Home Office

Covert Human Intelligence Sources

Draft Code of Practice

Autumn 2017

© Crown copyright [insert year]

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at [www.gov.uk/government/publications or other web/intranet address]

Any enquiries regarding this publication should be sent to us at [insert contact details].

Contents

1	Introduction	7
	Scope of covert human intelligence source activity to which this code applies	8
2	Covert human intelligence sources: definitions and examples	9
	Definition of a covert human intelligence source (CHIS)	9
	Scope of ‘use’ or ‘conduct’ authorisations	9
	Circumstances in which it would be appropriate to authorise the use or conduct of a CHIS	10
	Establishing, maintaining and using a relationship	11
	Legend building	11
	Human source activity falling outside CHIS definition	12
	Public volunteers	12
	Professional or statutory duty	12
	Tasking not involving relationships	13
	Identifying when a human source becomes a CHIS	13
3	General rules on authorisations	15
	Authorising Officer	15
	Necessity and Proportionality	15
	Extent of authorisations	16
	Collateral Intrusion	16
	Reviewing and renewing authorisations	17
	Local considerations and community impact assessments	18
	Combined authorisations	18
	Operations involving multiple CHIS	19
	Covert surveillance of a CHIS	19
	Use of equipment by a CHIS	19
	Use of covert human intelligence sources by local authorities	20
4	Special considerations for authorisations	21
	Vulnerable individuals	21
	Juvenile sources	21
	Scotland	21

International 22
Online Covert Activity 22

5 Authorisation procedures for covert human intelligence sources 25
Authorisation criteria 25
Relevant public authorities 25
Authorisation procedures 26
Information to be provided in applications for authorisation 27
Duration of authorisations 28
Reviews 28
Renewals 28
Cancellations 30
Refusal of approval of long term authorisation 31

6 Management of covert human intelligence sources 32
Tasking 32
Handlers and controllers 32
Joint working 33
Security and welfare 33

7 Keeping of records 35
Centrally retrievable record of authorisations 35
Individual records of authorisation and use of CHIS 35
Further documentation 36
Errors 36

8 Safeguards (including privileged or confidential information) 39
Use of material as evidence 40
Dissemination of information 41
Copying 42
Storage 42
Destruction 43
Protection of the identity of a CHIS 43
Confidential or privileged material 43
Confidential personal information and confidential constituent information 44

Applications to acquire material relating to confidential journalistic material and journalists sources 45

Matters subject to Legal Privilege - Introduction 47

Authorisations for the use or conduct of a CHIS intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege 48

Authorisations for the use or conduct of a CHIS likely to obtain, provide access to or disclose knowledge of matters subject to legal privilege 50

Authorisations for the use or conduct of a CHIS intended to result in the acquisition of knowledge of matters that would be subject to legal privilege if they were not created or held with the intention of furthering a criminal purpose 50

Unintentional obtaining of knowledge of matters subject to legal privilege by a CHIS 51

Lawyers' material 51

The handling, retention and deletion of material subject to legal privilege 52

9 Senior responsible officers and oversight by the Commissioner 55

The senior responsible officer 55

Oversight by the Commissioner 55

10 Complaints 57

11 ANNEX A 58

Enhanced authorisation levels when knowledge of privileged or confidential information may be acquired or when a vulnerable individual or juvenile is to be used as a source. 58

12 ANNEX B 62

Authorisation levels for the enhanced arrangements set out in the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 62

1 Introduction

1.1 This code of practice provides guidance on the authorisation of the use or conduct of covert human intelligence sources ("CHIS") by public authorities under Part II of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"). The code also provides guidance on the handling of any information obtained by use or conduct of a CHIS.

1.2 This code is issued pursuant to Section 71 of the 2000 Act, which provides that the Secretary of State shall issue one or more codes of practice in relation to the powers and duties in Part 2 of the 2000 Act. This code replaces the previous Covert Human Intelligence Sources Code of Practice (dated December 2014). This version of the code reflects changes to the oversight of investigatory powers made under the Investigatory Powers Act 2016 ("the 2016 Act"), including oversight by the Investigatory Powers Commissioner ("the Commissioner"). The previous arrangements, set out in the code of practice issued in December 2014, should be applied until the relevant provisions of the 2016 Act have been commenced.

1.3 This code of practice is primarily intended for use by the public authorities able to authorise activity under the 2000 Act. It will also allow other interested persons to understand the procedures to be followed by those public authorities. This code is publicly available and should be readily accessible by members of any relevant public authority seeking to use the 2000 Act to authorise the use or conduct of CHIS[1].

1.4 The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under the 2000 Act, or to the Investigatory Powers Commissioner, it must be taken into account. Public authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

1.5 Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are included for guidance only. It is not possible for theoretical examples to replicate the level of detail to be found in real cases. Consequently, public authorities should avoid allowing superficial similarities with the examples to determine their decisions and should not seek to justify their decisions solely by reference to the examples rather than to the law, including the provisions of this code. The examples should not be taken as confirmation that any particular public authority undertakes the activity described; the examples are for illustrative purposes only.

[1] Being those listed in or added to Part I of Schedule 1 of the 2000 Act.

Scope of covert human intelligence source activity to which this code applies

1.6 Part II of the 2000 Act provides for the authorisation of the use or conduct of CHIS. The definitions of these terms are laid out in section 26 of the 2000 Act and chapter 2 of this code. Not all human sources of information will fall within these definitions and an authorisation under the 2000 Act will therefore not always be appropriate.

1.7 Neither Part II of the 2000 Act nor this code of practice is intended to affect the existing practices and procedures surrounding criminal participation of CHIS.

2 Covert human intelligence sources: definitions and examples

Definition of a covert human intelligence source (CHIS)

2.1 Under the 2000 Act, a person is a CHIS if:

- they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph 26(8)(b) or (c);
- they covertly use such a relationship to obtain information or to provide access to any information to another person; or
- they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.[2]

2.2 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.[3]

2.3 A relationship is used covertly, and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.[4]

2.4 The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 ("the 2013 Relevant Sources Order") further defines a particular type of CHIS as a 'relevant source'. This is a source holding an office, rank or position with the public authorities listed in the Order and Annex B to this code. Enhanced authorisation arrangements are in place for this type of CHIS as detailed in this code. Such sources will be referred to as a 'relevant source' throughout this code.

2.5 Any Police Officer deployed as a 'relevant source' in England and Wales will be required to comply with and uphold the principles and standards of professional behaviour set out in the College of Policing Code of Ethics.

