Home Office

THE USE OF

COVERT HUMAN INTELLIGENCE SOURCES

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

Some forms of intrusive investigation, such as covert surveillance, have changed and developed over the years and become more sophisticated as a result of technical development. The use of human beings to provide information, on the other hand, goes back hundreds of years with informants playing a major role in or contributing to significant changes in history. Their use and value has also been recognised in various court judgments, together with the need to protect their identity. Up until now, the use of such sources has never been the subject of statutory control in this country. Their continued use is, however, essential to the maintenance of law and order and for the protection of the public.

Covert sources are uniquely able to provide information that comes to their notice during conversations with their associates or family. Members of the public are encouraged to give information or provide assistance to the police and other authorities carrying out their public functions and, generally, they see this as part of their civic duty, with no expectation of a reward. Trade and businesses will obtain personal information as part of their normal business practices, which they will pass to the police or other regulatory bodies, if they suspect criminal activity. The gathering and disclosure of information, in such a fashion, is governed primarily by the provisions of the Data Protection Act 1998. In other cases, there may be a different statutory basis for the disclosure of information. For example, the Drug Trafficking Act 1994 provides a statutory basis for disclosure of suspicious financial transactions. Nothing in the provisions of the Regulation of Investigatory Powers Act 2000, nor in this code of practice, affects such activity.

Similarly, these provisions are not intended to apply in circumstances where members of public contact numbers specifically set up to receive anonymous information (such as Crimestoppers, the Anti Terrorist Hotline or the Customs Drugs Freephone). The actions of these callers would not generally come within the definition of a covert source. However, someone might become a covert source as a result of a relationship with a public authority begun in this way.

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

CONTENTS

1 GENERAL

1.1 This code of practice provides guidance on the use and conduct of covert human intelligence sources by public authorities listed in Schedule 1 of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act").

1.2 A covert human intelligence source ("a source") is defined in section 25(7) of the 2000 Act as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

(a) covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(b) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

1.3 A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

1.4 Any interference with the rights protected by Article 8(1) of the European Convention on Human Rights will give rise to a violation of Article 8, unless the interference is in accordance with the law, is in pursuit of one or more of the legitimate aims referred to in Article 8(2) and is “necessary in a democratic society” to achieve the aim or aims in question. The provisions of the 2000 Act and this code cover those activities where a relationship is established or maintained specifically to obtain or provide access covertly to information about the private or family life of another person. They also cover those activities where the relationship itself can be construed as an infringement of a person’s private or family life.

General extent of powers

1.5 There is no geographical limitation on the use or conduct of a source. Authorisations can be given for the use or conduct of a source both inside and outside the United Kingdom.

1.6 There is also nothing in the 2000 Act, the effect of which is to exclude any material obtained from the use or conduct of a source from being adduced as evidence in court proceedings. There are well-established legal procedures which, at the court’s discretion, will protect the identity of a source from disclosure in such circumstances.

1.7 The code covers activities conducted by:

– police forces in England, Wales and Northern Ireland;

- police forces in Scotland, when acting under the provisions of the 2000 Act;;
- the National Crime Squad;
- the National Criminal Intelligence Service (NCIS);
- the British Transport Police;
- the Ministry of Defence Police;
- the Service Police (see interpretation section);
- HM Customs & Excise;
- the security and intelligence agencies;
- the Ministry of Defence;
- HM Armed Forces; and
- any other public authority listed in Schedule 1of the 2000 Act.

1.8 The provisions of the 2000 Act and this code extend to Scotland in all cases where a public authority authorises the use or conduct of a covert source under the 2000 Act.

1.9 A copy of the code should be readily available, for reference purposes, at public offices of public authorities designated to use sources, and where people are detained in custody. It should also be readily available to any members of an agency or department who are actively involved in operations where sources are deployed.

1.10 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.

Interpretation

1.11 For the purpose of this code:

- **"authorising officer"** is the person who is entitled to give an authorisation for the use or conduct of a source in accordance with section 29 of the 2000 Act;
- **"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 Police Act 1997 or in the 2000 Act in relation to the police (including the Service Police and the Ministry of Defence Police), NCIS, the National Crime Squad, HM Customs & Excise. They also undertake functions in relation to certain activities by the Ministry of Defence and HM Armed Forces in Northern Ireland, and in relation to Government departments and other public authorities;

– **"the conduct"** of a source is action of that source, falling within the terms of the 2000 Act, or action incidental to it;

– **"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

  – 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 privilege[1].

