



Home Office

COVERT SURVEILLANCE
DRAFT CODE OF PRACTICE

Preliminary draft code: This document is circulated by the Home Office in advance of enactment of the RIP Bill as an indication of current thinking. It will be subject to changes and additions. This circulation is not the publication referred to in clause 69(3) of the Bill, which can only take place after enactment. This is a preliminary draft on which comments are welcomed. Further, informal consultation will be required before the formal consultation process begins under clause 69(3) of the Bill.

FOREWORD

Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals but as a means of protecting the public from harm and preventing crime.

The covert surveillance covered by this code is in two categories: intrusive surveillance and directed surveillance. The code defines the two categories and the authorisation procedures for both. Authorisation for covert surveillance gives lawful authority to carry out surveillance. However, often surveillance operations will also involve interference with property. This requires separate authorisation and Part 5 of this code details the procedures which give lawful authority for the interference with property and wireless telegraphy.

General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime “hot spot” in order to identify and arrest offenders committing crime at that location. Trading standards or HM Customs & Excise 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 or tax. 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. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually require any authorisation under the provisions of the Regulation of Investigatory Powers Act 2000.

Neither do the provisions of the 2000 Act or of this code of practice cover authorisation for the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime.

Neither this foreword nor the guidance notes, which appear in the footnotes, are parts of the code. They are provided to assist police officers and others in its application.

CONTENTS

Section 1: GENERAL

Section 2: AUTHORISATIONS AND PRODUCT

Section 3: DIRECTED SURVEILLANCE

Section 4: INTRUSIVE SURVEILLANCE IN PART II OF 2000 ACT

Section 5: ENTRY ON AND INTERFERENCE WITH PROPERTY AND WIRELESS TELEGRAPHY

Section 6: OVERSIGHT

Section 7: COMPLAINTS AND REDRESS

Section 8: INFORMATION LEAFLET

PRELIMINARY
DRAFT

1 GENERAL

1.1 This code of practice provides guidance on the use of covert surveillance by public authorities under Part II of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"). The code also provides guidance on operations involving interference with property (or wireless telegraphy) under section 5 of the Intelligence Services Act 1994 ("the 1994 Act") or Part III of the Police Act 1997 ("the 1997 Act"). Such activity will often take place as part of a covert surveillance operation. This code replaces the code of practice on Intrusive Surveillance issued pursuant to section 101(3) of the 1997 Act.

1.2 A copy of the code should be readily available, for reference purposes, at public offices of public authorities designated to carry out covert surveillance, and where people are detained in custody. It should also be readily available to any members of a public authority or department who are actively involved in intrusive or directed surveillance operations.

1.3 The 2000 Act provides that the code is 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, it must be taken into account.

General extent of powers

1.4 There is nothing in the 1994 Act, the 1997 Act or Part II of the 2000 Act comparable to **section 16** of Part I of the 2000 Act, the effect of which is to exclude intercept material from being adduced as evidence in court proceedings. The carrying out of the surveillance described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996, where those rules apply to the law enforcement body in question.

1.5 Except where specified in this code, there is no geographical limitation on where covert surveillance can be conducted. Authorisations can be given for covert surveillance taking place both inside and outside the United Kingdom.

Interpretation

1.6 In this code:

- **"confidential material"** has the same meaning and definitions as in the Police Act 1997. It consists of:
 - matters subject to legal privilege;
 - confidential personal information; or

PRELIMINARY DRAFT

–confidential journalistic material.

“Matters subject to legal privilege” includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege¹.

“Confidential personal information” is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

- a) to his/her physical or mental health; or
- b) to spiritual counselling or other assistance given or to be given[to him/her], and

which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office². It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information 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 secrecy contained in existing or future legislation.

“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;

¹ **Guidance note:** Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; 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 shall apply to the provision of professional legal advice by any agency or organisation.

² **Guidance note:** Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- **"covert surveillance"** means 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;
- For the purposes of authorising intrusive surveillance under the 2000 Act or interference with property under the 1997 Act, a **"designated deputy"** means:
 - the person holding the rank of Assistant Chief Constable designated to act for the chief constable under section 12(4) of the Police Act 1996 or section 5(4) of the Police (Scotland) Act 1967;
 - the person designated to act in the absence of the Commissioner of the City of London Police under section 25 of the City of London Police Act 1839³;
 - the person designated to act in the absence of the Director General of the National Criminal Intelligence Service under section 8 of the 1997 Act;
 - the person designated to act in the absence of the Director General and Deputy Director General of the National Crime Squad under section 54 of the 1997 Act;

The "designated deputy" may act as "authorising officer" only in the circumstances outlined in section 12(4) of the Police Act 1996, section 5(4) of the Police (Scotland) Act 1967, section 25 of the City of London Police Act 1839, or sections 8 and 54 of the 1997 Act;

- **"Intelligence Services Commissioner"** is the person who holds or has held high judicial office and who has been appointed by the Prime Minister to undertake functions specified in the 2000 Act in relation to the Security Service, the Secret Intelligence Service and GCHQ and to the Ministry of Defence and HM Armed Forces (excluding the Ministry of Defence and HM Armed Forces in Northern Ireland);
- **"private information"** includes information about a person relating to his private or family life;
- **"private vehicle"** means any vehicle which is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use the vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft;

³ **Guidance note:** This will be the Assistant Commissioner of the City of London Police.

PRELIMINARY DRAFT

- For the purposes of authorising intrusive surveillance in residential premises under the 2000 Act and of authorising interference with property under the 1997 Act, “**relevant area**” or “**area of operation**”. means
 - in relation to a police force maintained under section 2 of the Police Act 1996, of the Metropolitan Police Service or the City of London Police, the area in England and Wales for which that force is maintained;
 - in relation to a police force maintained under section 1 of the Police (Scotland) Act 1967, the area in Scotland for which that force is maintained;
 - in relation to the Royal Ulster Constabulary, Northern Ireland;
 - in relation to the National Criminal Intelligence Service and the British Transport Police, the United Kingdom;
 - in relation to the National Crime Squad, England and Wales;
 - in relation to the Ministry of Defence Police, any premises where members of that force, under section 2 of the Ministry of Defence Police Act 1987, have the powers and privileges of a constable;
 - in relation to the Service Police, any premises owned or occupied by, or used for residential purposes by a person subject to the provisions of the Service Discipline Acts.
- “**residential premises**” means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.
- For the purposes of authorising intrusive surveillance, or interference with property under the 1997 Act, “**senior authorising officer**” (2000 Act) or “**authorising officer**” (1997 Act) means:
 - the chief constable of every police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London) or under section 1 of the Police (Scotland) Act (police forces in Scotland);
 - the Commissioner, Deputy Commissioner or an Assistant Commissioner of the Metropolitan Police force;
 - the Commissioner of the City of London Police force;