Scope of 'use' or 'conduct' authorisations

2.6 Subject to the procedures outlined in chapter 3 of this code, an authorisation may be obtained under Part II of the 2000 Act for the use or conduct of CHIS.

2.7 The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means

[2] See section 26(8) of the 2000 Act

[3] See section 26(9)(b) of the 2000 Act for full definition

[4] See section 26(9)(c) of the 2000 Act for full definition

of the conduct of a CHIS.[5] In general, therefore, an authorisation for use of a CHIS will be necessary to authorise steps taken by a public authority in relation to a CHIS.

2.8 The conduct of a CHIS is any conduct of a CHIS which falls within paragraph 2.1 above or is incidental to anything falling within that paragraph. In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of a public authority.[6]

2.9 Most CHIS authorisations will be for both use and conduct. This is because public authorities usually take action in connection with the CHIS, such as tasking the CHIS to undertake covert action, and because the CHIS will be expected to take action in relation to the public authority, such as responding to particular tasking.

2.10 Care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant applications, reviews, renewals and cancellations are correctly performed. A CHIS may in certain circumstances be the subject of different use or conduct authorisations obtained by one or more public authorities. Such authorisations should not conflict.

2.11 The reactive nature of the work of a CHIS, and the need for a CHIS to maintain cover, may make it necessary for a CHIS to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct. Such incidental conduct is regarded as properly authorised by virtue of sections 26(7)(a), 27 and 29(4) of the 2000 Act, even though it was not specified in the initial authorisation. This is likely to occur only in exceptional circumstances, such as where the incidental conduct is necessary to protect life and limb, including in relation to the CHIS, or national security, in circumstances that were not envisaged at the time the authorisation was granted.

Circumstances in which it would be appropriate to authorise the use or conduct of a CHIS

2.12 Public authorities are not required by the 2000 Act to seek or obtain an authorisation just because one is available (see section 80 of the 2000 Act), The use or conduct of a CHIS, however, can be a particularly intrusive and high risk covert technique, requiring dedicated and sufficient resources, oversight and management. Authorisation is therefore advisable where a public authority intends to task someone to act as a CHIS. Public authorities must ensure that all use or conduct is:

- necessary and proportionate to the intelligence dividend that it seeks to achieve;
- in compliance with relevant Articles of the European Convention on Human Rights (ECHR), particularly Articles 6 and 8.

2.13 Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. ECHR case law makes it clear that Article 8 includes the right to establish and

[5] See section 26(7)(b) of the 2000 Act

[6] See section 26(7)(a) of the 2000 Act

develop relationships. Accordingly, any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

2.14 It is therefore strongly recommended that a public authority consider an authorisation whenever the use or conduct of a 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 public authority.

Establishing, maintaining and using a relationship

2.15 The word "establishes" when applied to a relationship means "set up". It does not require, as "maintains" does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity.

Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

Legend building

2.16 When a relevant source (detailed at paragraph 2.4) is deployed to establish their 'legend'/ build up their cover profile, an authorisation must be considered under the 2000 Act if the activity will interfere with an individual's Article 8 rights. This will include circumstances where it is not clear to the individual that the relevant source is not who he or she claims to be. The individual does not have to be the subject of any current or future investigation. Interference with any individual's Article 8 rights requires authorisation under the 2000 Act. Where authorisation is not considered necessary, arrangements should be in place to maintain active review of this position, and any decision not to authorise should be made by the person prescribed to act as the authorising officer.

Human source activity falling outside CHIS definition

2.17 Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of a covert relationship. Further detail on each of these circumstances is provided below.

Public volunteers

2.18 In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that they have observed or acquired other than through a relationship, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation under the 2000 Act is required.[7]

Example 1: A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.

Example 2: A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.

Professional or statutory duty

2.19 Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 are required to report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

2.20 Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

[7] See Chapter 3 of this code for further guidance on types of source activity to which authorisations under Part II of the 2000 Act may or may not apply.

2.21 Furthermore, this reporting is undertaken 'in accordance with the law' and therefore any interference with an individual's privacy (Article 8 rights) will be in accordance with Article 8(2) ECHR.

2.22 This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on. For example, a travel agent who is asked by the police to find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances, a CHIS authorisation may be appropriate.

Tasking not involving relationships

2.23 Tasking a person to obtain information covertly may result in authorisation under Part II of the 2000 Act being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

Example: A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

Identifying when a human source becomes a CHIS

2.24 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

2.25 Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

Example: Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is

likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague.

2.26 However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible, therefore, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes.

3 General rules on authorisations

Authorising Officer

3.1 Responsibility for giving the authorisation will depend on which public authority is responsible for the CHIS. For the purposes of this code, the person in a public authority responsible for granting an authorisation will be referred to as the "authorising officer". The relevant public authorities and authorising officers are listed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") as amended by the 2013 Relevant Sources Order.

Necessity and Proportionality

3.2 The 2000 Act stipulates that the authorising officer must believe that an authorisation for the use or conduct of a CHIS is necessary in the circumstances of the particular case for one or more of the statutory grounds listed in section 29(3) of the 2000 Act.

3.3 If the use or conduct of the CHIS is deemed necessary on one or more of the statutory grounds, the person granting the authorisation must also believe that it is proportionate to what is sought to be achieved by carrying it out. The degree of intrusiveness of the actions tasked on or undertaken by an authorised CHIS will vary from case to case, and therefore proportionality must be assessed on an individual basis. This involves balancing the seriousness of the intrusion into the private or family life of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.4 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the use or conduct of a CHIS proportionate. Similarly, an offence may be so minor that any deployment of a CHIS would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.5 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully;

- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought.

3.6 The fact that an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the authorisation is necessary on the grounds on which authorisations may be granted.

Extent of authorisations

3.7 An authorisation under Part II of the 2000 Act for the use or conduct of a CHIS will provide lawful authority for any such activity that:

- involves the use or conduct of a CHIS as is specified or described in the authorisation;
- is carried out by or in relation to the person to whose actions as a CHIS the authorisation relates; and
- is carried out for the purposes of, or in connection with, the investigation or operation so described.[8]

3.8 In the above context, it is important that the CHIS is fully aware of the extent and limits of any conduct authorised, and that those involved in the use of a CHIS are fully aware of the extent and limits of the authorisation in question.

Collateral Intrusion

3.9 Before authorising the use or conduct of a source, the authorising officer should take into account the risk of interference with the private or family life of persons who are not the intended subjects of the CHIS activity (collateral intrusion). Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where confidential communications of a Member of Parliament may be involved (see chapter 8).

