Appendix B

1. Changes since to previous version

Issue 4.0 Changes to include an explanation of "urgency" and the roles and responsibilities of Authority employees.

All changes are underlined and highlighted in yellow.

Index

2. Introduction

2.1 Some Authority activities may require the use of covert surveillance as part of its enforcement functions. The Regulation of Investigatory Powers Act 2000 (RIPA) provides the statutory framework for the granting of authority to carry out surveillance.

2.2 The Authority is fully committed to complying with the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (RIPA). To ensure compliance, all covert surveillance and use of covert human intelligence source (CHIS), falling within the scope of the Act carried out by officers of the Authority, must be authorised by a designated 'Authorising Officer'.

2.3 In complying with RIPA, officers must have full regard to the Code of Practices issued by the Home Office which can be found at:

- Code of practice for the interception of communications
- Code of practice for investigation of protected electronic information
- Code of practice for the acquisition and disclosure of communications data
- Code of Practice for the Retention of Communications Data
- Covert human intelligence sources code of practice
- Covert Surveillance and Property Interference Code of Practice (2014)

3. Purpose

The purpose of this document is to set out the Authority's policy on RIPA, reinforce the requirements of the Act, the Order and Codes of Practice, provide guidance to officers, protect the rights of individuals and minimise the risk of legal challenge as a result of officer actions.

4. Access to communication data

4.1 The Authorities investigating criminal offences have powers (by virtue of The Regulation of Investigatory Powers (Communications Data) Order 2004 ("the Order") to gain access to information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations.

~~**5. Implementation**~~

~~5.1 On approval, this policy will be published on the Authority intranet supporting procedures. will be updated and also published on the Authority intranet and other training rolled out to officers, proportionate to their role. , as required.~~

5. Basic requirements

5.1 Under RIPA, the Order and Codes of Practice, directed covert surveillance, use of CHIS and access to communications data should only be authorised if the Authorising Officer is satisfied that:

a) The action is necessary for the prevention or detection of crime or the prevention of disorder or in the interests of public safety.

b) The surveillance/access to communications data is proportionate. A measure or action is proportionate if it:

- impairs as little as possible the rights and freedoms of the individual concerned and of innocent third parties.
- is carefully designed to meet the objectives in question, is not arbitrary, unfair or based on irrational considerations.

c) Three essential elements must be met:

- the proposed covert surveillance is proportional to the mischief under investigation;
- is proportional to the degree of anticipated intrusion on the target and others; and
- is the only option, other overt means having been considered and discounted.

6. Types of surveillance

6.1 Covert surveillance is surveillance that is carried out in a manner to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. Surveillance may be 'directed' or 'intrusive'.

6.2 The Authority is **not** authorised to conduct Intrusive Surveillance, or to interfere with the property of others whilst conducting directed surveillance.

6.3 Intrusive surveillance – is carried out in relation to anything taking place on any residential premises or in any private vehicle by an individual on the premises or in the vehicle or is carried out by means of a surveillance device. Although a surveillance device not on or in the premises/vehicle will only be intrusive if it consistently provides information of the same quality and detail as might be expected to be obtained for a device actually on/in the premises/vehicle.

6.4 Directed surveillance – is covert, but not intrusive and is undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather private information about them (which can include information about persons at work). Covert surveillance includes monitoring, observing or listening to persons without their knowledge.

6.5 Deciding when authorisation under RIPA is required involves making a judgement. Where surveillance is covert and is directed at individual(s) to obtain information about them, RIPA is likely to apply and prior authorisation obtained in accordance with this policy.

6.6 Directed surveillance must be authorised, in accordance with this policy, and only be used for legitimate purposes, when sufficient evidence exists and documented to warrant the exercise and when surveillance is shown to be both the least harmful means of meeting that purpose and proportionate to what it seeks to achieve.