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- the Chief Constable or Deputy Chief Constable of the Royal Ulster Constabulary;
- the Director General or a designated officer of Assistant Chief Constable rank⁴ of the National Crime Squad;
- the Director General of the National Criminal Intelligence Service;
- the Chief Constable of the British Transport Police;
- the Chief Constable of the Ministry of Defence Police;
- the Provost Marshal of the Royal Navy Regulating Branch;
- the Provost Marshal of the Royal Military Police;
- the Provost Marshal of the Royal Air Force Police;
- any other customs officer designated for this purpose by the Commissioners of HM Customs & Excise⁵;
- a **“senior official”** means a member of the Senior Civil Service or a member of the senior management structure of Her Majesty's Diplomatic Service;
- **“serious crime”** means conduct which constitutes one or more criminal offences where:
 - (a) it involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose, or
 - (b) the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more.
- **“the Service Police”** are:
 - a member of the Royal Navy Regulating Branch;
 - a member of the Royal Military Police;
 - a Royal Air Force Provost Officer or a member of the Royal Air Force Police.

⁴ **Guidance note: This** will be the Deputy Director General of the National Crime Squad.

⁵ **Guidance note: This** will be the Chief Investigation Officer or a designated Deputy Chief Investigation Officer of the National Investigation Service, HM Customs and Excise.

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- **working day**" means any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom;
- **"Chief Surveillance Commissioner", "Surveillance Commissioner" and "Assistant Surveillance Commissioner"** are persons who hold or have held high judicial office and who have been appointed by the Prime Minister to undertake functions specified in the 1997 Act and/or the 2000 Act in relation to the police (including Service Police), NCIS, the National Crime Squad and HM Customs & Excise. They have also been appointed to undertake functions specified in the 2000 Act in relation to certain activities undertaken by the Ministry of Defence and HM Armed Forces in Northern Ireland, and in relation to activities of Government departments and other public authorities.

DRAFT
PRELIMINARY

PRELIMINARY DRAFT

2 AUTHORISATIONS and PRODUCT

2.1 An authorisation 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 organisation is involved. There is no requirement on the part of a public authority to obtain an authorisation for a covert surveillance operation and the decision not to obtain an authorisation would not, of itself, make an action unlawful. However, public authorities are strongly recommended to seek an authorisation where the purpose of the covert surveillance, wherever that takes place, is to obtain private information about a person, whether or not that person is the target of the investigation or operation. Obtaining an authorisation will make the action less vulnerable to challenge under the Human Rights Act 1998.

2.2 Any person giving an authorisation should first satisfy him/herself that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve. The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect high degree of privacy, for instance in his/her home, or where there are special sensitivities, such as where the surveillance may give access to confidential material or communications between a Minister of any religion or faith and another individual relating to that individual's spiritual welfare. An authorisation should not be sought or obtained where the sole purpose of the authorisation is to obtain legally privileged material. However, an authorisation may be appropriate for other purposes but which, incidentally, catches legally privileged material.

2.3 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

2.4 An authorisation request should include an assessment of the risk of any collateral intrusion or interference. This will be taken into account by the authorising officer, particularly when considering the proportionality of the surveillance.

2.5 Those carrying out the covert surveillance should inform the authorising officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

2.6 Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking

PRELIMINARY DRAFT

place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. In this regard, it is recommended that the authorising officers in NCIS, the National Crime Squad and HM Customs & Excise consult the local chief constable where the authorising officer considers that conflicts might arise.

Combined authorisations

2.7 A single authorisation may combine:

- two or more different authorisations under Part II of the 2000 Act;
- an authorisation under Part II of the 2000 Act and an authorisation under Part III of the 1997 Act;
- a warrant for intrusive surveillance under Part II of the 2000 Act and a warrant under section 5 of the 1994 Act.

2.8 A single authorisation may combine two or more different authorisations under Part II of the 2000 Act. For example, a single authorisation may combine authorisations for directed surveillance or intrusive surveillance and the conduct of a source. However, the provisions applicable in the case of each of the authorisations must be considered separately. Thus, a police superintendent could authorise directed surveillance and the conduct of a source but an authorisation for the use of a source and intrusive surveillance would need the separate authority of a superintendent, a chief constable and the approval of a Surveillance Commissioner.

2.9 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.

Handling and disclosure of product

2.10 There should be a central record held in each force, Service, Squad or authority of all authorisations. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

The Police (including Service Police), NCIS, the National Crime Squad and HM Customs & Excise

PRELIMINARY DRAFT

PRELIMINARY DRAFT

2.11 If there is any reason to believe that the product obtained during the course of an investigation might be relevant to that investigation or to another investigation or to pending or future civil or criminal proceedings then it should not be destroyed but retained in accordance with established disclosure requirements. Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996, which requires that material should be retained if it forms part of the unused prosecution material gained in the course of an investigation, or which may be relevant to an investigation. Where it is believed that the product of intrusive surveillance may be of use in the interests of national security or of the economic well-being of the UK, that material may be retained for those purposes. Where the police or HM Customs & Excise believe that the product might be relevant to future civil or criminal proceedings, and there is a possibility that a Surveillance Commissioner might order the destruction of such material, they should inform the Surveillance Commissioner of their belief and the reasons for it.

2.12 Authorising officers are reminded of the importance of safeguarding confidential and sensitive information. They must also 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. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the senior authorising officer.

2.13 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the public authority which authorised the surveillance, or the courts, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

The Intelligence and Security Agencies, MOD and the Armed Forces

2.14 Each agency must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance.

2.15 The relevant heads of the public authorities are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except in so far as is necessary for the proper discharge of their functions. Such persons are also responsible for putting arrangements in place to ensure that no information is disclosed except in specified circumstances e.g. where it is necessary for the proper discharge of an

PRELIMINARY DRAFT

PRELIMINARY DRAFT

authority's functions, for the purpose of preventing or detecting serious crime or for the purpose of any criminal proceedings.