3.10 Measures should be taken, wherever practicable, to avoid or minimise interference with the private or family life of those who are not the intended subjects of the CHIS activity. Where such collateral intrusion is unavoidable, the activities may still be authorised providing this collateral intrusion is considered proportionate to the aims of the intended intrusion. Any collateral intrusion should be kept to the minimum necessary to achieve the objective of the operation.

3.11 All applications should therefore include an assessment of the risk of any collateral intrusion, and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed use or conduct of a CHIS.

3.12 Where CHIS activity is deliberately proposed against individuals who are not suspected of direct or culpable involvement in the matter being investigated, interference with the private or family life of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such

[8] See section 29(4) of the 2000 Act.

interference should be carefully considered against the necessity and proportionality criteria as described above.

Example 1: A relevant source is deployed to obtain information about the activities of a suspected criminal gang under CHIS authorisation. It is assessed that the relevant source will in the course of this deployment obtain private information about some individuals who are not involved in criminal activities and are of no interest to the investigation. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation.

Example 2: The police seek to establish the whereabouts of Mr W in the interests of national security. In order to do so, a relevant source is deployed to seek to obtain this information from Mr P, an associate of Mr W who is not of direct security interest. An application for a CHIS authorisation is made to authorise the deployment. The authorising officer will need to consider the necessity and proportionality of the operation against Mr P and Mr W, who will be the direct subjects of the intrusion. The authorising officer will also need to consider the proportionality of any collateral intrusion that will arise if there is any additional interference with the private or family life of other individuals of no interest to the investigation.

Reviewing and renewing authorisations

3.13 Except where enhanced arrangements under the 2013 Relevant Sources Order apply, the authorising officer who grants an authorisation should, where possible, be responsible for considering subsequent renewals of that authorisation and any related security and welfare issues.

3.14 The authorising officer will stipulate the frequency of formal reviews and the controller (see paragraph 6.9 below) should maintain an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation. This will not prevent additional reviews being conducted by the authorising officer in response to changing circumstances such as described below.

3.15 Where the nature or extent of intrusion into the private or family life of any person becomes greater than that anticipated in the original authorisation, the authorising officer should immediately review the authorisation and reconsider the proportionality of the operation. This should be highlighted at the next renewal (if applicable).

3.16 Where a CHIS authorisation provides for interference with the private or family life of initially unidentified individuals whose identity is later established, a new authorisation is not required provided the scope of the original authorisation envisaged interference with the private or family life of such individuals.

Example: An authorisation is obtained by the police to authorise a CHIS to use her relationship with "Mr X and his close associates" for the covert purpose of providing information relating to their suspected involvement in a crime. Mr X introduces the CHIS to Mr A, a close associate of Mr X. It is assessed that obtaining more information on Mr A will assist the investigation. The CHIS may use her relationship with Mr A to obtain such information but the review of the authorisation should

specify any interference with the private or family life of "Mr X and his associates, including Mr A" and that such an interference is in accordance with the original authorisation.

3.17 Any proposed changes to the nature of the CHIS operation (i.e. the activities involved) should immediately be brought to the attention of the authorising officer. The authorising officer should consider whether the proposed changes are within the scope of the existing authorisation and whether they are proportionate (bearing in mind any extra interference with private or family life or collateral intrusion), before approving or rejecting them. Any such changes should be highlighted at the next renewal (if applicable).

Local considerations and community impact assessments

3.18 Any person granting or applying for an authorisation will also need to be aware 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 have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS.

3.19 It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should, where possible, consult a senior officer within the police force area in which the CHIS is deployed. All public authorities, where possible, should consider consulting with other relevant public authorities to gauge community impact.

Combined authorisations

3.20 A single authorisation may combine two or more different authorisations under Part II of the 2000 Act.[9] For example, a single authorisation may combine authorisations for intrusive surveillance and the conduct of a CHIS. In such cases, the provisions applicable to each of the authorisations must be considered separately by the appropriate authorising officer. Thus, a superintendent or an assistant chief constable (for relevant sources) can authorise the conduct of a CHIS, but an authorisation for intrusive surveillance by the police needs the separate authorisation of a chief constable (and the prior approval of a Judicial Commissioner, except in cases of urgency).

3.21 Where an authorisation for the use or conduct of a CHIS is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State.

3.22 The above considerations do not preclude public authorities from obtaining separate authorisations.

[9] See section 43(2) of the 2000 Act.

Operations involving multiple CHIS

3.23 A single authorisation under Part II of the 2000 Act may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several undercover operatives acting as CHISs in situations where the activities to be authorised, the subjects of the operation, the interference with private or family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each officer. If an authorisation includes more than one relevant source, each relevant source must be clearly identifiable within the documentation. In these circumstances, adequate records must be kept of the length of deployment of a relevant source to ensure the enhanced authorisation process set out in the 2013 Relevant Sources Order and Annex B of this code can be adhered to. (See also paragraph 4.16)

Covert surveillance of a CHIS

3.24 It may be necessary to deploy covert surveillance against a potential or authorised CHIS, other than those acting in the capacity of an undercover operative, as part of the process of assessing their suitability for recruitment, deployment or in planning how best to make the approach to them. Covert surveillance in such circumstances may or may not be necessary on one of the statutory grounds on which directed surveillance authorisations can be granted, depending on the facts of the case. Whether or not a directed surveillance authorisation is available, any such surveillance must be justifiable under Article 8(2) of the ECHR.

Use of equipment by a CHIS

3.25 A CHIS wearing or carrying a surveillance device does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. However, if a surveillance device is to be used other than in the presence of the CHIS, an intrusive or directed surveillance authorisation should be obtained where appropriate, together with an authorisation for interference with property, if applicable. See the Covert Surveillance and Property Interference code of practice.

3.26 A CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations or other forms of communication, other than by interception, which takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way.

3.27 If a CHIS is acting on behalf of one of the bodies to which the equipment interference provisions of the Investigatory Powers Act 2016 apply, and is required as part of his or her tasking to interfere with equipment in order to obtain communications, equipment data or other information, that interference should be authorised separately by a warrant under that Act.

