Powers (Notification of Authorisations etc.) (Scotland) Order 2000; SSI No. 340).

## **Ceasing of surveillance activity**

6.33 As soon as the decision is taken that the intrusive surveillance should be discontinued, instructions must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be

recorded in the central record of authorisation (see paragraphs 3.14-3.15) and the notification of cancellation where relevant.

6.34 In cases where an authorisation is quashed or cancelled by a Surveillance Commissioner, the senior authorising officer must immediately instruct those carrying out the surveillance to stop monitoring, observing, listening or recording the activities of the subject of the authorisation. The date and time when such an instruction was given should be recorded on the central record or authorisation (see paragraphs 3.14-3.15).

## **7 AUTHORISATION PROCEDURES FOR ENTRY ON OR INTERFERENCE WITH PROPERTY OR WITH WIRELESS TELEGRAPHY**

7.1 Part III of the 1997 Act provides lawful authority for entry on or interference with property or wireless telegraphy by the police.

7.2 In many cases a covert surveillance operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. This can be done as a combined authorisation, although the criteria for authorisation of each activity must be considered separately (see paragraph 3.11).

7.3 Responsibility for such authorisations rests with the authorising officer as defined in section 93(5) of the 1997 Act, that is the Chief Constable or equivalent. Authorisations require the personal authority of the authorising officer (or their designated deputy) except in urgent situations, where it is not reasonably practicable for the application to be considered by such a person. The person entitled to act in such cases is set out in section 94 of the 1997 Act.

7.4 Authorisations under the 1997 Act may not be necessary where the police are acting with the consent of a person able to give permission in respect of relevant property. However consideration should still be given to the need to obtain an authorisation under the RIP(S) Act.

7.5 Authorisations may only be given by an authorising officer on application by a member of his or her own force for entry on or interference with property or with wireless telegraphy within the authorising officer's own area of operation. However, an authorising officer may authorise the taking of action outside the relevant area solely for the purpose of maintaining or retrieving any device, apparatus or equipment.

7.6 Any person giving an authorisation for entry on or interference with property or with wireless telegraphy under section 93(2) of the 1997 Act must be satisfied that:

- it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime; and
- that the taking of the action is proportionate to what the action seeks to achieve.

7.7 The authorising officer must take into account whether what it is thought necessary to achieve by the authorised conduct could reasonably be achieved by other means.

7.8 Any person granting or applying for an authorisation to enter on or interfere with property or with wireless telegraphy will also need to be aware of particular sensitivities in the local community where entry or interference is taking place and of similar activities being undertaken by other public authorities which could impact on

the deployment. In this regard, it is recommended that the authorising officers should consult a senior officer within the police force in which the investigation or operation takes place, where the authorising officer considers that conflicts might arise.

### **Authorisation procedures**

7.9 Authorisations will generally be given in writing by the authorising officer. However, in urgent cases, they may be given orally by the authorising officer. 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. This should be done by the person with whom the authorising officer spoke.

7.10 If the authorising officer is absent then as provided for in section 5(4) of the Police (Scotland) Act 1967, an authorisation can be given in writing or, in urgent cases, orally by the designated deputy.

7.11 Where, however, in an urgent case, it is not reasonably practicable for the designated deputy to consider an application, then written authorisation may be given by an Assistant Chief Constable (other than a designated deputy).

7.12 Applications to the authorising officer for authorisation must be made in writing by a police officer (within the terms of section 93(3) of the 1997 Act) and should specify:

- the identity or identities of those to be targeted (where known);
- the property which the entry or interference with will affect;
- the identity of individuals and/or categories of people, where known, who are likely to be affected by collateral intrusion;
- details of the offence planned or committed;
- details of the intrusive surveillance involved;
- how the authorisation criteria (as set out in paragraphs 7.6 and 7.7) have been met;
- any action which may be necessary to retrieve any equipment used in the surveillance;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an authorisation was given or refused, by whom and the time and date.

7.13 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or designated deputy considered the case so urgent that an oral instead of a written authorisation was given; and
- the reasons why (if relevant) the person granting the authorisation did not consider it reasonably practicable for the application to be considered by the senior authorising officer or the designated deputy.

7.14 Where the application is oral, the information referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

### **Notifications to Surveillance Commissioners**

7.15 Where a person gives, renews or cancels an authorisation, they must, as soon as is reasonably practicable, give notice of it in writing to a Surveillance Commissioner, in accordance with arrangements made by the Chief Surveillance Commissioner. In urgent cases which would otherwise have required the approval of a Surveillance Commissioner, the notification must specify the grounds on which the case is believed to be one of urgency.

7.16 There may be cases which become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the authorising officer should notify the Surveillance Commissioner that the case is urgent (pointing out that it has become urgent since the previous notification). In these cases, the authorisation will take effect immediately.

7.17 Notifications to Surveillance Commissioners in relation to the authorisation, renewal and cancellation of authorisations in respect of entry on or interference with property should be in accordance with the requirements of The Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No. 3241.