**PRELIMINARY
DRAFT**

PRELIMINARY DRAFT

3 DIRECTED SURVEILLANCE

3.1 Surveillance is directed if it is covert, but not intrusive, and is undertaken:

- (a) for the purposes of a specific investigation or operation; and
- (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 this Part to be sought for the carrying out of the surveillance.

3.2 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. However, it 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 plain clothes police officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of a patrol. However, the longer the observation continues, the less likely it would be considered to be an immediate response.

3.3 Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. Such activity is defined as "intrusive surveillance" and is dealt with in **section 4**. 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 (a tracking device), the activity is classed as directed surveillance and should be authorised accordingly.

3.4 Nor does directed surveillance include entry on or interference with property or wireless telegraphy. These activities are subject to a separate regime of authorisation or warrant, as set out in **section 5**.

3.5 An authorisation for directed surveillance may be issued when an authorising officer believes that the action is necessary:

PRELIMINARY DRAFT

- in the interests of national security^{6, 7};
- for the prevention or detection of crime or the prevention of disorder;
- in the interests of the economic well-being of the UK⁸;
- in the interests of public safety;
- for the protection of public health⁹;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for any other purpose prescribed in an order made by the Secretary of State.

3.6 The authorising officer must believe that:

- the action is necessary on one or more of the grounds set out in **section 3.5**; and
- the surveillance is proportionate to what it seeks to achieve.

Authorisation Procedures

3.7 The public authorities entitled to authorise directed surveillance are listed in **Schedule 1** to the 2000 Act.

3.8 Authorisations will generally be given in writing by the authorising officer. However, in urgent cases, they may be given orally. In such cases, a written record that the authorising officer has expressly authorised the action should be recorded in writing as soon as is reasonably practicable. This should be done by the person to whom the authorising officer spoke.

⁶ **Guidance note:** One of the functions of the Security Service is the protection of national security. This function extends throughout the United Kingdom, save that, in Northern Ireland, the lead responsibility for investigating the threat from terrorism related to the affairs of Northern Ireland lies with the Royal Ulster Constabulary. An authorising officer in another public authority should not issue an authorisation for directed surveillance where the operation falls within the responsibilities of the Security Service as set out above, except where the operation is to be carried out by a Special Branch or has been agreed with the Service.

⁷ **Guidance note:** The Armed Forces may also undertake operations in connection with the military threat to national security and, subject to Guidance Note 6, other operations in connection with national security in support of the Security Service, the RUC or other Civil Powers.

⁸ **Guidance note:** an authorisation for the conduct or use of a source on the grounds that it is in the interests of the economic well-being of the UK should only be given by one of the intelligence agencies and within the strict meaning of the term contained in the Intelligence Services Act 1994.

⁹ **Guidance note:** This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

PRELIMINARY DRAFT

PRELIMINARY DRAFT

3.9 If an authorising officer is not available, authorisation may be given by a person entitled to act in the absence of the authorising officer, as specified in [*title of Statutory Instrument*]. Such an authorisation must be in writing.

3.10 Ideally, authorising officers should not be responsible for authorising their own activities ie those in which they are directly involved. However, it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently.

3.11 Designated persons within the Police, NCIS, National Crime Squad and HM Customs & Excise authorisations may only grant authorisations on application by a member their own force, Squad, Service or organisation. Except in circumstances set out in **section 3.15** authorising officers are a police superintendent or equivalent. Those designated as being able to authorise directed surveillance are listed in [*title of statutory instrument*].

3.12 Officers entitled to act in urgent cases in the absence of the authorising officer, except in circumstances set out in **section 3.15**, are those of inspector rank or equivalent.

3.13 Authorisations for directed surveillance are subject to review by the relevant Commissioner (see **section 6**).

SPECIAL RULES

3.14 There are certain cases that call for a higher level of authority because of the sensitive nature of the directed surveillance. Details of these categories of cases are set out in **section 3.15**.

Confidential material

3.15 In cases where the likely consequence of the directed surveillance would be for any person to acquire knowledge of confidential material¹⁰, the authorising officer will be a chief constable or equivalent (see **statutory instrument**). In urgent cases, the person designated to act in the absence of the chief constable or equivalent will be entitled to authorise such surveillance.

3.16 In this connection, any person giving an authorisation is reminded that police forces in England and Wales, NCIS, the National Crime Squad and HM Customs & Excise have given an undertaking not to mount surveillance operations in circumstances covered by the Seal of the Confession (see **section 5**).

Recording of telephone or other conversations

¹⁰ **Guidance note:** see definition of confidential material in interpretation section.

PRELIMINARY DRAFT

3.17 The interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be authorised only by the Secretary of State, in accordance with the terms of Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.

3.18 The question will frequently arise whether a surveillance device may legitimately be used in circumstances where the incidental effect will be to enable the overhearing of what is said by a party to a telephone conversation who is speaking from a location where a device is installed. The use of a surveillance device should not be ruled out simply because it may incidentally pick up one end of a telephone conversation, and 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 moment of interception, is being transmitted by a telecommunications system. In such cases an application should be made for a warrant under **section 7** of the 2000 Act.

3.19 Part I of the 2000 Act provides an exception to the rule that interception of telephone conversations must be warranted under that Part. Where one party to the conversation consents, and where the interception is authorised under Part II, no warrant is required. In such cases, the interception is treated as directed surveillance. For example, a person may consent to the recording of a telephone conversation sent by or to him. Authorisation should be given by a police superintendent or equivalent [see **statutory instrument**].

3.20 However, such an authorisation cannot be used as a means of deploying recording equipment without obtaining the proper authorisation. If any other recording equipment is to be used, other than in the presence of the person who has consented to the recording, an intrusive surveillance authorisation or authorisation for interference with property should be obtained, where necessary.

Information to be provided in applications for authorisation

3.21 A written application for authorisation for directed surveillance must record:

- the grounds on which authorisation is sought (eg for the detection of crime or the protection of public health);
- consideration of why the directed surveillance is proportionate to what it seeks to achieve;
- the identity or identities, where known, of those to be the subject of directed surveillance;
- the action to be authorised and level of authority required;

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- an account of the investigation or operation;
- an explanation of the information which it is desired to obtain as a result of the authorisation;
- any potential for collateral intrusion;
- the likelihood of acquiring any confidential material.