Use of CHIS by local authorities

3.28 The Protection of Freedoms Act 2012 amended the 2000 Act to make CHIS authorisations by local authorities in England and Wales subject to judicial approval. These changes mean that local authorities need to obtain an order approving the grant or renewal of a CHIS authorisation from a Justice of the Peace before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the CHIS as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of CHIS. Further detail on these changes is set out in separate guidance for local authorities and the judiciary, available on the .gov.uk website.[10]

3.29 In Northern Ireland the requirement introduced by the Protection of Freedoms Act applies only to local authority CHIS authorisations where the grant or renewal relates to a Northern Ireland excepted or reserved matter. Where such an authorisation is required by a local authority in Northern Ireland, an application for a grant or renewal should be made to a district judge. For other authorisations, local authorities in Northern Ireland should refer to the general requirements for authorisation set out in this code. In Scotland, CHIS authorisations are governed by RIP(S)A and a separate code of practice applies.

3.30 Elected members of a local authority should review the authority's use of the 2000 Act and set the policy at least once a year. They should also consider internal reports on use of the 2000 Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

[10] https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

4 Special considerations for authorisations

Vulnerable individuals

4.1 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an individual may be vulnerable, they should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases, Annex A lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a CHIS.

Juvenile sources

4.2 Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for him. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000, are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is one month from the time of grant or renewal (instead of twelve months). For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

Scotland

4.3 Where all the conduct authorised is likely to take place in Scotland, authorisations should be granted under RIP(S)A, unless:

- the authorisation is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000;
- the authorisation is to be granted or renewed (by any relevant public authority) for the purposes of national security or the economic well-being of the UK; or
- the authorisation authorises conduct that is surveillance by virtue of section 48(4) of the 2000 Act.

4.4 This code of practice is extended to Scotland in relation to authorisations granted under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to authorisations granted under RIP(S)A.

International

4.5 Authorisations under the 2000 Act can be given for the use or conduct of CHIS both inside and outside the UK. However, authorisations for actions outside the UK can usually only validate them for the purposes of UK law. The risks of any liability arising under local law should be considered and mitigated where possible.

4.6 Public authorities are therefore advised to seek authorisations where available under the 2000 Act for any overseas operations where the subject of investigation is a UK national or is likely to become the subject of criminal or civil proceedings in the UK, or if the operation is likely to affect a UK national or give rise to material likely to be used in evidence before a UK court.

4.7 Public authorities must have in place internal systems to manage any overseas CHIS deployments and it is recognised practice for UK law enforcement agencies to follow the authorisation and management regime under the 2000 Act, even where such deployments are only intended to impact locally and are therefore authorised under local domestic law. However, public authorities should take care to monitor such deployments to identify where civil or criminal proceedings may become a prospect in the UK and ensure that, where appropriate, an authorisation under Part II of the 2000 Act is sought if this becomes the case.

4.8 The Human Rights Act 1998 applies to all activity taking place within the UK. This should be taken to include overseas territories and facilities which are within the jurisdiction of the UK. Authorisations under the 2000 Act may therefore be appropriate for overseas covert operations occurring in UK Embassies, military bases, detention facilities, etc., in order to comply with rights to privacy under Article 8 of the ECHR.[11]

4.9 Members of foreign law enforcement or other agencies or CHIS of those agencies may be authorised under the 2000 Act in the UK in support of domestic and international investigations. When a member of a foreign law enforcement agency is authorised in support of a domestic or international investigation or operation consideration should be given to authorising the individual at the level prescribed by the 2013 Relevant Sources Order as if the individual holds an 'office, rank or position' with an organisation listed in the same Order.

Online Covert Activity

4.10 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity[12], should consider whether the activity requires a CHIS authorisation. A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

---

[11] See Al Skeini v UK June 2007. If conduct is to take place overseas the NPCC Covert Legislation and Guidance Working Group may be able to offer additional advice.

[12] As an official rather than private individual

4.11 Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person.
- Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.
- Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

4.12 A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authority need not be sought.

Example 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4.13 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Example 1: *An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or*

investigation. As part of the legend building activity he "follows" a variety of people and entities and "likes" occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.

Example 2: *The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.*

4.14 When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

4.15 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.13 of this code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

4.16 Where it is intended that more than one officer will share the same online persona each officer should be clearly identifiable within the overarching authorisation for that operation providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved. (See also paragraph 3.23)

5 Authorisation procedures for CHIS

Authorisation criteria

5.1 Under section 29(3) of the 2000 Act an authorisation for the use or conduct of a CHIS may be granted by the authorising officer where they believe that the authorisation is necessary:

- in the interests of national security;[13]
- for the purpose of preventing or detecting crime[14] or of preventing disorder;
- in the interests of the economic well-being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health;[15]
- 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.[16]

5.2 The authorising officer must also believe that the authorised use or conduct of CHIS is proportionate to what is sought to be achieved by that use or conduct.

Relevant public authorities

5.3 The public authorities entitled to authorise the use or conduct of a CHIS, together with the specific purposes for which each public authority may authorise the use or conduct of a CHIS, are laid out in Schedule 1 of the 2000 Act and the 2010 CHIS Order as amended by the 2013 Relevant Sources Order.

---

[13] One of the functions of the Security Service is the protection of national security and in particular the protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. These functions extend throughout the UK. An authorising officer in another public authority should not issue an authorisation under Part II of the 2000 Act where the operation or investigation falls within the responsibilities of the Security Service, as set out above, except where it is to be carried out by a Special Branch, Counter Terrorism Unit or Counter Terrorism Intelligence Unit or where the Security Service has agreed that another public authority can authorise the use or conduct of a CHIS which would normally fall within the responsibilities of the Security Service. HM Forces may also undertake operations in connection with national security in support of the Security Service or other Civil Powers.

[14] Detecting crime is defined in section 81(5) of the 2000 Act. Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

[15] This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

[16] This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

Authorisation procedures

5.4 Responsibility for authorising the use or conduct of a CHIS rests with the authorising officer and all authorisations require the personal authority of the authorising officer. The 2010 CHIS Order as amended by the 2013 Relevant Sources Order designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases. In certain circumstances the Secretary of State will be the authorising officer (see section 30(2) of the 2000 Act).

5.5 The authorising officer must give authorisations 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).

5.6 Other officers entitled to act in urgent cases may only give authorisation in writing e.g. written authorisation for use or conduct of a relevant source given by a Superintendent.

5.7 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.

