

www.defra.gov.uk

Directed surveillance and covert human intelligence source policy and operational document

Regulation of Investigatory Powers Act 2000

January 2007

Department for Environment, Food and Rural Affairs
Nobel House
17 Smith Square
London SW1P 3JR
Telephone 020 7238 6000
Website: www.defra.gov.uk

© Crown copyright 2007

Copyright in the typographical arrangement and design rests with the Crown.

This publication (excluding the Royal Arms and departmental logos) may be re-used free of charge in any format or medium for research for non-commercial purposes, private study or for internal circulation within an organisation. This is subject to it being re-used accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the publication specified.

For any other use of this material please apply for a Click-Use Licence for Public Sector Information (PSI) or core material at

<http://www.opsi.gov.uk/click-use/psi-licence-information/index.htm>

or by writing to:

Office of Public Sector Information
Information Policy Team
St Clements House
2-16 Colegate
Norwich
NR3 1BQ
Fax: 01603 723000
E-mail: licensing@cabinet-office.x.gsi.gov.uk

Information about this publication and further copies are available from:

Enforcement Policy Unit, Legal Group, B1
Defra
Nobel House
3E
17 Smith Square
London SW1P 3JR

Tel: 020 7238 5155

This document is also available on the Defra website.

Published by the Department for Environment, Food and Rural Affairs

CONTENTS

	Page
1. Introduction	4
2. Statutes, Codes and other Materials	4
3. Other Relevant Legislation and Information	4
4. Policy and Scope of Procedure	6
5. Directed Surveillance (DS)	7
• General Matters Relating to Authorisations of DS	7
• Duration of Authorisations	9
• Renewals	9
• Reviews	10
• Cancellations	10
• Local Record of Authorisations and Reviews	10
• Central Record of Authorisations and Reviews	11
• Security, Retention and Destruction of Documents	11
• Oversight	11
• Complaints	12
• Further information	12
6. Covert Human Intelligence Source (CHIS)	12
• General Matters Relating to Authorisations of CHIS	12
• Payments and Other Rewards	16
• Duration of Authorisations	17
• Renewals	17
• Reviews	17
• Cancellations	18
• Local Record of Authorisations and Reviews	18
• Central Record of Authorisations and Reviews	19
• Security, Retention and Destruction of Documents	19
• Oversight	19
• Complaints	20
• Further Information	20
7. Definitions	20

	Page
Annex 1 - List of Authorising Officers	22
<ul style="list-style-type: none">• Directed Surveillance• Covert Human Intelligence Source	
Annex 2 - Points for Authorising Officers to consider	23
Annex 3 - Relevant Forms	24
<ul style="list-style-type: none">• Directed Surveillance• Covert Human Intelligence Source	
Annex 4 - Directed Surveillance Form for return to EPU	25
Annex 5 - Covert Human Intelligence Source Form for return to EPU	26

1. INTRODUCTION

1.1 In some circumstances, it may be necessary for Defra, and its Agencies, in the course of their enforcement or investigatory duties, to make observations of a person, or place where persons are likely to be, in a covert manner. There will also be situations where the use of a Covert Human Intelligence Source (CHIS) is appropriate. (A CHIS is a person who establishes or maintains a relationship with someone in order to covertly obtain information, to provide another person with access to information, or to disclose information as a consequence of that relationship).

1.2 By their nature, actions of this sort may constitute an interference with a person's right to respect for private life under Article 8 of the European Convention on Human Rights and the Human Rights Act 1998.

2. STATUTES, CODES AND OTHER MATERIALS

2.1 The Regulation of Investigatory Powers Act (2000) (RIPA) provides a legal framework for authorising such covert surveillance activities by public authorities and an independent inspection regime to monitor these activities.

The Act needs to be read in conjunction with:

- The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 (SI 2003/3171);
- the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources)(Amendment) Order 2006 (SI 2006/1874);
- the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725);
- the Home Office's Code of Practice on the Use of Covert Human Intelligence Sources and the Code of Practice on Covert Surveillance. (See <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/?version=1>).
- the best practice guidance issued by the Office of Surveillance Commissioner (See www.surveillancecommissioners.gov.uk).
- Defra's Enforcement Policy Statement sets out the matters which Defra takes into account when deciding to investigate a matter. (This may be found at <http://defraweb/corporate/enforcement/enforce-policy.pdf>).