"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

[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.

paid or unpaid office[2]. 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;

– **"controller"** means the person/the designated managerial officer within the relevant public authority referred to in section 28(5)(b) of the 2000 Act, responsible for the general oversight of the use of the source;

– **"directed surveillance"** means covert surveillance (other than intrusive surveillance) where this is in relation to a specific investigation or operation carried out to obtain (or likely to obtain) private information about a particular person or persons (whether or not they have been specifically identified for the purposes of the investigation or operation). It does not include surveillance undertaken by way of an immediate response to events or circumstances where it would not have been reasonably practicable for an authorisation to have been sought;

– **"handler"** means the person referred to in section 28(5)(a) of the 2000 Act holding an office, rank or position within the relevant investigating authority and who will have day to day responsibility for:

– dealing with the source on behalf of that authority;

– directing the day to day activities of the source;

– recording the information supplied by the source; and

– monitoring the source's security and welfare;

– **"Intelligence Services Commissioner"** is the person who holds or has held high judicial office and who has been appointed by the Prime

[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.

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);

- **"a public authority"** means any public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal;

- **"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.

- **“the use”** of a source is any action to induce, ask or assist a person to engage in the conduct of a source or to obtain information by means of an action of the source.

2 AUTHORISATION

2.1 Responsibility for authorising the use or conduct of a source rests with the authorising officer. Authorisations require the personal authority of the authorising officer.

2.2 Any person giving an authorisation for the use or conduct of a source must believe that:

– the authorisation is necessary on the grounds specified in **section 2.3**;

– the authorised use or conduct is proportionate to what it seeks to achieve (see **section 2.3**); and

– satisfactory arrangements exist for the management of the source (see **section 3**).

2.3 An authorisation will be considered necessary if it is necessary:

– in the interests of national security[3] ;

– for the prevention or detection of crime or for the prevention of disorder;

– in the interests of the economic well-being of the country[4] ;

– in the interests of public safety;

– for the protection of public health;

– for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

– for any other purpose prescribed in an order made by the Secretary of State[5].

[3] **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 is vested in the Royal Ulster Constabulary. An authorising officer in another public authority should not issue an authorisation for the use or conduct of a source 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.

[4] **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.

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

2.4 A source has no licence to commit crime. They may, in the context of an authorised operation, infiltrate a criminal conspiracy or be a party to the commission of criminal offences, within the limits recognised by case law and with the approval of the authorising officer. A source who acts beyond these limits will be at risk of prosecution. The need to protect the source cannot alter this principle.

2.5 Before authorising the use or conduct of a source, the authorising officer should first satisfy himself that the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He or she should also take into account the risk of intrusion into the privacy of persons other than those directly implicated in the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation. Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, "confidential material" is likely to be obtained. For example, 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. Consideration should also be given to any adverse impact on community confidence that may result from the use or conduct of a source or information obtained from that source.

2.6 Additionally, the authorising officer must make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

Cultivation of a source

2.7 Cultivation is the process of developing a relationship with a potential source, with the intention of:

- making a judgement as to his/her likely value as a source of information;
- determining whether and, if so, the best way in which to propose to the subject that he/she become a source.

2.8 It may be necessary to infringe the personal privacy of the potential source in the process of cultivation. In such cases, authorisation is needed for the cultivation process itself, as constituting the conduct (by the person undertaking the cultivation) of a source.

Use of directed surveillance against a potential source

2.9 Similarly, it may be necessary to deploy directed surveillance against a potential source as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them.

Authorisation for such use of directed surveillance would need to be obtained separately but could be part of a combined authorisation (see **section 2.34**).

Use and conduct of a source

2.10 Many relationships with sources are established without an initial cultivation process. However, both the use and conduct of the source will still require authorisation.

2.11 Authorisation for the use and conduct of a source is required prior to any tasking. Tasking is an assignment given to the source, asking him or her to obtain information, to provide access to information and to otherwise act, incidentally, for the benefit of the relevant public authority. It may involve the source in infiltrating existing criminal or terrorist activity in order to obtain that information.

Authorisation procedures

2.12 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 as soon as is reasonably practicable. This should be done by the person to whom the authorising officer spoke but should later be endorsed by the authorising officer.

2.13 An authorising officer can also act as the controller or handler of a source. Ideally, though, authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the source or in tasking the source. However, it is recognised that this is not always possible, especially in the cases of small organisations.