5.8 Authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the CHIS, the handler of the CHIS or the controller. Furthermore, authorising officers should, where possible, be independent of the investigation. However, it is recognised that this is not always possible, especially in the cases of small organisations, or where it is necessary to act urgently or for security reasons. However, where possible, clear separation should be maintained between those responsible for the investigation and those managing the CHIS to ensure that the welfare and safety of the CHIS are always given due consideration. Where an authorising officer authorises their own activity, the central record of authorisations should highlight this and the attention of the Investigatory Powers Commissioner or inspectors who support the work of the Commissioner should be invited to it during the next inspection. Where a relevant source is deployed on more than one operation, in the same or different force/regions, it is essential that the authorising officer is informed of that other authorised activity and any risk in relation to this that might affect the activity for which they are responsible.

5.9 Authorising officers within Police Scotland may only grant authorisations on application by a member of (including those formally seconded to) their own force. The same rules apply to authorising officers within police forces and the National Crime Agency, unless relevant Chief Officers have made collaboration agreements under the Police Act 1996. Authorising officers within HMRC may only grant authorisations on application by an officer of Revenue and Customs.

5.10 All authorisations of relevant sources by public authorities named in the 2013 Relevant Sources Order should be notified to the Investigatory Powers Commissioner within 7 days when granted by the authorising officer, save where there is a requirement to seek prior approval. A Judicial Commissioner may provide comments to the authorising officer. The authorising officer will be advised promptly of any comments made by a Judicial Commissioner. The authorising officer will wish to consider all comments made by the Judicial Commissioner. Public authorities listed in the 2013 Relevant Sources Order should provide the Investigatory Powers Commissioner with the authorisation and associated risk assessment for each relevant source.

Information to be provided in applications for authorisation

5.11 An application for authorisation for the use or conduct of a CHIS should be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in section 29(3) of the 2000 Act (e.g. for the purpose of preventing or detecting crime);
- the purpose for which the CHIS will be tasked or deployed (e.g. in relation to drug supply, stolen property, a series of racially motivated crimes, etc.);
- where a specific investigation or operation is involved, the nature of that investigation or operation;
- the nature of what the CHIS conduct will be;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any material subject to legal privilege or other confidential material that may be obtained as a consequence of the authorisation;
- where the intention is to acquire knowledge of matters subject to legal privilege, the exceptional and compelling circumstances that make the authorisation necessary;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the level of authorisation required (or recommended, where that is different); and
- a subsequent record of whether authorisation was given or refused, by whom and the time and date.

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

- the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was given; or
- the reasons why the officer entitled to act in urgent cases considered the case so urgent and why it was not reasonably practicable for the application to be considered by the authorising officer.

5.13 Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant when reasonably practicable (generally the next working day).

5.14 When completing an application, the public authority must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In

particular, all reasonable efforts should be made to take account of information which weakens the case for the authorisation.

Duration of authorisations

5.15 A written authorisation will, unless renewed or cancelled, cease to have effect at the end of a period of twelve months beginning with the day on which it took effect, except in the case of juvenile CHIS or where it is intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege. So an authorisation given at 09.00 on 12 February will expire on 11 February. Authorisations (except those granted under urgency procedures) will cease at 23.59 on the last day, with any subsequent renewal commencing at 00.00 hours the following day.

5.16 An authorisation for the use or conduct of a juvenile CHIS is one month from the date the authorisation is given (see 4.2 above for further detail).

5.17 An authorisation where it is intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege is reduced from the usual 12 months to 6 months (in the case of an intelligence service authorisation), or 3 months (for any other public authority). Paragraphs 8.54 to 8.59 provide more detail on authorisations where the 2010 Legal Privilege Order is applicable.

5.18 Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy two hours, beginning with the time when the authorisation was granted. Local authorities are not able to orally authorise the use of CHIS (see paragraph 3.28 above), but arrangements should be in place with Her Majesty's Court Service to enable judicial approval of out of hours applications.

Reviews

5.19 Regular reviews of authorisations should be undertaken by the authorising officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. (See paragraphs 8.9 to 8.11 below)

Renewals

5.20 Before an authorising officer renews an authorisation, they must be satisfied that a review has been carried out of the use of a CHIS, as outlined above, and that the results of the review have been considered.

5.21 If, 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, they may renew it in writing for a further period of twelve months. Renewals may also be granted orally in urgent cases and last for a period of seventy-two hours.

5.22 A renewal takes effect at the time at which the authorisation would have ceased to have effect but for the renewal. An application for renewal should therefore not be made until shortly before the authorisation period is drawing to an end.

5.23 Except where enhanced arrangements exist, the authorising officer who granted the authorisation, or the officer undertaking that function, should renew the authorisation. In the case of a relevant source, renewals for deployment beyond 12 months should be carried out by a Chief Constable or equivalent and pre-approved by a Judicial Commissioner.

5.24 Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. Documentation of the renewal should be retained for at least three years (see chapter 7).

5.25 All applications by public authorities named in the 2013 Relevant Sources Order for an authorisation of a relevant source beyond 12 months (i.e. long term authorisation) must be approved by a Judicial Commissioner before authorisation by the appropriate authorising officer. The 2013 Relevant Sources Order creates an enhanced regime of prior approval for such authorisations.

5.26 The 2013 Relevant Sources Order defines long term authorisation by reference to the cumulative periods for which the relevant source will be/has been authorised on the same investigation or operation. A long term authorisation is one where the cumulative periods exceed 12 months, or, where the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 ("the 2010 Legal Privilege Order") applies, 3 months. If a relevant source has not been authorised on the same investigation or operation for at least 3 years, any previous authorisations will be disregarded for the purposes of calculating the 12 months.

5.27 When deciding if the relevant source is authorised as part of the 'same investigation or operation' in calculating the period of total or accrued deployment or cumulative authorisation periods, the following should be considered:

- common subject or subjects of the investigation or operation;
- the nature and details of relationships established in previous or corresponding relevant investigations or operations;
- whether or not the current investigation is a development of or recommencement to previous periods of authorisation, which may include a focus on the same crime group or individuals;
- previous activity by the relevant source that has a bearing by way of subject, locality, environment or other consistent factors should be considered in calculating the period;
- the career history of the 'relevant source'.

5.28 Where an over-arching authorisation has been provided as a framework for investigators to establish an online presence intended to provide a basis for future enforcement activity, this should be treated as part of the same investigation or operation for renewal purposes. However, where this generic activity leads to a separate operation against subjects identified through the online presence, a fresh authorisation should be considered on a case by case basis.

5.29 Public authorities named in the 2013 Relevant Sources Order should notify the Investigatory Powers Commissioner at the 9 month point of any authorisation that may require renewal beyond 12 months (as calculated in the paragraph above).