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

- reasons why the authorising officer or the person entitled to act in his/her absence considered the case urgent;
- reasons why the authorising officer or person entitled to act in his/her absence was not available to give an authorisation.

Duration of authorisations

3.23 A written authorisation will cease to have effect at the end of a period of three months beginning with the day on which it took effect.

3.24 Urgent oral authorisations or written authorisations given by a person who is entitled to act only in urgent cases will, unless renewed in writing, cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

Renewals

3.25 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, except in circumstances set down in **section 3.26**, he/she may renew it in writing for a further period of three months, beginning with the day when the authorisation would have expired but for the renewal. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

3.26 If at any time before an authorisation for directed surveillance, granted on the grounds of it being in the interests of national security or in the interests of the economic well-being of the UK, would cease to have effect, and an authorising officer who is member of the security or intelligence services considers it necessary for it to continue, he/she may renew it in writing for a further period of six months, beginning with the day on which it would have ceased to have effect but for the renewal.

3.27 All requests for the renewal of an authorisation for directed surveillance must record:

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- the information required in the original request for a authorisation, as listed in **section 3.21**;

together with

- any significant changes to the information in the previous authorisation;
- why it is necessary to continue with the surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- an estimate of the length of time the surveillance will continue to be necessary.

Cancellations

3.28 The authorising officer must cancel an authorisation if he/she is satisfied that the directed surveillance no longer meets the criteria for authorisation. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the post of authorising officer or the person who is acting as authorising officer until the post is filled.

3.29 Authorisations for directed surveillance, and any subsequent renewals and cancellations, are subject to review by the Commissioner

PRELIMINARY DRAFT

4 INTRUSIVE SURVEILLANCE IN PART II OF 2000 ACT

4.1 Covert surveillance as defined in Part II of the 2000 Act is "intrusive surveillance" if it:

- (a) involves the presence of an individual, or of any surveillance device on any residential premises or in any private vehicle; or
- (b) is carried out in relation to anything taking place on residential premises or in a private vehicle by means of any surveillance device that is not present on the premises or in the vehicle (other than television licence evasion detection equipment).

4.2 However, it is only "intrusive" under 4.1(b), if it 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 any private 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. "Residential premises" might be in the form of a house, a yacht, a railway arch or other makeshift shelter. It includes hotel rooms, bedrooms in barracks and prison cells but not any common area to which a person is allowed access in connection with his or her occupation of any accommodation¹¹. A private vehicle is defined in the interpretation section and could include any vehicle used for family, leisure or domestic use.

4.3 In many cases, a surveillance operation may involve both intrusive surveillance and interference with property. In such cases, both activities need authorisation. This can be done as a combined authorisation (see **section 2.7**), although the criteria for authorisation of each activity must be considered separately.

4.4 An authorisation for intrusive surveillance may be issued by the Secretary of State (for intelligence services, MOD and Armed Forces) or by a senior authorising officer (for police and HM Customs & Excise). Neither may authorise intrusive surveillance unless he/she believes that the authorisation is necessary on the grounds that it is:

- in the interests of national security¹²;
- for the purpose of preventing or detecting serious crime; or
- in the interests of the economic well-being of the UK ¹³;

¹¹ **Guidance note:** In cases of doubt about what constitutes residential premises, officers should seek guidance from the appropriate Commissioner through the recognised contact point in each agency.

¹² **Guidance note:** A senior authorising officer of a law enforcement agency should not issue an authorisation for intrusive surveillance where the operation is within the responsibilities of the security and intelligence agencies and properly falls to be authorised by warrant issued by the Secretary of State under Part II of the 2000 Act.

and

- the authorised surveillance is proportionate to what it seeks to achieve.

4.5 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 means.

Use of covert human intelligence source with technical equipment

4.6 A covert human intelligence source wearing or carrying a surveillance device and invited into residential premises or a private vehicle does not require special authorisation to record activity taking place inside those premises or vehicle. Authorisation for the use of that covert source may be obtained in the usual way¹⁴. The human source should not, however, use an invitation into residential premises or a private vehicle as a means of installing equipment without the proper authorisation being in place. If the equipment is to be used, other than in the presence of the covert source, an intrusive surveillance authorisation and, if necessary, interference with property authorisation, should be obtained.

Seal of Confession

4.7 The undertaking not to mount a covert surveillance operation in circumstances that may breach the Seal of Confession (see **section 5**) also applies to intrusive surveillance operations.

Authorisation procedures for the police, NCIS, the National Crime Squad and HM Customs & Excise

4.8 Authorisations will generally be given in writing by the senior authorising officer. However, in urgent cases, they may be given orally. In such cases, a statement that the senior authorising officer has expressly authorised the action should be recorded in writing as soon as is reasonably practicable. This should be done by the person with whom the senior authorising officer spoke. If the senior authorising officer is absent as provided for in section 12(4) of the Police Act 1996, section 5(4) of the Police (Scotland) Act 1967, section 25 of the City of London Police Act 1839, or sections 8 and 54 of the Police Act 1997, an authorisation can be given in writing or, in urgent cases, orally by the designated deputy. 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:

- in the case of the police, by an assistant chief constable ;

¹³ **Guidance note:** see footnote 8

¹⁴ **Guidance note:** see the code of practice for the use of covert human intelligence sources.

PRELIMINARY DRAFT

- in the case of the Metropolitan Police and City of London Police, by a commander;
- in the case of the Ministry of Defence Police or the British Transport Police, by a deputy or assistant chief constable;
- in the Royal Military Police or the Royal Air Force Police, by a deputy Provost Marshal;
- in the Royal Navy Regulating Branch, by an assistant Provost Marshal;
- in the case of NCIS and the National Crime Squad, by the person designated by the relevant Director General¹⁵;
- in the case of HM Customs & Excise, by the person designated by the Commissioners of Customs & Excise¹⁶.