2.14 Designated person within the Police, National Crime Squad, NCIS and Customs authorisations may only grant authorisations on application by a member of their own force, Squad, Service or organisation.

2.15 Officers entitled to act in urgent cases in the absence of an authorising officer, except in circumstances set out in **section 2.22-2.27**, are those of, at least, inspector rank or equivalent (see ***statutory instrument***).

Officers working under cover

2.16 A member of a public authority may, by concealing his or her identity or otherwise acting covertly:

- infiltrate an existing criminal or terrorist conspiracy;
- arrest a suspected criminal or criminals;
- counter a threat to national security;

– counter a significant threat to public order;

– counter a significant threat to public safety;

– counter a threat to the economic well being of the UK.

2.17 Members of foreign law enforcement or other agencies may be authorised to be deployed in the UK in support of domestic and international investigations.

2.18 In some cases, officers of a public authority undertake work in which they represent themselves (in their own identity or by use of an alias) to be an official of a different public authority. This, in itself, may not necessarily require authorisation. However, an authorisation may be required when the officer is engaging in the conduct of a source.

2.19 In cases where officers of a public authority undertake work in which they represent themselves to be acting on behalf of another person (ie not a public authority) to establish a personal or other relationship for the covert purpose of obtaining information, authorisation will be required for the officer to engage in the conduct of a source in relation to each cover capacity used.

2.20 Authorising officers who can give authority for officers to work under cover, as described in **sections 2.16** to **2.19**, are the same as those giving authority for the use of a source (ie superintendent or equivalent level).

SPECIAL RULES

2.21 There are certain cases, as set out in **sections 2.22-2.27**, that call for a higher level of authority either:

– because of the nature of the source deployed; or

– because the use or conduct of a source is particularly sensitive.

Confidential material

2.22 In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of 'confidential material'[6], the deployment of the source requires special authorisation. In these cases, the authorising officer will be a chief constable or equivalent (see ***statutory instrument***).

2.23 In urgent cases, a person designated or entitled to act in the absence of the authorising officer will be able to authorise the use or conduct of a source.

[6] **Guidance note:** see interpretation section at 1.11.

Vulnerable individuals

2.24 Vulnerable individuals, such as the mentally impaired, will only be authorised to act as a source in the most exceptional circumstances. Authorisation would be required by an assistant chief constable or equivalent (see ***statutory instrument***).

Juvenile sources

2.25 Special safeguards also apply to the authorisation for the use or conduct of juvenile sources; that is sources under the age of 18 years. **On no occasion can the use or conduct of a source under 16 years of age and living with his parents be authorised, to give information against his or her parents**. In other cases, authorisations can be given with the following additional safeguards;

- juvenile sources can give information about other members of their immediate family in exceptional cases;
- a parent/guardian or other "appropriate adult" should be present at meetings with the juvenile source under the age of 16 years.

2.26 In addition, an authorisation should not be granted unless or until:

- the safety and welfare of the juvenile has been fully considered;
- the authorising officer has satisfied him/herself that any risk has been properly explained and understood by the juvenile;
- a risk assessment has been undertaken as part of the application to deploy a juvenile source, covering the physical dangers and the moral and psychological aspects of his or her deployment;

2.27 Authority for the deployment of a juvenile source is at assistant chief constable level or equivalent (see ***statutory instrument***). Authorisations should last for one month, renewable for a period of a further month.

Recording of telephone or other conversations

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

2.29 However, the question will frequently arise whether a recording may be made by one party to a conversation, without the knowledge or consent of the other party. For example, a person may consent to the recording of telephone

conversation sent by or to him. In such circumstances, the 2000 Act provides that a warrant by the Secretary of State or an authorisation by a chief officer with approval by a Surveillance Commissioner is not required. Instead, authorisation should be given for directed surveillance (see the code of practice on surveillance) by a police superintendent or equivalent (see ***statutory instrument***).

2.30 However, a source cannot use an invitation into residential premises or a private vehicle as a means of deploying equipment without obtaining the proper authorisation. If any recording equipment is to be used other than in the presence of the source, a separate authorisation or warrant for intrusive surveillance, directed surveillance and/or interference with property must be obtained (see the code of practice on surveillance).

Use of covert human intelligence source with technical equipment

2.31 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 way. 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 should be obtained.