Example 1: A twelve month authorisation has been granted by the Assistant Chief Constable of a police force for a relevant source against a subject for the purposes of collecting intelligence about drug supply. The authority is cancelled after six months because the subject disappears and there is insufficient evidence obtained at that time to prosecute. A year later, the subject then returns to deal drugs in the area again and the police force wishes to authorise another relevant source against the subject. If the same relevant source is used, authorisation by an Assistant Chief Constable will be for maximum of 6 months. If the police force decides to use different relevant sources against the subject, an Assistant Chief Constable can grant the authority for 12 months and it is treated as a new authority, provided the relevant sources have not been previously authorised in respect of the same investigation or operation.

Example 2: An authorisation for use of a relevant source is initially granted by an Assistant Chief Constable. After 3 months, it is apparent that legally privileged material may be accessed. Prior approval by the Investigatory Powers Commissioner was granted and a new authorisation granted by the Chief Constable for an additional three months. At the end of this period it was agreed the relevant source would no longer be likely to access any legally privileged material. A new authorisation for a maximum of 6 months could then be granted by the Assistant Chief Constable. The entire period of deployment, including the three months at the higher level for access to legally privileged material, would count toward the 12 month period. Who granted the authorisation for the relevant source and what type of material they had access to is not relevant for the purposes of calculating the 12 month period. If the authorisation is renewed at the end of the 6 month period, it becomes a long term authorisation and approval of the Investigatory Powers Commissioner and authorisation by the Chief Constable is required.

5.30 All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in the initial application;
- the reasons why it is necessary for the authorisation to continue;
- 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 or conduct of the CHIS; and
- the results of regular reviews of the use of the CHIS.

Cancellations

5.31 The authorising officer who granted or renewed the authorisation must cancel it if they are satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation, or that arrangements for the CHIS's case no longer satisfy the requirements described in section 29 of the 2000 Act. Where the authorising officer is no longer available, this duty will fall to the person who has taken over the role of authorising officer or the person who is acting as authorising officer.

5.32 Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and risk assessments maintained in accordance with paragraph 6.13 below. The authorising

officer will wish to satisfy themselves that all welfare matters are addressed, and should make appropriate comment in their written commentary.

Refusal of approval of long term authorisation

5.33 If a Judicial Commissioner does not conclude a long term authorisation of a relevant source should be granted by the Chief Constable (or equivalent), the relevant public authority may appeal against the decision to the Investigatory Powers Commissioner within 7 days.

5.34 Any risk assessment produced for a relevant source should include details of how the relevant source can be safely extracted should approval by a Judicial Commissioner be refused.

6 Management of CHIS

Tasking

6.1 Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain, provide access to or disclose information. Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

6.2 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If there is a step change in the nature of the task that significantly alters the entire deployment, then a new authorisation may need to be sought. If in doubt, advice should be sought from the Investigatory Powers Commissioner.

6.3 It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event, and if the existing authorisation is insufficient, it should either be updated at a review (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

6.4 Similarly, where it is intended to task a CHIS in a significantly greater or different way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Handlers and controllers

6.5 Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officersacting as 'controller' and 'handler' for each CHIS (as defined in sections 29(4A) and (4B) and 29(5)(a) and (b) of the 2000 Act).

6.6 The person referred to in section 29(5)(a) of the 2000 Act (the "handler") will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

6.7 The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

6.8 The person referred to in section 29(5)(b) of the 2000 Act (the "controller") will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

6.9 Oversight and management arrangements for undercover operatives, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of public authorities. The role of the handler will be undertaken by a person referred to as a 'cover officer' and the role of controller will be undertaken by a 'covert operations manager'.

Joint working

6.10 There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. Such cases may include:

- The prevention or detection of criminal matters affecting a national or regional area, for example where the CHIS provides information relating to cross boundary or international drug trafficking;
- The prevention or detection of criminal matters affecting crime and disorder, requiring joint agency operational activity, for example where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/ local authority anti-social behaviour operation on a housing estate;
- Matters of national security, for example where the CHIS provides information relating to terrorist activity and associated criminal offences for the benefit of the police and the Security Service.

6.11 In cases where the authorisation is for the use or conduct of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The applicant, controller and handler of a CHIS need not be from the same public authority. In such situations, however, the public authorities involved must lay out in writing their agreed oversight arrangements.

6.12 Management responsibility for CHIS, and relevant roles, may also be divided between different police forces and the National Crime Agency where there is a collaboration agreement under the Police Act 1996 and the collaboration agreement provides for this to happen.

Security and welfare

6.13 Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each

authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset and reviewed throughout the period of authorised activity by that CHIS. Consideration should also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of a CHIS. For example this could be by means of disclosure to a Court or Tribunal, or any other circumstances where disclosure of information may be required, and strategies for minimising the risks to the CHIS or others should be put in place. Additional guidance about protecting the identity of the CHIS is provided at paragraphs 8.22 to 8.25 below.

6.14 The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

6.15 Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

7 Keeping of records

Centrally retrievable record of authorisations

7.1 A centrally retrievable record of all authorisations should be held by each public authority. These records need only contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised. These records should be updated whenever an authorisation is granted, renewed or cancelled and should be made available to the Investigatory Powers Commissioner upon request. These records should be used when calculating the period of deployment for the purposes of the 2013 Relevant Sources Order. These records should be retained for a period of at least five years from the ending of the authorisations to which they relate.

7.2 While retaining such records for the time stipulated, public authorities must take into consideration the duty of care to the CHIS, the likelihood of future criminal or civil proceedings relating to information supplied by the CHIS or activities undertaken, and specific rules relating to data retention, review and deletion under the Data Protection Act and, where applicable, the code of practice on the Management of Police Information.

7.3 Records must be retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of the Act), particularly where continuing conduct is alleged. It is thus desirable if possible to retain records for up to five years.

Individual records of authorisation and use of CHIS

7.4 Detailed records must be kept of the authorisation and use made of a CHIS. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records. Where a CHIS is authorised under the terms of a Police Act 1996 collaboration agreement, that agreement should explicitly state on which force or agency's central record the authorisation should be recorded. This is likely to be either the force or agency providing the authorising officer, or the designated lead force or agency. The fact that the authorisation was given under these terms should be recorded on the central record.

7.5 Public authorities are encouraged to maintain auditable records for individuals providing intelligence who do not meet the definition of a CHIS. This will assist authorities to monitor the status of a human source and identify whether that person should be duly authorised as a CHIS. This should be updated regularly to explain

why authorisation is not considered necessary. Such decisions should rest with those designated as authorising officers within public authorities.