Part 7 below sets out definitions used in this document.

3. OTHER RELEVANT LEGISLATION AND INFORMATION

3.1 The Data Protection Act 1998

The Data Protection Act 1998 (DPA) provides eight principles to be observed to ensure that the requirements of the Act are complied with. They provide that personal data, which includes personal data obtained from covert surveillance techniques, must:

- be fairly and lawfully obtained and processed;
- be processed for the specified purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- not be kept for longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure;
- not be transferred to non-European Economic Area countries without adequate protection.

3.2 The Human Rights Act 1998

The Human Rights Act 1998 (HRA) gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights. Article 8 of the Convention is relevant in the context of covert surveillance in that *“everyone has the right to respect for their private and family life, home and correspondence”*. Consequently, there is to be no interference with the exercise of these rights by any public authority except where such interference is in accordance with the law.

3.3 The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA) and its associated regulations aims to strike a balance between effective law enforcement, and individual rights and freedoms.

The Act requires that the person granting an authorisation believe that the authorisation of an interference with private life is necessary in the circumstances of the particular case for one or more of the statutory grounds:

- a) in the interests of national security;
- b) for the purpose of preventing or detecting crime or of preventing disorder;
- c) in the interests of the economic well-being of the UK;
- d) in the interests of public safety;
- e) for the purpose of protecting public health;
- f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge, payable to a government department;
- g) for the purpose, in an emergency, of preventing death or injury;
- h) for any other purpose prescribed in an order made by the Secretary of State.

It is important to note that Defra only has the power to grant authority for the purpose of “preventing or detecting crime” and that authorisations must be by an officer of a certain rank (see Annex 1).

3.4 The two Home Office Codes of Practice make it clear that certain routine enforcement work will not require authorisation under RIPA. In relation to Directed Surveillance the code says “*General observation forms part of the duties of many enforcement officers and is not usually regulated by the 2000 Act. For example, police officers will be on patrol to prevent and detect crime, and Trading Standards or 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*”. (Covert Surveillance, Home Office Code of Practice, para 1.3).

3.5 Surveillance that is unforeseen and undertaken as an immediate response to a situation when it is not reasonably practicable to obtain authorisation falls outside the definition of Directed Surveillance and therefore authorisation is not required (Covert Surveillance, Home Office Code of Practice, para 4.4).

3.6 Members of the public volunteering information would not generally be regarded as CHIS and the provisions of the 2000 Act would not apply in such circumstances (Covert Human Intelligence Sources, Home Office Code of Practice para 1.3).

3.7 A test purchaser carrying out an everyday retail transaction as any normal shopper would is not a CHIS. However, a test purchaser operating in circumstances other than an everyday retail transaction eg purchasing illegal goods is, owing to the attendant circumstances, most likely to be operating as a CHIS.

3.8 Employees of Defra have no power to carry out “intrusive surveillance” within the meaning of the Regulation of Investigatory Powers Act 2000.

3.9 If there is any doubt as to whether or not surveillance falls within the scope of RIPA, officers should seek further advice from the Enforcement Policy Unit (EPU), Legal Group, Nobel House.

4. POLICY AND SCOPE OF PROCEDURE

4.1 This Policy has been developed in consultation with representatives from Legal Group (LG), Defra Investigation Services (DIS), Marine Fisheries Agency (MFA), Centre for Environment, Fisheries and Aquaculture Science (CEFAS), and The Gangmasters Licensing Authority (GLA).

4.2 The policy will be reviewed and continuously monitored in light of any relevant changes to the application of the Act or through Defra re-organisation.

4.3 A copy of this Policy and Procedure Document together with the two Home Office Codes of Practice will be made available for inspection at Enforcement Policy Unit (EPU), Legal Group, Nobel House.