6.7 It is imperative that all reasonable alternative methods to resolve a situation, such as naked-eye observation, interview or changing methods of working or levels of security should be attempted first and recorded in writing with the reason for surveillance being requested fully documented. Where the subject of covert surveillance is an employee, the Authority's Legal Officer (the Director of Legal & Governance) must be informed.

7. Authorisation and duration

7.1 All requests to conduct, extend or discontinue a covert surveillance exercise must be made in writing on the appropriate forms[1] and submitted to the Authorising Officer. Prior to seeking authorisation applicants should speak to the Co-ordinating Officer who will issue a Unique Reference Number and maintain a register of the status of the investigation. All requests and extensions must be considered and authorised in writing, by the Authorising Officer, before any covert

[1] except that in urgent cases they may be given orally by the authorising officer. In such cases, a record that the authorising officer has expressly authorised the action should be recorded in writing by both the authorising officer and the applicant as soon as is reasonably practicable, together with the information set out at §5.9 Covert Surveillance and Property Interference Revised Code of Practice, Home Office 2014 . A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's or applicant's own making.

surveillance operation can commence or continue. The Authorising Officer will notify the Co-ordinating Officer when an application has been granted or refused.

7.2 Authorisation can only be granted where covert surveillance is believed, by the Authorising Officer, to be necessary and proportionate. Written authorisations for direct covert surveillance will be valid for 3 months from the date of the original authorisation or extension, the Authorising Officer is responsible for ensuring that surveillance is cancelled as soon as it is no longer required.

7.3 If during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

7.4 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the Authority must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer.

~~**9. Authorising Officer**~~

~~The Authorising Officer will be a post holder in the role of Group Manager or above~~.

8. Evidence

8.1 During a covert operation, recorded material or information collected will be stored and transported securely. It will be reviewed regularly (at least weekly) and access to it will be restricted to the Authorising Officer and the Enforcement Officers concerned.

8.2 The Authorising Officer will decide whether to allow requests for access by third parties. Access will generally only be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings). Authorising Officers will maintain a record of all reviews of material recorded and collected covertly.

8.3 Once a covert operation results in an individual being under suspicion of having committed a criminal offence, he/she must be informed of this as promptly as is reasonably practicable if the fire authority is pursuing the offences. This is in order to ensure their right to a fair trial or hearing within a reasonable time in accordance with the Human Rights Act.

8.4 In a situation where it is considered that a matter gives rise to a potential criminal prosecution, any interview with the suspect must be 'under caution' and conducted by a suitably trained officer.

9. Covert human intelligence sources

9.1 A person is a CHIS if they:

a) establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c) below;

b) covertly use such a relationship to obtain information or to provide access to any information to another person; or

c) covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

9.2 A CHIS may be required to establish or maintain a personal or other relationship for a covert purpose, i.e. one which the person with whom the relationship is established is unaware of. A CHIS is "tasked" to obtain information, provide access to information or to otherwise act, incidentally, for the benefit of the Authority. Authorisation for the use or conduct of a CHIS is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

9.3 The Code of Practice strongly recommends that the Authority consider an authorisation whenever the use or conduct of CHIS is likely to engage an individual's rights under Article 8, whether this is through obtaining information, particularly private information, or simply through the covert manipulation of a relationship. An authorisation will be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the Authority.

9.4 However, the provisions of the 2000 Act do not apply in circumstances where members of the public volunteer information as part of their normal civic duties, or to contact numbers set up to receive information e.g. Crime stoppers or Anti-Fraud Hotline. Members of the public acting in this way would not generally be regarded as sources. A routine test purchase which does not go beyond a normal transaction is unlikely to be considered a CHIS activity.

9.5 The use of CHIS by the Authority is likely to be infrequent. A judgement must be made in determining when an individual taking part in an investigation may be acting as a CHIS and if in any doubt, should seek advice from the Authorising Officer.

10. Chis authorisation

10.1 The same principles and procedures apply for the authorisation of CHIS as for directed surveillance. The Authorising Officer[2] may authorise the use of CHIS if they are satisfied that it is necessary and proportionate to do so, and arrangements are in place for managing a CHIS.