Further documentation

7.6 In addition, records or copies of the following, as appropriate, should be kept by the relevant authority for at least five years:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation; and
- the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.
- A copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months (where applicable).

7.7 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS.

Errors

7.8 This section provides information regarding errors. Proper application of the covert human intelligence source provisions provided for in Part II of the 2000 Act should reduce the scope for making errors. Public authorities will be expected to have thorough procedures in place to comply with these provisions, including for example the careful preparation and checking of warrants and authorisations, reducing the scope for making errors.

7.9 Wherever possible, any technical systems should incorporate functionality to minimise errors. A person holding a senior position within each public authority must undertake a regular review of errors and a written record must be made of each review.

7.10 An error must be reported if it is a “relevant error”. Under section 231(9) of the 2016 Act, a relevant error for the purpose of activity covered by this code is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act. Examples of relevant errors occurring would include circumstances where:

- Covert human intelligence source activity has taken place without lawful authority.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 8 of this Code.

7.11 Errors can have very significant consequences on an affected individual's rights and, in accordance with section 235(6) of the 2016 Act, all relevant errors made by public authorities must be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error.

7.12 When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the Investigatory Powers Commissioner. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

7.13 From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the public authority must also inform the Commissioner of when it was initially identified that an error may have taken place.

7.14 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days (or as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report should include information on the cause of the error; the amount of covert human intelligence source activity conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

7.15 The Investigatory Powers Commissioner may issue guidance as necessary, including guidance on the format of error reports. Public authorities must have regard to any guidance on errors issued by the Investigatory Powers Commissioners.

7.16 In addition to the above, errors may arise where a warrant or authorisation has been obtained as a result of the public authority having been provided with information which later proved to be incorrect due to an error on the part of the person providing the information, but on which the public authority relied in good faith. Whilst these actions do not constitute a relevant error on the part of the authority which acted on the information, such occurrences should be brought to the attention of the Investigatory Powers Commissioner. Where reporting such circumstances to the Investigatory Powers Commissioner, the processes outlined at paragraph 7.12 apply as they apply to the reporting of a relevant error.

Serious Errors

7.17 Section 231 of the Act states that the Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

7.18 In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

- The seriousness of the error and its effect on the person concerned;
- The extent to which disclosing the error would be contrary to the public interest or prejudicial to:
    - national security;
    - the prevention or detection of serious crime;
    - the economic well-being of the United Kingdom; or
    - the continued discharge of the functions of any of the security and intelligence services

7.19 Before making his or her decision, the Commissioner must ask the public authority which has made the error to make submissions on the matters concerned. The submissions from the public authority should include any information which they consider is relevant to the Commissioner's decision. For example, the public authority should flag any risks that the disclosure of information may pose to the safety or security of any person or the possibility of compromising the use of covert tactics and techniques. Public authorities must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

7.20 When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

8 Safeguards (including privileged or confidential information)

8.1 This chapter provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through use or conduct of a CHIS. It also details the procedures and safeguards to be applied where authorisations are likely to result in the acquisition of material subject to legal privilege, or other confidential material including journalistic material and the constituency business of Members of Parliament.

8.2 Public authorities should ensure that their actions when handling private information obtained by means of the use or conduct of a CHIS comply with relevant legal frameworks so that any interference with privacy is justified in accordance with Article 8(2) of the ECHR. Compliance with these legal frameworks, including data protection requirements, will ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.

8.3 All material obtained through the use or conduct of a CHIS must be handled in accordance with safeguards which the public authority has implemented in line with the requirements of this code. These safeguards should be made available to the Investigatory Powers Commissioner. Breaches of these safeguards must be reported to the Investigatory Powers Commissioner in a fashion agreed with him or her. Any breaches of data protection requirements should also be reported to the Information Commissioner. Public authorities must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, public authorities must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

8.4 Dissemination, copying and retention of material obtained through use or conduct of a CHIS must be limited to the minimum necessary for the authorised purposes. Something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary for any of the statutory purposes set out in the 2000 Act in relation to the use or conduct of a CHIS;
- is necessary for facilitating the carrying out of the functions under the Act of the public authority;
- is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

Use of material as evidence

8.5 Subject to the provisions in this chapter of the code, material obtained from a CHIS may be used as evidence in criminal proceedings.[17] The admissibility of evidence is governed by the common law, section 78 of the Police and Criminal Evidence Act 1984[18] and the Human Rights Act 1998. Whilst this code does not affect the application of those rules, obtaining appropriate authorisations should help ensure the admissibility of evidence derived from CHIS.

8.6 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the Criminal Procedure and Investigations Act 1996 and these considerations will apply to any material acquired through use or conduct of a CHIS that is used in evidence. When information obtained through use or conduct of a CHIS is used evidentially, the public authority should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

8.7 Where material acquired through use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In the case of the law enforcement agencies, product obtained by a CHIS is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996. Particular attention is drawn to the requirements of the code of practice issued under this Act, which requires that the investigator retain all material obtained in an investigation which may be relevant to the investigation.

8.8 With regard to the service police forces (the Royal Navy Police, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the Criminal Procedure and Investigations Act 1996 (Code of Practice) (Armed Forces) Order 2008, which requires that the investigator retain all material obtained in a service investigation which may be relevant to the investigation.

Reviewing authorisations

8.9 Regular reviews of authorisations should be undertaken by the authorising officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS, the information obtained from the CHIS and, if appropriate to the authorising officer's remit, the reasons why executive action is not possible at this stage. The results of a review should be retained for at least three years (see chapter 7 above). Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or the use of a CHIS may provide access to particularly sensitive information. At the point the public authority is considering applying for an authorisation, they must have regard to

[17] whether these proceedings are brought by the public authority that obtained the authorisation or by another public authority (subject to handling arrangements agreed between the authorities)

[18] and section 76 of the Police & Criminal Evidence (Northern Ireland) Order 1989

whether the level of protection to be applied in relation to information obtained under the authorisation is higher because of the particular sensitivity of that information.

8.10 In each case, unless specified by the Secretary of State or Investigatory Powers Commissioner, 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, but should not prevent reviews being conducted in response to changing circumstances. It is good practice to have independent internal review of long term authorisations to ensure alignment with the organisational priorities of the authority.

8.11 In the event that there are any significant and substantive changes to the nature of the operation during the currency of the authorisation, the public authority should consider whether it is necessary to apply for a new authorisation.