4.4 Defra Investigation Services (DIS), now based in the Rural Payments Agency (RPA), provides investigation services across those parts of Defra where agreement

has been reached and a Service Level Agreement (SLA) put in place. Some agencies within Defra continue to conduct their own investigations i.e. MFA, CEFAS and the GLA.

4.5 This policy document sets out the circumstances in which Defra staff will be permitted to embark on a covert directed surveillance operation and the use of CHIS and the requirements that will need to be observed in order that Defra will not contravene the relevant legislation, the Codes of Practice issued by the Home Office, or the guidance of the Office of Surveillance Commissioners.

4.6 Any wilful failure to comply with the procedures in place for the implementation of this policy may potentially be a disciplinary offence.

5. DIRECTED SURVEILLANCE

5.1 Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

- for the purposes of a specific investigation or operation;
- 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 purpose of the investigation or operation);
- otherwise than by way of an immediate response to events or circumstances the nature of which would mean it would not be reasonable practicable for an authorisation to be sought.

General matters relating to the authorisation of Directed Surveillance

5.2 Employees of Defra have no power to carry out “intrusive surveillance” within the meaning of the Regulation of Investigatory Powers Act 2000.

5.3 Directed Surveillance may only be carried out by Defra agencies for the purpose of “preventing and detecting crime”.

5.4 Any person giving an authorisation for the use of directed surveillance must be satisfied that:

- the authorisation is **necessary and proportionate** - i.e. it shall be in proportion to the significance of the matter being investigated;
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation (**‘collateral intrusion’**). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.

5.5 The Authorising Officers permitted to authorise such surveillance for the purposes of a specific investigation are listed at Annex 1. In their absence authority must be sought from a higher grade.

5.6 All applications to conduct, renew, or cancel a covert surveillance exercise must be made in writing (see Annex 3) and submitted to an Authorising Officer and must record:

- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required for the surveillance.

5.7 In urgent cases, authorisations may be given orally by the Authorising Officer. In such cases, a statement that the Authorising Officer has expressly authorised the action should be recorded in writing by the requesting officer as soon as is reasonably practicable.

5.8 A case is not normally to be regarded as urgent unless a delay in obtaining the authorisation would be likely to endanger life or jeopardise the investigation for which the authorisation was being given.

5.9 An authorisation is not to be regarded as urgent when the need for an authorisation has been neglected or the urgency is of the Authorising Officer's own making.

5.10 Following authorisation a Unique Reference Number (URN) will be allocated to the Directed Surveillance, future correspondence will refer only to the Unique Reference Number.

5.11 Authorising Officers should not normally be responsible for authorising investigations in which they are directly involved, although it is recognised this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently (Home Office Codes of Practice, Directed Surveillance: para 4.14). Where an Authorising Officer authorises such an investigation the Record of Authorisations should identify this and the attention of an Inspector from the Office of Surveillance Commissioners should be drawn to it during his next inspection.

5.12 When unforeseen events occur, this must be recorded as soon as practicable and, if the existing authorisation is insufficient, it should either be updated and reauthorised or it should be cancelled and a new authorisation should be obtained before any further action is carried out.

5.13 Directed surveillance operations shall be undertaken only by suitably trained or experienced staff, or under their direct supervision.

5.14 Defra's requirements for covert surveillance will normally be carefully planned so that the necessary investigations regarding risk assessment and health and safety can be carried out and the required precautions put in place before directed surveillance commences.

5.15 Particular care should be taken in cases where the subject of the investigation might reasonably expect a high degree of privacy, or where confidential information is involved. (Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material). In cases where it is likely that knowledge of such confidential information will be acquired, the authorisation must be at a higher level than normal.

5.16 In no circumstance can matters applicable to Directed Surveillance be given backdated authorisation after it has commenced.

Duration of Authorisations

5.17 Written authorisations for a Directed Surveillance operation will be valid for a maximum of **3 months** (unless renewed) from the date of the original authorisation.

5.18 Urgent oral authorisations will cease to have effect after **72 hours**, beginning from the time when the authorisation was granted or renewed.