10.2 Applications to use, extend or discontinue the use of CHIS must be made in writing, except in urgent cases, where they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant (or the person with whom the authorising officer spoke) as a priority. This statement need not contain the full detail of the application, which should however subsequently be recorded in writing when reasonably practicable (generally the next working day). A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the applicant's or authorising officer's own making[3].

10.3 Written authorisations for CHIS will be valid for 12 months from the date of authorisation or extension. Exceptionally, an oral authorisation may be granted for the use of a CHIS in circumstances of urgency.

10.4 An oral authorisation will be valid for 72 hours but will be subject to the same requirements as that set out in part 2 relating to urgent authorisations for directed surveillance. As with directed surveillance, the Authorising Officer is responsible for ensuring that authorisation is cancelled as soon as it is no longer required, and that reviews of authorisations are carried out on at least a monthly basis.

10.5 There are additional considerations which must be taken into account before the use of a CHIS can be authorised. These relate to the security, welfare and management of the source and records relating to his/her use. Details of these issues are set out in paragraphs 14.1 – 14.3 below.

10.6 Material obtained from a CHIS may be used as evidence in criminal proceedings and the proper authorisation of a CHIS should ensure the legality of such evidence.

[2] The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases.

[3] § 5.7 Code of Practice for the use of Human Intelligence Sources (2014 edition)

10.7 Before authorising the use of a CHIS, the Authorising Officer and Enforcing Officers must ensure that, as far as is possible, measures are taken to avoid unnecessary intrusion into the lives of those not directly connected with the investigation.

10.8 An authorisation for a CHIS may be in broad terms and highlight the nature of the CHIS's task. However, where it is intended to task a source in a new or significantly greater way, the handler or controller must refer the proposed tasking to the Authorising Officer, who should consider whether a separate authorisation is required.

11. Management of the source

11.1 The Authorising Officer must not grant an authorisation for the use or conduct of a source unless he/she has appointed a person who is responsible for having day to day contact with the source, and a person with the responsibility for the general oversight of the use of the source.

11.2 The person with day to day responsibility will be a 'Handler' and will deal with the CHIS on behalf of the Authority, direct the day to day activities of the CHIS, record the information supplied by him/her and monitor the security and welfare of the CHIS. Meetings with the source must be recorded, along with details of meeting between the source and the subject of the investigation. Where there are unforeseen occurrences, these should be recorded as soon as practicable after the event, and the authority checked to ensure that it covers the circumstances that have arisen.

11.3 The person with the general oversight of the CHIS will be a 'Controller'.

12. Record keeping

12.1 The Regulation of Investigatory Powers (Source Records) Regulations 2000 provides that the following records must be kept when a CHIS is authorised:

- The identity of the source.
- The identity, where known, used by the source.
- Any relevant investigating authority, other than the Authority, maintaining the records.

- The means by which the source is referred to within each relevant investigating authority.
- Any other significant information connected with the security and welfare of the source.
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that relevant information has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source.
- The date when, and the circumstances in which, the source was recruited.
- The identifies of the persons who will act as handler, controller and person responsible for maintaining records of the use of the source.
- The periods during which those persons have discharged those responsibilities.
- The tasks given to the source and the demands made of him in relation to his activities as a source.
- All contacts or communications between the source and the authority's handler.
- The information obtained by the authority by the conduct or use of the source.
- Any dissemination by that authority of information obtained in that way.
- Any payment benefit or reward made or provided to the source (other than where the source is an authority employee acting as an undercover operative).

12.2 The Code of Practice on the use of CHIS also contains additional advice on records to be kept in relation to a source. In addition to the authorisation forms, risk assessment, and the above information, a record should be kept of the circumstances in which tasks were given to the source and the value of the source to the authority.

12.3 The records must be kept in a way that preserves the confidentiality of the source and the information provided by him/her. Records must not be made available to officers unless it is necessary for them to do so.