### **Duration of authorisations**

7.18 Written authorisations given by authorising officers will cease to have effect at the end of a period of **three months** beginning with the day on which they took effect. In cases requiring prior approval by a Surveillance Commissioner this means from the time the Surveillance Commissioner has approved the authorisation and the person who gave the authorisation has been notified. This means that the approval will not take effect until the notice has been received in the office of the person who granted the authorisation within the relevant police force. In cases not requiring prior approval, this means from the time the authorisation was given.

7.19 Oral authorisations given in urgent cases by:

- authorising officers; or
- designated deputies

and written authorisations given by:

- Assistant Chief Constables (other than a designated deputy).

will cease at the end of the period of **seventy-two** hours beginning with the time when they took effect.

## Renewals

7.20 If at any time before the day on which an authorisation expires the authorising officer or, in his absence, the designated deputy considers the authorisation should continue to have effect for the purpose for which it was issued, the authorisation may be renewed in writing for a period of **three months** beginning with the day on which the authorisation would otherwise have ceased to have effect. Authorisations may be renewed more than once, if necessary, and the renewal should be recorded on the authorisation record (see paragraph 7.27).

7.21 Commissioners must be notified of renewals of authorisations. The information to be included in the notification is set out in The Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No: 3241.

7.22 If, at the time of renewal, the criteria in paragraph 7.30 exist, then the approval of a Surveillance Commissioner must be sought before the renewal can take effect. The fact that the initial authorisation required the approval of a Commissioner before taking effect does not mean that its renewal will automatically require such approval. It will only do so if, at the time of the renewal, it falls into one of the categories requiring approval (and is not urgent).

## Reviews

7.23 Authorising officers should regularly review authorisations to assess the need for the entry on or interference with property or with wireless telegraphy to continue. This should be recorded on the authorisation record (see paragraph 7.27). The authorising officer should determine how often a review should take place when giving an authorisation. This should be as frequently as is considered necessary and practicable and at no greater interval than one month. Particular attention is drawn to the need to review authorisations and renewals regularly and frequently where the entry on or interference with property or with wireless telegraphy provides access to confidential information or involves collateral intrusion.

## Cancellations

7.24 The senior authorising officer who granted or last renewed the authorisation must cancel it must apply for its cancellation, if that officer is satisfied that the authorisation no longer meets the criteria upon which it was authorised. Where the senior authorising officer is no longer available, this duty will fall on the person who has taken over the role of senior authorising officer or the person who is acting as the senior authorising officer (see The Regulation of Investigatory Powers (Cancellation of Authorisations) (Scotland) Regulations 2000; SSI No. 207).

7.25 The Surveillance Commissioners must be notified of cancellations of authorisations. The information to be included in the notification is set out in The Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No. 3421.

7.26 The Surveillance Commissioners have the power to cancel an authorisation if they are satisfied that, at any time after an authorisation was given or renewed, there were no reasonable grounds for believing the matters set out in paragraphs 7.6 and 7.7 above. In such circumstances, a Surveillance Commissioner may order the destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

### **Authorisation record**

7.27 An authorisation record should be created which records:

- the time and date when an authorisation is given;
- whether an authorisation is in written or oral form;
- the time and date when it was notified to a Surveillance Commissioner; and
- the time and date when the Surveillance Commissioner notified his approval (where appropriate).

The authorisation record should also record:

- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the authorisation;
- the date of every renewal; and
- it should record the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy.

### **Ceasing of entry on or interference with property or with wireless telegraphy**

7.28 Once an authorisation or renewal expires or is cancelled or quashed, the authorising officer must immediately instruct those carrying out the surveillance to cease all the actions authorised for the entry on or interference with property or with wireless telegraphy. The time and date when such an instruction was given should be recorded on the authorisation record (see paragraph 7.27).

## **Retrieval of equipment**

7.29 Where a Surveillance Commissioner quashes or cancels an authorisation or renewal, that Surveillance Commissioner will, if there are reasonable grounds for doing so, order that the authorisation remain effective for a specified period, to enable officers to retrieve anything left on the property by virtue of the authorisation. The Surveillance Commissioner can only do so if the authorisation or renewal makes provision for this. A decision by the Surveillance Commissioner not to give such an order can be the subject of an appeal to the Chief Surveillance Commissioner.

## **SPECIAL RULES**

### **Cases requiring prior approval of a Surveillance Commissioner**

7.30 In certain cases, an authorisation for entry on or interference with property will not take effect until a Surveillance Commissioner has approved it and the notice has been received in the office of the person who granted the authorisation within the relevant police force . These are cases where the person giving the authorisation is satisfied that:

- any of the property specified in the authorisation:
  - is used wholly or mainly as a dwelling or as a bedroom in a hotel; or
  - constitutes office premises; or
- the action authorised is likely to result in any person acquiring knowledge of:
  - matters subject to legal privilege;
  - confidential personal information; or
  - confidential journalistic material.

7.31 Office premises are defined as any building or part of a building whose sole or principal use is as an office or for office purposes (which means purposes of administration, clerical work, handling money and telephone or telegraph operation).

## **8 OVERSIGHT BY COMMISSIONERS**

8.1 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).

8.2 This code does not cover the exercise of any of the Commissioners' functions. It will be 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 discharge his functions.


8.3 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.

## 9 COMPLAINTS

9.1 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.

9.2 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

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