4.9 Applications to the senior authorising officer for authorisation must be made in writing by a member of that officer's own force, Squad, Service or organisation. In relation to intrusive surveillance in residential premises, an authorisation can only be given where those premises are within the area of operation of that police force, Service or Squad. The application should specify:

- the identity or identities of those to be the subject of the intrusive surveillance (where known);
- the property which the intrusive surveillance will affect;
- the identity of individuals and/or categories of people, where known, who are likely to be affected by collateral surveillance;
- details of the offence planned or committed and of the intrusive surveillance involved;
- how the authorisation criteria (as set out in **section 4.4 and 4.5**) have been met;
- whether the operation or investigation is likely to lead to the acquisition of any confidential material;
- in case of a renewal, the content and value to the investigation of the product so far obtained, or an explanation of the failure to obtain any results;

¹⁵ **Guidance note:** This will be an officer of a rank no lower than an assistant chief constable, or a commander in the Metropolitan Police or City of London Police forces, or additionally in the case of the National Criminal Intelligence Service, an assistant chief investigation officer of Customs and Excise;

¹⁶ **Guidance note:** This will be an officer of the rank of assistant chief investigation officer.

PRELIMINARY DRAFT

PRELIMINARY DRAFT

and subsequently record whether authority was given or refused, by whom and the time and date.

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

- reasons why the senior authorising officer or designated deputy considered the case urgent;
- reasons why the senior authorising officer or the designated deputy was not available to give an authorisation.

Approval of Surveillance Commissioners

4.11 The authorisation for intrusive surveillance under Part II of the 2000 Act will not take effect until it has been approved by a Surveillance Commissioner and the authorising officer has been notified, except in cases of urgency.

4.12 Where the case is urgent, the authorisation can take effect immediately and intrusive surveillance can begin without the approval of the Surveillance Commissioner. Much will depend on the circumstances of the individual operation, but the urgency provisions should **not** be used routinely. However, it must be recognised that there may be exceptional circumstances, for example, where it is impractical to obtain the approval of a Surveillance Commissioner. In such cases, the authorising officer must include his/her reasons for considering the case to be urgent in the notification of authorisation which he/she sends to the Surveillance Commissioner (see **section 4.13**). If the Surveillance Commissioner does not believe the reasons for treating the case as urgent to be reasonable, he has the power to quash the authorisation.

Notifications

4.13 Where a person gives, renews or cancels an authorisation, he/she 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. In urgent cases, the notification must specify the grounds on which the case is believed to be one of urgency.

4.14 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 give a fresh authorisation and 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.

4.15 The information to be included in the notification to the Surveillance Commissioner of the authorisation is set out in the **[title of Statutory Instrument]**. All notifications must record:

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- the grounds on which the case was considered to be urgent (where relevant);
- how the authorisation criteria have been met (see **section 4.4**);
- the identity or identities of those to be the subject of the intrusive surveillance (where known);
- the property against which any intrusive surveillance is to take place;
- the nature of the surveillance authorised;
- whether the intrusive surveillance is considered likely to lead to collateral intrusion;
- whether the surveillance is likely to lead to the acquisition of any confidential material.

Authorisation procedures for the security and intelligence agencies and for government departments and the Armed Forces

4.16 An authorisation for intrusive surveillance by the security and intelligence agencies, MOD, the Armed Forces and any other public authority designated for this purpose requires a Secretary of State authorisation/warrant, unless they are acting on behalf of another public authority that has obtained an authorisation. In this context, Secretary of State can mean any Secretary of State, although an authorisation/warrant would normally be obtained from the Secretary of State of the relevant department.

4.17 Intelligence services authorisations are made by issue of a warrant. Such warrants will generally be given in writing by the Secretary of State. In urgent cases, a warrant may be signed (but not renewed) by a senior official, provided the Secretary of State has expressly authorised this.

4.18 Applications to the Secretary of State for authorisations should specify:

- how the authorisation criteria have been met (see **section 4.4**);
- the identity or identities of those to be the subject of the intrusive surveillance (where known);
- the property against which any intrusive surveillance is to take place;
- the nature of the surveillance authorised;
- whether the intrusive surveillance is considered likely to lead to collateral intrusion

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- whether the surveillance is likely to lead to the acquisition of any confidential material.
- in case of a renewal, the requirement for the continued authorisation including for example, the results obtained so far, or a full explanation of the failure to obtain any results.

Authorisation Records

4.19 In all cases of intrusive surveillance, the relevant authority should maintain:

- a copy of the warrant/authorisation given by the Secretary of State or the notification to the Surveillance Commissioner and notification of approval given by him or her;
- a record of the period over which the intrusive surveillance has taken place (including any significant suspensions of coverage);
- a record of the result of periodic reviews of the authorisation (see **section 4.29**); and
- a copy of any renewal of a warrant or authorisation, plus the supporting documentation submitted when the renewal was requested.

4.20 Finally, it should record the date and time when any instruction was given by the senior authorising officer to cease intrusive surveillance or when the warrant/authorisation was cancelled [or quashed]. Where an authorisation is quashed or cancelled a written instruction should be given to those carrying out the surveillance to inform them that the surveillance is not to be continued. A record should be kept of this instruction.

Duration of Authorisations

4.21 A written authorisation given by a senior authorising officer or a designated deputy will cease to have effect at the end of a period of three months, beginning with the day on which it took effect. This means from the time the authorisation was granted under the urgency procedures or from when the Surveillance Commissioner approved the authorisation and the person who gave the authorisation has been notified.

4.22 A warrant issued by the Secretary of State will cease to have effect at the end of a period of six months beginning with the day on which it was issued.

4.23 Oral authorisations given in urgent cases by authorising officers or their designated deputies, and written authorisations given by those only entitled to

PRELIMINARY DRAFT

PRELIMINARY DRAFT

act in urgent cases (see **section 4.8**), will cease at the end of the period of 72 hours beginning with the time when they took effect.

4.24 Warrants expressly authorised by a Secretary of State, and signed on his behalf by a senior civil servant, will cease to have effect at the end of the second working day following the day of issue of the warrant.

Renewals

4.25 If at any time before the day on which an authorisation expires the senior authorising officer 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. As with the initial authorisation, the senior authorising officer must first seek the approval of a Surveillance Commissioner to its renewal. The renewal will take effect from the time the Surveillance Commissioner has approved the renewal and the person who gave the authorisation has been notified (but not before the day on which the authorisation would have ceased to have effect). In urgent cases, where a renewal suddenly becomes necessary, it can take effect immediately but a Surveillance Commissioner must be notified of the renewal as soon as is reasonably practicable. The notification must specify the grounds on which the case is believed to be one of urgency.