Information to be provided in applications for authorisation

2.32 An application for authorisation for the use or conduct of a source must record:

- details of the purpose for which the source will be tasked or deployed (e.g. In relation to an organised serious crime, espionage, a series of racially motivated crime etc);
- the grounds on which authorisation is sought (e.g. for the detection of crime or the protection of public health);
- where a specific investigation is involved, details of that investigation or operation;
- details of what the source will be tasked to do;
- details of the level of authority required.
- details of who will be affected;

– details of any confidential material that might be obtained as a consequence of the authorisation.

2.33 A standard form for use in applications for authorisation is attached to this code. This sets out the basic information that is required on an application and can be adapted to the needs and requirements of particular public authorities.

Combined authorisations

2.34 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.

Duration of authorisations

2.35 Except in relation to juvenile sources, a written authorisation will cease to have effect at the end of a period of twelve months beginning with the day on which it took effect.

2.36 Oral authorisations or 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

2.37 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, it may be renewed, in writing, for a further period of twelve months, beginning with the day on which the authorisation would otherwise cease to have effect, but for the renewal. An application for renewal should not, though, be made until shortly before the authorisation period is drawing to an end. An authorisation can be renewed at any time before the time at which it ceases to have effect, by any person who would be entitled to grant a new authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

Reviews

2.38 Before an authorising officer renews an authorisation, he must be satisfied that a review has been carried out of the use made of the source during the period authorised, the tasks given to the source and the information obtained from the use or conduct of the source.

2.39 If satisfied that the criteria necessary for the initial authorisation continue to be met, he/she may renew it in writing for a further period.

Cancellations

2.40 The authorising officer must cancel an authorisation if he/she is satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that the procedures for the management of the source are no longer in place (see **section 3.5**). Where the authorising officer is no longer available, this duty will fall to any person who has taken the place of the authorising officer or who is deputising for the authorising officer in his absence or while the post is vacant. where possible, the source must be informed that the authorisation has been cancelled.

3 MANAGEMENT OF SOURCES

Tasking

3.1 Tasking is the assignment given to the source by the handler or controller, asking him/her to obtain information, or to otherwise take an action leading to the obtaining of information.

3.2 In some instances, the tasking given to a person will not necessarily involve interference with a person's ECHR Article 8 rights. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a trading standards officer or health inspector may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may interfere with Article 8 and require authorisation.

3.3 The deployment of a source to infiltrate or gain trust in order to obtain personal information is not amenable to specific, step by step authorisation. In many cases, the source will be a relative or associate of the target and will already have details of that person's private life or have access to that person's home on a regular basis. For this reason it is not possible or necessary to define and authorise each separate occasion when a meeting with the source is for the specific purpose of obtaining personal information to pass on to the police or other public authority.

3.4 It is equally difficult to predict exactly what might occur each time a source meets with the target of an investigation. There may be occasions when unforeseen action or undertakings which, had they been foreseen would have needed authorisation, might be required of the source by the target. When this happens, it must be recorded as soon as practicable after the event and an authorisation should be obtained before any such further conduct is carried out.

Management responsibility

3.5 All authorisations for the use or conduct of a source should be in writing. In addition, public authorities should ensure that arrangements are in place for the proper oversight and management of sources. These require that:

(a) every source must have a designated handler;

(b) every source must have a designated controller.

3.6 The day-to-day contact between the public authority and the source is to be conducted by the handler, who will be an officer below the rank of the authorising officer. Some tasking may be given in direct response to

information provided by the source on the occasion of his/her meeting with the handler and, as such, will come within the control of the handler.

3.7 In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

3.8 Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known to the target or those involved in the target activity.

3.9 The handler is responsible for bringing to the controller's attention any concerns about the personal circumstances of the source, insofar as they might affect:

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

3.10 Where deemed appropriate, the controller must ensure that the information is considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to stand.

Record keeping

3.11 The records maintained by public authorities must be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use and conduct made of a source. Such a record must contain the following details (except in the case of undercover officers, where not all the requirements will apply):

- a means of referring to the source - without disclosing his true identity - to those who have a legitimate interest in the source's reporting;
- the source's true identity (available only to those within the organisation who need to know);

- details of the target or area of activity against which the source is to be deployed;

- the authorisation for the use or cultivation of the source (where appropriate) ;

- a risk assessment on the deployment of the source (see **section 3.8**);

- the authorisation for the conduct of the source,

- why, if appropriate, there has been an oral authorisation;

- all subsequent renewals;

- written details of the date and circumstances of the initial recruitment and registration for use of the source (where appropriate);