Renewals

5.19 If the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of three months.

5.20 All applications for the renewal of an authorisation should be made in writing (see Annex 3) and record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information held.

5.21 Renewals may also be granted orally in urgent cases and last for a period of **72 hours**. A renewal takes effect from the time and day on which the authorisation ceased to have effect.

5.22 An application for renewal should not be made until shortly before the authorisation period is drawing to an end.

5.23 Any person who would be entitled to grant a new authorisation can renew an authorisation.

5.24 Authorisations may be renewed more than once provided they continue to meet the criteria for authorisation.

Reviews

5.25 Para 4.22 of the Code of Practice on Covert Surveillance states that *“the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable”*. However, in Defra, the Authorising Officer shall review all authorisations at intervals of not more than **one month** to assess the need for the authorisation to continue.

5.26 The result of the review should be recorded (see Annex 3).

5.27 Particular attention is drawn to the need to review authorisations frequently where there is likely to be access to confidential information or the possibility of collateral intrusion.

Cancellations

5.28 Where authorisation ceases to be necessary the Authorising Officer will cancel the authorisation (see Annex 3). The Authorising Officer must cancel an authorisation if satisfied that the original criteria for authorisation no longer applies. Every authorisation must be cancelled at some stage rather than left to expire.

Local Record of Authorisations and Reviews

5.29 A record of all authorisations should be held securely and regularly updated whenever an authorisation is granted, reviewed, renewed or cancelled. A nominated officer should be identified for this role.

5.30 These records should be retained for a period of five years from the ending of the authorisation and should contain the following information:

- a copy of the application and authorisation together with any supplementary documentation provided;
- a record of the reviews of the authorisations conducted by the Authorising Officer;
- a copy of any renewal of the authorisation, together with the supporting documentation submitted when the renewal was requested and the reason why the person renewing an authorisation considered it necessary to do so;

- any authorisation which was granted or renewed orally and the reason why the case was considered urgent;
- the reason and date the authorisation was cancelled.

5.31 Where the product of surveillance could be relevant to future criminal or civil proceedings, records may be retained for a suitable further period.

5.32 Access to all files should be limited to the Authorising Officer and Controller.

Central Record of Authorisations and Reviews

5.33 The EPU will maintain a Central Record of Authorisations and Reviews and be responsible for monitoring authorisations and carrying out an annual review of applications, authorisations, refusals, renewals, reviews and cancellations.

5.34 Authorising Officers shall send a **brief record** of authorisations granted, renewed, reviewed or cancelled to the Head of the EPU within 3 working days of it taking place to ensure the accuracy of the Central Record. For security reasons it is not necessary to send the actual forms themselves or to identify the subject of the Directed Surveillance. Use can be made of the Unique Reference Number (URN) to identify and monitor the authorisation process (see Annex 4).

5.35 The Central Record of Authorisations will record:

- the Authorising Body;
- the Unique Reference Number (URN) of the investigation;
- the date the Authorisation, Renewal, Cancellation, Review was given/held;
- name and rank of Authorising Officer;
- any authorisation which was granted or renewed orally and the reason why the case was considered urgent.

Security, Retention and Destruction of Documents

5.36 Documents created under this procedure are highly confidential and shall be marked and treated as such. Authorising Officers must make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998.

5.37 Once a covert operation results in an individual being proceeded against for a criminal offence, the material must be dealt with as “unused material” under the requirements of the Criminal Procedure and Investigation Act 1996 if not used in evidence.

Oversight

5.38 The Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers Act 2000. This oversight includes inspection visits by Inspectors appointed by the OSC. It is the duty of any person who uses powers under RIPA to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

Complaints

5.39 The Regulation of Investigatory Powers Act 2000 establishes an Independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction.

Further Information

5.40 Annex 2 contains brief guidelines to help determine whether authorisation for the proposed activity should be granted.

5.41 Any enquiries about the policy should be referred to Mike Piggott or Martin Jones, Enforcement Policy Unit, LG, Nobel House.

6. COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

6.1 The use of a CHIS involves inducing, asking, or assisting a person to engage in the conduct of a CHIS to obtain information by means of the conduct of such a source. A person is a CHIS if:

- he establishes a relationship with another person for the covert purpose of using such a relationship to obtain information about a third person;
- he covertly discloses information obtained by the use of such a relationship;
- a CHIS may include those referred to as agents, informants and officers working undercover.

General matters relating to the authorisation of a CHIS

6.2 It is important to note that anyone purporting to be someone other than an Enforcement Officer in order to obtain information from others is to be regarded as a CHIS and authorisation will be necessary.

6.3 Authorisation for the use of a CHIS by Defra, or its Agencies, may only be granted by the Authorising Officer where he believes that the authorisation is for the purpose of “preventing or detecting crime”.

6.4 Any person giving an authorisation for the use of a CHIS must be satisfied that:

- the authorisation is **necessary and proportionate** - i.e. it shall be in proportion to the significance of the matter being investigated;

- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ('**collateral intrusion**'). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.

6.5 The authorising officers permitted to authorise use of a CHIS are listed at Annex 1. In their absence authority must be sought from a higher grade.

6.6 Officers should be aware of the motivating factors behind a person's agreement to become a CHIS. These factors may include:

- Financial reward;
- Public spirited action;
- Vengeance;
- False allegations against another party;
- Involvement in an offence;
- Excitement or adventure;
- Over-inflated ego.

6.7 Officers should deal with a potential CHIS in a professional manner and **must not make any promises** about the future particularly in respect of the officer's ability to influence the outcome of any judicial proceedings or provide any reward. (See 6.28ff below for fuller details).

6.8 Before an individual is registered and used as a CHIS, he/she should be interviewed (normally by the appointed Handler – see below) and as much background information obtained as possible including his/her motivation for becoming a CHIS. It is important that detailed records are kept which will include:

- the identity and profile of the CHIS and details of any criminal record;
- geographical area of operation and contacts;
- "tasking potential" and relevance of information;
- the date when, and the circumstances in which, the CHIS was recruited;
- the tasks given to the CHIS and the demands made of him/her in relation to his activities as a CHIS;
- any significant information connected with the security and welfare of the CHIS;
- confirmation by the Authorising Officer granting authorisation for the use of a CHIS that any identified risks to the security and welfare of the CHIS have been properly explained to and understood by the CHIS;

- the identities of the Handler, Controller and Record Keeper and the periods during which those persons have discharged those responsibilities;
- any other relevant investigating authority involved other than the authority maintaining the records and the means by which the CHIS is referred to within each relevant investigating authority;
- all contacts or communications between the CHIS and persons acting on behalf of any relevant investigating authority;
- the information obtained by each relevant investigating authority by the use of the CHIS and any dissemination by that authority of the information obtained in that way;
- every payment, benefit or reward that is made by any relevant investigating authority in respect of the CHIS's activities for the benefit of that or any other relevant investigating authority.

6.9 An application for authorisation for the use of a CHIS should be made in writing (see Annex 3) and record:

- the level of authority required;
- the nature of the investigation or operation;
- a profile of the CHIS and the purpose for which the CHIS will be tasked;
- the reasons why the authorisation is necessary and on what grounds (i.e. "for the purpose of preventing or detecting crime"). It is extremely important that all reasonable alternative methods to resolve a situation have been considered first and recorded in writing before requesting authorisation;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation;
- the details of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could impact on the deployment of the CHIS;
- any concerns that might affect the safety and welfare of the CHIS or others. A **risk assessment** should be carried out to determine the risk to the CHIS and the likely consequences should the role of the CHIS become known. Concerns about the future security and welfare of the CHIS must be

considered by the Authorising Officer from the outset and a decision taken on whether or not to give the authorisation. Where a CHIS has been compromised the Authorising Officer must make an immediate assessment of the situation and decide whether the use of the CHIS should be terminated.

6.10 In urgent cases, authorisations may be given orally by the Authorising Officer. In such cases, a statement that the Authorising Officer has expressly authorised the action should be recorded in writing by the requesting officer as soon as is reasonably practicable.