4.26 If at any time before the day on which an intelligence service warrant expires, the Secretary of State considers it necessary for the warrant to be renewed for the purpose for which it was issued, he/she may renew it in writing for a further period of six months, beginning with the day on which it would have ceased to have effect, but for the renewal.

4.27 If at any time before the day on which a Secretary of State authorisation expires, the Secretary of State considers it necessary for the warrant to be renewed for the purpose for which it was issued, he/she may renew it in writing for a further period of three months, beginning with the day on which it would have ceased to have effect, but for the renewal.

4.28 All requests for renewal of a warrant or authorisation or for approval of a renewal to a Surveillance Commissioner [see **title of SI**] must record:

- whether this is the first renewal or every occasion on which the warrant/authorisation has been renewed previously;
- the information required in the original request for a warrant/authorisation, as listed in **section 4.9** and **4.18**;

together with:

- any significant changes to the information in the previous application for a warrant/authorisation;

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- why it is necessary to continue with the intrusive surveillance;
- the content and value to the investigation of the product so far obtained under the surveillance;
- the results of periodic reviews of the operation by a senior officer.
- an estimate of the length of time the intrusive surveillance will continue to be necessary.

4.29 Authorisations may be renewed more than once, if necessary, and the renewal should be noted as part of the “authorisation record” (see **section 4.19**).

Reviews and Cancellations

4.30 A person who has given an authorisation must cancel it (or one given in his/her absence) if satisfied that the action authorised by it is no longer necessary. Regular reviews of authorisations should be undertaken to assess the need for the intrusive surveillance to continue. These should be recorded on the authorisation record (see **section 4.19**). Particular attention is drawn to the need to frequently review¹⁷ authorisations where the intrusive surveillance involves confidential material or collateral surveillance on persons other than those who are the subjects of surveillance.

The police, NCIS, the National Crime Squad and Customs & Excise

4.31 Surveillance Commissioners must be notified of cancellations of authorisations given by the police, NCIS, the National Crime Squad and HM Customs & Excise. The information to be included in the notification is set out in the [title of statutory instrument]. All notifications must record:

- the time and date when the instruction was given by the senior authorising officer to cease surveillance;
- the reason why the authorisation was cancelled;
- the outcome of the investigation and the nature of any criminal proceedings contemplated;
- the arrangements made for the storage of material obtained as a result of surveillance, for its review and destruction when it is no longer of use and for the immediate destruction of unrelated material.

4.32 The Surveillance Commissioner has the power to cancel an authorisation if he/she is satisfied that, at any time after an authorisation was

¹⁷ **Guidance note:** The senior authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

PRELIMINARY DRAFT

given or renewed, there were no reasonable grounds for believing that the criteria set out in **section 4.4** were met. In such circumstances, the Surveillance Commissioner may order the destruction of records, in whole or in part, other than those required for pending civil or criminal proceedings.

**PRELIMINARY
DRAFT**

PRELIMINARY DRAFT

Ceasing of surveillance activity

4.33 As soon as the decision is taken that an intrusive surveillance operation should be discontinued, the instruction must be given to those involved in the operation to stop listening, watching or recording the activities of the subject(s). The date when such an instruction was given should be recorded in the authorisation record and the notification of cancellation.

The police, NCIS, the National Crime Squad and HM Customs & Excise

4.34 In cases where an authorisation is quashed/cancelled by a Surveillance Commissioner, the senior authorising officer must immediately instruct those carrying out the surveillance to stop listening, watching or recording the activities of the subject of the authorisation. The date (and time, if appropriate) when such an instruction was given should be recorded on the authorisation record.

DRAFT
PRELIMINARY

5 ENTRY ON AND INTERFERENCE WITH PROPERTY AND WIRELESS TELEGRAPHY

5.1 The 1994 Act and 1997 Act provide lawful authority for the interference with property and wireless telegraphy by the security and intelligence agencies and police, the National Crime Squad, NCIS, HM Customs & Excise. Many of the same conditions apply to this type of operation (known by the security and intelligence agencies as property warrant operations) as apply to intrusive surveillance. Where this is so, reference is made to earlier parts of the code.

5.2 In many cases a surveillance operation may involve both covert intrusive surveillance and interference with property. In such cases, both activities need authorisation to be in accordance with the law. This can be done as a combined authorisation, although the criteria for authorisation of each activity must be considered separately (see **section 2.5**).

Authorisations for interference with property by the police, NCIS, the National Crime Squad and HM Customs & Excise

5.3 Responsibility for such authorisations rests with the "authorising officer" as defined in the 1997 Act, that is the chief constable or equivalent. Authorisations require the personal authority of the authorising officer except in urgent situations, where the authorising officer is absent. The urgency procedures are the same as those under the 2000 Act (see **section 4.8**). Authorisations under the 1997 Act may not be necessary where the authority is 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 2000 Act.

5.4 Authorisations may only be given by an authorising officer on application by a member of his or her own force, Squad, Service or authority for interference with property and wireless telegraphy within the authorising officer's own area of operation (see **section 1.6** for interpretation of "relevant area"). However, an authorising officer may authorise the taking of action outside the relevant area solely for the purpose of maintenance or retrieval of devices or equipment.

5.5 Any person giving an authorisation for interference with property must believe that:

- the action is necessary for the purpose of preventing or detecting serious crime as defined in the 1997 Act (see interpretation section);
- or, in the case of the Royal Ulster Constabulary, in the interests of national security; and
- the action is proportionate to what it seeks to achieve.

PRELIMINARY DRAFT

The authorising officer will also take into account whether what the authorised conduct seeks to achieve could reasonably be achieved by other means.

5.6 Any person giving an authorisation for interference with property has the same need to be aware of any impact on local communities in the same way as other covert surveillance operations. To ensure that the authorising officer is aware of any particular local community sensitivities, it is recommended that authorising officers in NCIS, the National Crime Squad and HM Customs & Excise consult the local chief constable, where they consider this appropriate. In the case of Northern Ireland, the Chief Constable of the RUC should be informed of any surveillance operation undertaken by other law enforcement agencies which involve those officers in maintaining or retrieving covert surveillance equipment within the RUC area.

Cases requiring prior approval of a Surveillance Commissioner

5.7 In certain cases, an authorisation for interference with property will not take effect until it has been approved by a Surveillance Commissioner and the authorising officer has been notified (but see procedures outlined in **section 4.12** regarding cases of urgency). These are cases where the person giving the authorisation believes 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.