- a record of the identity of the source's handler(s) and controller, and a note of when these change;

- records of contact between the investigating public authority and the source (whether or not tasking was issued or information exchanged);

- detailed records of tasking (as defined in **section 3.1** above) given by the handler and/or controller to the source ;

- records of all information given by the source;

- detailed records of intelligence derived and disseminated from this information;

- details of any review (which should occur no less frequently than annually) of the use or conduct made of the source and the information provided by him/her;

- details of any rewards or other benefits offered and/or given to the source, in cash or otherwise[7];

- details of any information relevant to the security of the source which may have an impact on the validity of the most recently conducted risk assessment;

[7] **Guidance note:** a benefit may include the supply to a Court of information which may lead to a reduced sentence for a source who has been convicted of an offence.

- confirmation that such information has been considered by the authorising officer, and a decision taken to allow the authorisation to stand;

- the grounds for withdrawal of an authorisation or refusal to renew an authorisation.

3.12 In the event that a source is specifically tasked in a way which is intended or likely to interfere with the ECHR Article 8 rights of any person or persons not previously considered as coming within the remit of the original authorisation, or to a degree significantly greater than previously identified, the handler or controller must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Retention and destruction of the product and records of the use of a source

3.13 All records relating to the use and conduct of a source must be available for inspection by one of the Commissioners described in **section 4**. They must therefore be capable of being retrieved at a central point within each public authority.

3.14 Where there is reasonable belief that material relating to any activity by a source could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In the cases of the law enforcement agencies (not including the Service Police), particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996 (CPIA). This requires that material should be retained if it forms part of the unused prosecution material gained in the course of a criminal investigation, or which may be relevant to an investigation.

3.15 Authorising officers must also ensure compliance with data protection requirements and, where appropriate, with any relevant code of practice on data protection.

3.16 Subject to 3.14, all records should be retained for a minimum of one year to ensure that they are available for inspection by a Commissioner. Thereafter material must not be destroyed, save with the authority of the authorising officer. It is essential that this responsibility should be managed at a senior level in the relevant organisation and that officers are clearly identified and are held accountable for carrying out this function.

4 OVERSIGHT BY COMMISSIONERS

4.1 Oversight of the use of the powers contained in the 2000 Act will be provided by:

- the Intelligence Services Commissioner, in respect of Security Service, SIS, GCHQ and the Ministry of Defence and HM Armed Forces (excluding the Service Police, Ministry of Defence Police and the Ministry of Defence and HM Armed Forces in Northern Ireland);

- the Chief Surveillance Commissioner, Surveillance Commissioners and Assistant Surveillance Commissioners, in respect of operations by the police (including the Service Police and the Ministry of Defence Police), NCIS, the National Crime Squad, British Transport Police, HM Customs & Excise, the Ministry of Defence and HM Armed Forces in Northern Ireland and other public authorities;

4.2 It will be the duty of any person having functions under the 2000 Act and any person taking action in relation to which an 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.

Functions of Commissioners

4.3 The 2000 Act provides for the Intelligence Services Commissioner and extends the remit of the Chief Surveillance Commissioners so that they will be responsible for:

- monitoring the use by the agency for which they have responsibility of the powers relating to the use and conduct of sources;

- 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/her functions under the 2000 Act and to report at any other time on any matter relating to those functions.

4.4 The Chief Surveillance Commissioner may seek the assistance of any Surveillance Commissioner or Assistant Surveillance Commissioner in carrying out these functions.

5 COMPLAINTS AND REDRESS

5.1 A single Tribunal will deal, among other things, with all complaints in relation to:

- proceedings brought under section 7 of the Human Rights Act in relation to use or conduct of a source by the police including the Ministry of Defence Police and the Service Police, NCIS, the National Crime Squad, Customs & Excise, the security and intelligence agencies, the Ministry of Defence and HM Armed Forces;

- any complaint brought in relation to conduct under Part II (Surveillance and covert human intelligence sources) of the 2000 Act.

5.2 The Tribunal will deal with any complaint or proceedings, within the terms of paragraph 5.1, relating to conduct which is alleged to have taken place, or which might reasonably have been considered should have taken place, under an authorisation for the use or conduct of a source.

6 INFORMATION LEAFLET

6.1 In general, 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 public office of that public authority.

6.2 In addition, any public authority specified in the 2000 Act, or designated by order, should ensure that details of the relevant complaints procedure are provided to anyone making representations that disclose some ground of complaint against one or more of these authorities.