6.11 A case is not normally to be regarded as urgent unless a delay in obtaining the authorisation would be likely to endanger life or jeopardise the investigation for which the authorisation was being given.

6.12 An authorisation is not to be regarded as urgent when the need for an authorisation has been neglected or the urgency is of the Authorising Officer's own making.

6.13 Applications for the use of a CHIS will be submitted under "confidential cover" or by hand. All correspondence will be in double envelopes which are sealed.

6.14 Following authorisation a Unique Reference Number (URN) will be allocated to the CHIS, future correspondence will refer only to the Unique Reference Number.

6.15 Authorising Officers should not normally be responsible for authorising investigations in which they are directly involved, although it is recognised this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently (Home Office Codes of Practice, Covert Human Intelligence Source: para 4.12). Where an Authorising Officer authorises such an investigation the Record of Authorisations should identify this and the attention of an Inspector from the Office of Surveillance Commissioners should be drawn to it during his next inspection.

6.16 An Authorising Officer must not grant an authorisation for the use of a CHIS unless a person with the responsibility for handling, controlling and maintaining a record of the use made of the CHIS is in place.

6.17 The Handler will usually have day-to-day responsibility for:

- dealing with the CHIS;
- directing the day-to-day activities of the CHIS;
- recording the information supplied by the CHIS;
- monitoring the security and welfare of the CHIS.

6.18 All Handlers must have received training in the use and management of CHIS.

6.19 Where possible, the Handler should be of the same gender as the CHIS.

6.20 The Controller will be responsible for the general oversight of the use of the CHIS, to channel requests to the Authorising Officer, and to keep central records. When the Controller is going to be absent for any appreciable length of time, he/she will arrange for another officer to deputise.

6.21 Authorisation for the use of a CHIS is required prior to any tasking. "Tasking" is a legitimate and productive means of deploying a registered CHIS to obtain intelligence on a specific problem, nominated individual or network. Tasking can involve clearly defined parameters, specific objectives or objectives within a geographical area.

6.22 Tasking should follow the principles of the National Intelligence Model.

6.23 When unforeseen events occur, this must be recorded as soon as practicable and, if the existing authorisation is insufficient it should either be updated and reauthorised or it should be cancelled and a new authorisation should be obtained before any further action is carried out. Similarly where it is intended to task a CHIS in a new or significantly greater way than previously identified this must be referred to the Authorising Officer, who should consider whether a separate authorisation is required.

6.24 In cases where the authorisation is for the use of a CHIS whose activities benefit more than a single authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. If it is necessary to pass full control of the CHIS over, the authority of the Authorising Officer should be obtained and recorded. All current authorisations for conduct and use must be cancelled.

6.25 The use of vulnerable individuals, such as the mentally impaired, for a CHIS purpose should only be authorised in the most exceptional cases. Authorising Officers should abide by the Home Office Code of Conduct relating to Juveniles.

6.26 In no circumstance can matters applicable to CHIS be given backdated authorisation after it has commenced.

6.27 There is nothing in RIPA which prevents material obtained from the properly authorised use of a CHIS being used in other investigations.

Payments and Other Rewards

6.28 A CHIS may be motivated to provide information for a variety of reasons and rewards. This will include monetary payments in appropriate circumstances.

6.29 Where other possible rewards are being considered – the Authorising Officer should consult with the Enforcement Policy Unit. However, the final decision will be that of the Authorising Officer.

6.30 The provision of a "text" for court detailing the assistance provided by a CHIS is a valuable means of reward and may be considered for a CHIS facing a prosecution. The Enforcement Policy Unit should be consulted.

Duration of Authorisations

6.31 Written authorisations for a CHIS are for a maximum of **12 months** (unless renewed), both from the date of the original authorisation.

6.32 Urgent oral authorisations will cease to have effect after **72 hours**, beginning from the time when the authorisation was granted or renewed.