12.4The Authorising Officer must not authorise the use of a CHIS until an appropriate officer has been designated as the person with responsibility for maintaining a record of the use made of the CHIS, and arrangements are in place for ensuring that the records will be kept securely.

12.5 All records will be protectively marked, in accordance the with Authority Protective Marking Scheme, to assist in protecting their confidentiality.

13. Safety & security

13.1 Prior to the authorising of a CHIS, the Authorising Officer shall have regard to the safety and welfare of the CHIS and shall continue to have such regard, throughout the use of the CHIS. The safety and welfare of the CHIS after the authorisation has been cancelled or where the investigation has been closed must also be taken into account at the outset. Officers seeking authorisation to use a CHIS must consider the corporate risks to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The nature and magnitude of risk to the source must be identified and evaluated. Risk on a personal, operational and ethical basis must be considered.

These risk assessments must be taken into account by the Authorising Officer in deciding whether it is appropriate for authorisation to be granted for the use of the CHIS, along with the usual considerations of proportionality, necessity etc. The Authorising Officer must satisfy him/herself that any risks identified are justified in relation to the investigation, and that any identified risks have been properly explained and understood by the source. A copy of the risk assessment must be kept in accordance with the preceding paragraph.

13.2 The handler of the CHIS will be responsible for bringing any concerns about the personal circumstances of the source to the attention of the controller, in so far as they may affect the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. Where appropriate such concerns should be brought to the attention of the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

13.3 The use of vulnerable individuals or juveniles for a CHIS purpose must only be authorised by the Chief Fire Officer/ Chief Executive or the Chief Operating Officer and only in the most exceptional cases. The Authorising Officer must also abide by the Code of Practice relating to juveniles. On no account should the use or conduct of a source under 16 years of age be authorised to give information where the relationship to which the use of the source relates is between the source and his parents or any person who has parental responsibility for him. In other cases authorisation should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. These requirements relate to the presence of an appropriate adult (e.g. a parent) at meetings with the source and consideration of risk assessments.

Authorisation of juvenile CHIS may only be granted by the Chief Fire Officer/ Chief Executive or the Chief Operating Officer (or equivalent) and the duration of such an authorisation will be only one month, rather than twelve months.

14. Annual review

14.1 The Authority's Overview & Audit Committee should review use of RIPA and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on a ~~regular~~ quarterly basis to ensure that it is being used consistently with the policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

15. Roles and responsibilities

Senior Responsible Officer

The Senior Responsible Officer (SRO) should be someone, of at least the rank of authorising officer, and should be responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance;
- compliance with Part 2 of the Act and with the Codes;
- engagement with the Office of Surveillance Commissioners (OSC) inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.
- Within local authorities, the SRO should be a member of the corporate leadership team and
- should be responsible for ensuring that all authorising officers are of an appropriate standard in the light of any recommendations in OSC inspection reports. Where a report highlights concerns about the standard of authorising officers, the SRO will be responsible for ensuring the concerns are addressed.

Authorising Officer

- The Authorising Officer is responsible for ensuring that investigations are necessary and proportionate by reference to the law.

- For ensuring that he/she has appoints a person who is responsible for having day to day contact with the CHIS, and a person with the responsibility for the general oversight of the use of the source.
- The Authorising Officer will be a post holder in the role of Group Manager or above.

Co-ordinating Officer

- To provide quarterly reports on RIPA authorisations to Members.
- To review this policy at least annually and provide a full report to Members.
- To publish this policy for use as a training guide for employees.
- To hold a copy of the procedures and guidance issued by the Chief Surveillance Commissioner.
- To support the authorisation process and maintain appropriate records and registers.
- To maintain a training plan to ensure that all Authority employees have an understanding of the legislation proportionate to their role.

16. Record history

1.0 First issue

2.0 Amended to reflect changes in legislation

3.0 Reflects changes in legislation (2012) that came into effect in December 2014

4.0 This issue.