5.8 “Office premises” are defined, by reference to section 1(2) of the Offices, Shops and Railway Premises Act 1963 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).

Seal of Confession

5.9 Any person giving an authorisation is reminded that police forces in England and Wales, NCIS, the National Crime Squad and HM Customs & Excise have given an undertaking not to mount operations in circumstances

PRELIMINARY DRAFT

PRELIMINARY DRAFT

covered by the Seal of the Confession. In addition, where they are satisfied that a Minister of Religion is not him/herself involved in the matter under investigation, and they believe that surveillance will lead to them intruding on spiritual counselling between the Minister and a member of his/her faith, they should, in preparing the case for authorisation, give serious consideration to discussing the matter first with a relevant senior representative of the religious authority. The views of the senior representative would be included in the request for authorisation. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity. Spiritual counselling does not amount to a sacramental confession, but the person being counselled is seeking or the Minister is imparting forgiveness, absolution and the resolution of conscience with the authority of the Divine Being of their faith.

Authorisations for interference with property by the intelligence agencies

5.10 Before granting a warrant, the Secretary of State must:

- think it necessary for the purpose of assisting the relevant agency in carrying out its functions;
- be satisfied that the taking of the action is proportionate to what the action seeks to achieve; and
- be satisfied that suitable arrangements are in force in respect of disclosure of any material obtained by means of the warrant and that material obtained will be subject to those arrangements.

5.11 An application for a warrant must be made by a member of the intelligence agencies for the taking of action in relation to that agency. In addition, the Security Service may make an application for a warrant to act on behalf of the Secret Intelligence Service (SIS) and GCHQ. SIS and GCHQ may not be granted a warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands

Authorisation procedures

5.12 The same procedures apply to applications for interference with property as for authorisations for intrusive surveillance under Part II of the 2000 Act. In detail:

- applications will normally be in writing, except in urgent cases (see **sections 4.8 or 4.17**);
- the information which should be included in applications to the authorising officer or the Secretary of State are set out in **sections 4.9 and 4.18**;

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- the duration of authorisations will be the same (see **sections 4.21-4.24**);
- authorisations/warrants can be renewed (see **sections 4.25-4.28**);
- authorisations/warrants should be reviewed and cancelled (see **sections 4.29-4.31**);
- an "authorisation record" should be maintained (see **sections 4.19-4.20**);
- instructions should be given for the ceasing of interference with property (see **section 4.33**);
- the same procedures should apply for the handling and disclosure of product (see **sections 2.10-2.15**).

Notifications to Surveillance Commissioners – Police and HM Customs & Excise

5.13 The notifications to Surveillance Commissioners in relation to the authorisation, renewal and cancellation of authorisations in respect of interference with property are in accordance with the requirements of the Police Act 1997 (Notifications of Authorisations etc) Order 1998. They differ slightly from the notifications for intrusive surveillance under the 2000 Act and are therefore reproduced in full below.

5.14 All notifications of authorisations must record:

- whether it is a case for which the approval of a Surveillance Commissioner is required;
- if it is a case which would otherwise require the approval of a Surveillance Commissioner but in which interference with property has started because of urgency, the grounds on which the case was considered to be urgent;
- the grounds on which the authorising officer believes the matters specified in section 93(2) of the 1997 Act (ie how the authorisation criteria have been met);
- the identity or identities of those to be the subject of the interference with property, where known;
- the property against which any interference is to take place;
- the nature of the interference authorised and the reason why the interference with property in question is necessary;

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- whether the interference with property is considered likely to lead to collateral intrusion on or interference with persons other than the person being directed by the authorisation;
- whether or not it will be necessary to retrieve any equipment used in the operation.

5.15 All notifications of renewals must record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- the information required in a notification of authorisation, as they apply at the time of renewal; plus
- every respect in which the information in the previous authorisation has changed;
- why it is necessary to continue with the authorisation;
- the content and value to the investigation of the product so far obtained through the interference;
- the results of periodic reviews of the authorisation, so as to enable the authorising officer to review his decision;
- an estimate of the length of time the authorisation will continue to be necessary.

5.16 All notifications of cancellation must record:

- the time and date when the instruction was given by the authorising officer to cease interference, and when the interference with property ceased, where that is different;
- the reason why the authorisation was cancelled;
- the outcome of the investigation and the nature of any criminal proceedings contemplated;
- the arrangements made for the storage of material obtained as a result of interference with property, for its review and destruction when it is no longer of use and for the immediate destruction of unrelated material.

5.18 The intelligence agencies should provide the same information, as and where appropriate, when making applications, requests for renewal and requests for cancellation of property warrants.

PRELIMINARY DRAFT

Retrieval of equipment

5.19 Where a Surveillance Commissioner quashes or cancels an authorisation or renewal, he/she 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. He or she 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.

5.20 Because of the time it can take to remove equipment from the person's property it may also be necessary to renew a property warrant in order to complete a retrieval. Applications to the Secretary of State for renewal should state why the operation is being or has been closed down, why it has not been possible to remove the equipment and any timescales for removal, where known.

**PRELIMINARY
DRAFT**

6 OVERSIGHT

6.1 Oversight of the use of the powers contained in the 1989, 1994, 1997 and 2000 Acts will be provided by:

- the Intelligence Services Commissioner, in respect of operations by the Security Service, SIS and GCHQ;
- the Chief Surveillance Commissioner, Surveillance Commissioners and Assistant Surveillance Commissioners, in respect of operations by the police, HM Customs & Excise and other public authorities;

6.2 It will be the duty of any person having functions under the 1994, 1997 and 2000 Acts and any person taking action in relation to which a warrant or authorisation was given, to comply with any request of the relevant Commissioner for documents or information as required by him/her for the purpose of enabling him/her to discharge his/her functions.