Renewals

6.33 If the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of twelve months.

6.34 All applications for the renewal of an authorisation should be made in writing (see Annex 3) and record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information held;
- the reasons why it is necessary to continue to use the CHIS;
- the use made of the CHIS in the period since the grant or, as the case may be, latest renewal of the authorisation;
- the tasks given to the CHIS during that period and the information obtained from the use of the CHIS;
- the results of regular reviews of the use of the CHIS.

6.35 Renewals may also be granted orally in urgent cases and last for a period of **72 hours**. A renewal takes effect from the time and day on which the authorisation ceased to have effect.

6.36 An application for renewal should not be made until shortly before the authorisation period is drawing to an end.

6.37 Any person who would be entitled to grant a new authorisation can renew an authorisation.

6.38 Authorisations may be renewed more than once provided they continue to meet the criteria for authorisation.

Reviews

6.39 Para 4.20 of the Code of Practice on Covert Human Intelligence Sources states *that “the Authorising Officer within each public authority should determine how*

often a review should take place. This should be as frequently as is considered necessary and practicable". However, in Defra the Authorising Officer shall review all authorisations at intervals of not more than **one month** to assess the need for the authorisation to continue.

6.40 The result of the review should be recorded (see Annex 3).

6.41 The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS.

6.42 Particular attention is drawn to the need to review authorisations frequently where the use of the CHIS provides access to confidential information or involves collateral intrusion.

Cancellations

6.43 Where authorisation ceases to be necessary the Authorising Officer will cancel the authorisation (see Annex 3). The Authorising Officer must cancel an authorisation if satisfied that the original criteria for authorisation no longer applies. Every authorisation must be cancelled at some stage rather than left to expire.

6.44 Where necessary, the safety and welfare of any CHIS used should continue to be taken into account after the authorisation has been cancelled.

Local Record of Authorisations and Reviews

6.45 A record of all authorisations should be held securely and regularly updated whenever an authorisation is granted, reviewed, renewed or cancelled. A nominated officer should be identified for this role.

6.46 These records should be retained for a period of five years from the ending of the authorisation and should contain the following information:

- a copy of the application and authorisation together with any supplementary documentation provided;
- a copy of the risk assessment made and the value of the CHIS to the investigating authority;
- a record of the reviews of the authorisations conducted by the Authorising Officer;
- a copy of any renewal of the authorisation, together with the supporting documentation submitted when the renewal was requested and the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally and the reason why the case was considered urgent;
- the reason and date the authorisation was cancelled.

6.47 Where the product of the CHIS could be relevant to future criminal or civil proceedings, records may be retained for a suitable further period.

6.48 Access to all files should be limited to the Authorising Officer, Controller and Handler.

Central Record of Authorisations and Reviews

6.49 The EPU will maintain a Central Record of Authorisations and Reviews and be responsible for monitoring authorisations and carrying out an annual review of applications, authorisations, refusals, renewals, reviews and cancellations.

6.50 Authorising Officers shall send a **brief record** of CHIS authorisations granted, renewed, reviewed or cancelled to the Head of the EPU within 3 working days of taking place to ensure the accuracy of the Central Record (see Annex 5).

6.51 For security reasons it is not necessary to send the actual forms themselves or to identify the person used as a CHIS. Use can be made of the Unique Reference Number (URN) to identify and monitor the authorisation process.

6.52 The Central Record of Authorisations will record;

- the Authorising body;
- the Unique Reference Number (URN) of the investigation;
- the date the Authorisation, Renewal, Cancellation, Review was given/held;
- name, rank and signature of the Authorising Officer;
- any authorisation which was granted or renewed orally and the reason why the case was considered urgent.

Security, Retention and Destruction of Documents

6.53 Documents created under this procedure are highly confidential and shall be marked and treated as such. Authorising Officers must make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998.

6.54 Once a covert operation results in an individual being proceeded against for a criminal offence, the material must be dealt with as “unused material” under the requirements of the Criminal Procedure and Investigation Act 1996 if not used in evidence.

Oversight

6.55 The Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within the Regulation of Investigatory

Powers Act 2000. This oversight includes inspection visits by Inspectors appointed by the OSC. It is the duty of any person who uses powers under RIPA to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

Complaints

6.56 The Regulation of Investigatory Powers Act 2000 establishes an Independent Tribunal. This has full powers to investigate and decide any cases within its jurisdiction.

Further Information

6.57 Annex 2 contains brief guidelines to help determine whether authorisation for the proposed activity should be granted.

6.58 Any enquiries about the policy should be referred to Mike Piggott or Martin Jones, Enforcement Policy Unit, Legal Group, Nobel House.

7. DEFINITIONS

7.1 **Covert surveillance** is surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

7.2 **Directed Surveillance** is covert but not intrusive and undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather information about them.

7.3 A **Covert Human Intelligence Source (CHIS)** is a person who establishes a relationship with someone in order to covertly obtain information, to provide another person with access to information or to disclose information as a consequence of that relationship.

7.4 **Intrusive Surveillance** is defined as covert surveillance that is conducted:

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

7.5 **Private information** includes information about a person relating to his private or family life.

7.6 **Residential premises** means any premises used, however temporarily, for residential purposes.

7.7 **Private vehicle** means a vehicle that is used primarily for the private purpose of the person who owns it or has the right to use it. A vehicle includes any vessel, aircraft or hovercraft.

7.8 **Authorising officer** is the person who is entitled to give an authorisation for Directed Surveillance or use of a CHIS in accordance with of the Regulation of Investigatory Powers Act 2000 and the Statutory Instruments.

ANNEX 1

AUTHORISING OFFICERS

By virtue of The Regulation of Investigatory Powers Act 2000 (RIPA), The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 and The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources)(Amendment) Order 2006 (SI2006/1874), Designated Authorising Officers shall be:-

DIRECTED SURVEILLANCE

Senior Investigation Officer	DIS
District Inspector	MFA
Senior Investigation Officer	CEFAS
Head of Enforcement	GLA

COVERT HUMAN INTELLIGENCE SOURCE

Senior Investigation Officer	DIS
Deputy Chief Inspector	MFA
Senior Investigation Officer	CEFAS
Head of Enforcement	GLA

together with all more senior officers with the Authority.

ANNEX 2

POINTS TO BE CONSIDERED BY AUTHORISING OFFICERS

1. Is the authorisation;
 - Necessary for the statutory purpose?
 - Proportionate to what it seeks to achieve?
 - Proportionate to the intrusion of privacy including collateral intrusion?

2. Consider whether or not Confidential Information is likely to be obtained, if so refer to the Home Office Code of Practice.

3. In the case of a CHIS;
 - Ensure that arrangements are made to manage the CHIS, appoint a Handler and Controller;
 - Ensure that a Risk Assessment is carried out;
 - Consider the vulnerability of individuals and whether juveniles are involved.

ANNEX 3

RELEVANT FORMS

DIRECTED SURVEILLANCE

- 1). Application for Authorisation to conduct Directed Surveillance.
- 2). Application for Renewal of a Directed Surveillance.
- 3). Review of Directed Surveillance Authorisation.
- 4). Cancellation of a Directed Surveillance Authorisation.

COVERT HUMAN INTELLIGENCE SOURCES

- 1). Application for Authorisation of the use of a CHIS.
- 2). Application for Renewal of CHIS Authorisation
- 3). Review of a CHIS Authorisation.
- 4). Cancellation of an Authorisation for use of a CHIS.

The above forms are available from <http://security.homeoffice.gov.uk/ripa/about-ripa/news/ripa-forms>. Care must be taken during the completion of these forms as only the activities referred to on the application form will be regarded as “lawful”, any deviation from the authorisation may jeopardise the operation and may render any evidence obtained under the authority inadmissible.

ANNEX 4

EPU NOTIFICATION – DIRECTED SURVEILLANCE

AUTHORISING BODY:

URN:

TYPE	DATE	AUTHORISING OFFICER	GRADE	SIGNATURE
AUTHORISATION				
RENEWAL				
REVIEW				
CANCELLATION				

State if authorisation was granted or renewed orally and the reason why the case was considered urgent.

Please return within 3 days of authorisation to:

**Martin Jones
EPU
Level 3E
Nobel House
London SW1**