For the Security Service, SIS, GCHQ and MOD/Armed Forces operations outside Northern Ireland

6.3 The 2000 Act establishes the role of the Intelligence Services Commissioner so that he is responsible for:

- keeping under review the exercise by the Secretary of State of the power to grant warrants relating to the interference with property and wireless telegraphy by the Security Service, SIS and GCHQ (see **section 5**);
- keeping under review the exercise by the Secretary of State of the power to grant warrants for carrying out intrusive surveillance (see **section 4**);
- keeping under review the use by the Security Service, SIS and GCHQ of the powers to undertake operations which interfere with property or wireless telegraphy;
- keeping under review the use by the Security Service, SIS and GCHQ and MOD/ Armed Forces operations outside Northern Ireland of the powers to undertake intrusive surveillance and to authorise and conduct directed surveillance;
- giving all assistance to the Tribunal set up under the 2000 Act for the investigation of complaints;
- making an annual report to the Prime Minister on the discharge of his functions under the 1994 and 2000 Acts and to report at any other time on any matter relating to those functions.

PRELIMINARY DRAFT

For operations by the police, NCIS, the National Crime Squad, HM Customs & Excise, British Transport Police, Ministry of Defence Police and Service Police and for the MOD and HM Armed Forces (operating in Northern Ireland in respect of 2000 Act only)

Functions of Surveillance Commissioners

6.4 The 2000 Act amends the functions of the Chief Surveillance Commissioner and Surveillance Commissioners and introduces Assistant Surveillance Commissioners.

Functions of Assistant Surveillance Commissioners

6.5 Each Assistant Surveillance Commissioner will be responsible for providing an oversight of authorisations for directed surveillance and the conduct or use of covert sources by public authorities, other than the police and Customs.

Functions of Surveillance Commissioners

6.6 Each Surveillance Commissioner is responsible for:

- scrutinising as soon as is reasonably practicable every notice of authorisation for interference with property and intrusive surveillance received;
- deciding whether to grant or refuse approval of authorisations under the 1997 Act which involve a dwelling, hotel bedroom or an office or matters subject to legal privilege, confidential personal information or confidential journalistic material;
- deciding whether to give or refuse approval of authorisations under the 2000 Act which involve intrusive surveillance;
- notifying the authorising officer whether or not an authorisation, which the authorising officer believes requires approval, is approved;
- quashing an authorisation or renewal where the Surveillance Commissioner is, at any time, satisfied that there were no reasonable grounds for believing that it met the criteria for authorisation for interference with property or intrusive surveillance (those matters detailed in **sections 4.4** and **5.5**) or for the case to be one of urgency (see **section 4.12**) or cancelling an authorisation where the Surveillance Commissioner is satisfied that, at any time, there were no reasonable grounds for continuing to believe that it met the criteria;
- reporting the findings to the authorising officer and to the Chief Surveillance Commissioner when the Surveillance Commissioner

PRELIMINARY DRAFT

PRELIMINARY DRAFT

decides to cancel or quash an authorisation for interference with property or intrusive surveillance;

- deciding whether to order the destruction of records obtained as a result of interference with property or intrusive surveillance, wholly or in part (other than those required for pending criminal or civil proceedings),
- ordering, in appropriate cases, that an authorisation for interference with property under the 1997 Act remain effective for a specified period to retrieve anything from the property;
- giving assistance to the Tribunal set up under the 2000 Act for the investigation of complaints;
- assisting the Chief Surveillance Commissioner in keeping under review the use by the police, NCIS, the National Crime Squad and HM Customs & Excise of powers to authorise and conduct directed surveillance.

Functions of the Chief Surveillance Commissioner

6.7 The Chief Surveillance Commissioner is responsible for:

- keeping under review the adequacy of the arrangements and the performance of functions by authorising officers, Surveillance Commissioners and Assistant Surveillance Commissioners under the 1997 and 2000 Acts;
- considering appeals by authorising officers, modifying the decisions of Surveillance Commissioners in relation to intrusive surveillance authorisations, and notifying the outcome as required by the 1997 and 2000 Acts;
- giving assistance to the Tribunal set up under the 2000 Act for the investigation of complaints;
- keeping under review the use by the police, NCIS, the National Crime Squad and HM Customs & Excise of powers to authorise and conduct directed surveillance;
- making an annual report to the Prime Minister on the discharge of functions under the 1997 and 2000 Acts and reporting at any other time on any matter relating to those functions.

Appeals under the 1997 and 2000 Acts

6.8 Authorising officers may appeal to the Chief Surveillance Commissioner within a period of 7 days against any decision made by a Surveillance Commissioner:

PRELIMINARY DRAFT

PRELIMINARY DRAFT

- to refuse to approve an authorisation or its renewal;
- to quash an authorisation or renewal;
- to cancel an authorisation;
- to order the destruction of records when cancelling or quashing an authorisation (other than those required for pending civil or criminal proceedings);
- to refuse to order that the authorisation remain effective for a specified period to allow the retrieval of anything left on the premises by virtue of the authorisation (in respect of 1997 Act only).

6.9 Any decision by a Surveillance Commissioner to order the destruction of records will not become operative until the period for appealing against the decision has expired and, where there is an appeal, a decision dismissing it has been made by the Chief Surveillance Commissioner.

6.10 The Chief Surveillance Commissioner and Surveillance Commissioners will not give any reasons for a determination except, where appropriate, to the authorising officer, the Surveillance Commissioner who made a decision and the Prime Minister (when he dismisses an appeal),

For operations by other public authorities

6.11 The Assistant Surveillance Commissioners and Surveillance Commissioners are also responsible for:

- assisting the Chief Surveillance Commissioner, as required, in keeping under review the use by designated public authorities of the powers to authorise and conduct directed surveillance;
- giving assistance to the Tribunal set up under the 2000 Act for the investigation of complaints.

7 COMPLAINTS AND REDRESS

7.1 A single Tribunal will deal with all:

- proceedings brought under section 7 of the Human Rights Act against the security and intelligence agencies, or which concern Part II of the 2000 Act or which concern property warrants obtained under the 1994 Act or authorisations under Part III of the 1997 Act;
- any complaint brought in relation to conduct under Part II of the 2000 Act, or in relation to warrants obtained under the 1994 Act or authorisations under Part III of the 1997 Act or otherwise against the security and intelligence agencies.

7.2 The Tribunal will deal with any complaint or proceedings, within the terms of paragraph 7.1, relating to conduct which has taken place under an authorisation or warrant or which should not have taken place without such an authorisation/warrant.

8 INFORMATION LEAFLET

8.1 All public authorities listed in the schedule to the legislation should ensure that the information leaflet "Complaints about the exercise of powers under the Regulation of Investigatory Powers Act 2000" is readily available at any premises to which the public have access.

PRELIMINARY
DRAFT