Handling material

8.12 Paragraphs 8.16 to 8.21 of this code provide guidance as to the safeguards which govern the dissemination, copying, storage and destruction of material obtained through use or conduct of a CHIS. Each public authority must ensure that there are internal arrangements in force for securing that the requirements of these safeguards are satisfied in relation to such material. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

8.13 The heads of the intelligence services are also under a duty to ensure that arrangements are in force to secure: (i) that no information is obtained except so far as necessary for the proper discharge of their functions; and (ii) that no information is disclosed except so far as is necessary for those functions, for the purpose of any criminal proceedings, and, in the case of SIS and the Security Service, for the other purposes specified.

8.14 Public authorities' internal arrangements should be made available to the Investigatory Powers Commissioner or inspector. The arrangements should ensure that the disclosure, copying and retention of material obtained through use or conduct of a CHIS is limited to the minimum necessary for the authorised purposes. Breaches of these handling arrangements should be reported to the Commissioner or inspector. Where the breach also contravenes data protection requirements, notification of the Information Commissioner may also be necessary.

8.15 There is nothing in the 2000 Act which prevents material obtained through use or conduct of a CHIS from being used to further other investigations where it becomes relevant and in accordance with the safeguards in this chapter.

Dissemination of information

8.16 Material acquired through use or conduct of a CHIS may need to be disseminated both within and between public authorities, as well as to consumers of intelligence

(which includes oversight bodies and the Secretary of State for example), where necessary in order for action to be taken on it. Material which tends to indicate the presence, activity or identity of a specific CHIS should be classified and handled as highly sensitive material. The number of persons to whom such material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out at 8.4 above. This obligation applies equally to disclosure to additional persons within a public authority, and to disclosure outside an agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle in accordance with section 29(4A), (4B) and (5) (c) of RIPA: material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the material to carry out those duties. In the same way, only so much of the material may be disclosed as the recipient needs. For example, if a summary of the material will suffice, no more than that should be disclosed. See also the Prosecution Disclosure Manual.

8.17 The obligations should apply not just to the original public authority, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the original public authority's permission before disclosing the material further. In others, explicit safeguards should be applied to secondary recipients. The above is not intended to affect arrangements for sharing actionable intelligence in accordance with the statutory functions and procedures of public authorities.

Copying

8.18 Material obtained through use or conduct of a CHIS may only be copied to the extent necessary for the authorised purpose. Copies include not only direct copies of the whole of the material, but also extracts and summaries and any other records which contain material obtained through use or conduct of a CHIS.

Storage

8.19 Material obtained through use or conduct of a CHIS and all copies, extracts and summaries which contain such material, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the appropriate level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

8.20 In particular, each public authority must apply the following protective security measures:

- Physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- An appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

8.21 Material obtained through use or conduct of a CHIS, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purposes set out at 8.4 above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.[19]

Protection of the identity of a CHIS

8.22 People who take on the role of a CHIS may place themselves at considerable risk, while their continued co-operation is of great importance to the effectiveness of investigation and law enforcement work. All organisations have a responsibility to protect the identity of individuals working as CHIS, and others who may be affected by the disclosure of the CHIS's identity. Organisations using CHIS should attempt to protect the identities of CHIS by all reasonable and lawful means possible and where appropriate by neither confirming nor denying the existence or identity of the CHIS.

8.23 There are well-established legal procedures under public interest immunity or closed material procedures that can be applied when seeking to protect the identity of a CHIS from disclosure in such circumstances. These procedures should normally be considered in any circumstances where disclosure of the identity of a CHIS or material obtained by a CHIS is likely to lead to heightened risk to them or others.

8.24 It will always be for the party claiming reliance on these procedures to clearly articulate the potential damage which would arise were there to be a departure from them, and it should be considered on a case by case basis. It is then for the Court to balance the public interest in the disclosure of the information against the public interest in protecting it.

8.25 In all cases it should be borne in mind that the risk to the CHIS may not disappear or decline with time. The CHIS may have been involved in numerous operations either before or since the specific case where their identity is being considered. Exposing their identity, even long after their deployment has concluded, may cause risk not only to them but may cause risk to other individuals associated with the role they performed or be harmful to the future sustainability of the CHIS tactic. Such an approach may also be appropriate in circumstances where the CHIS themselves have disclosed their identity, as official confirmation has the potential to lead to the adverse impacts described above.

Confidential or privileged material

8.26 Particular care should be taken in cases where the subject of any intrusion might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege,

[19] For example, by taking reasonable steps to make the data unavailable or inaccessible to authorised persons. No further steps are required, such as physical destruction of hardware.

confidential personal information, confidential constituent information or confidential journalistic material. So, for example, extra care should be taken where, through the use or conduct of a CHIS, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of Parliament and an individual or group of constituents relating to private constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved. References to a Member of Parliament include references to Members of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

8.27 Annex A of this code lists the authorising officer for each public authority, permitted to authorise the use or conduct of a CHIS, in circumstances where knowledge of privileged or confidential information may be acquired. The authorisation levels are set at a more senior level than that required for other CHIS activity, reflecting the sensitive nature of such information.

8.28 In cases where, through the use or conduct of a CHIS, it is intended to obtain material subject to legal privilege, the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 ("the 2010 Legal Privilege Order") applies. The 2010 Legal Privilege Order provides that authorisation of CHIS in these circumstances is subject to an enhanced authorisation process, requiring prior notification to and approval from the Secretary of State or Judicial Commissioner as applicable. Paragraphs8.54 to 8.59 below provide further detail on authorisations involving legally privileged material.

8.29 There may be circumstances when a 'relevant source', as described in the 2013 Relevant Sources Order (see paragraph 2.4 above), will have access to legally privileged or confidential information. In such circumstances, the authorisation processes set out in the 2010 Legal Privilege Order, where applicable, and the 2013 Relevant Sources Order should be adhered to.

Confidential personal information and confidential constituent information

8.30 Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above 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 any legal obligation of confidentiality. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

8.31 Spiritual counselling is conversation between an individual and a Minister of Religion acting in his or her official capacity, and where the individual being counselled is seeking, or the Minister is imparting, forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

8.32 Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency business. Again, such 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 confidentiality contained in existing legislation.

8.33 Where the intention is to acquire confidential personal or constituent information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered by the authorising officer in accordance with the safeguards in this chapter. If the information is exchanged with the intention of furthering a criminal purpose, for example, if purported spiritual counselling involves incitement to murder or to acts of terrorism, then the information will not be considered confidential for the purposes of this code. If the acquisition of confidential personal or constituent information is likely but not intended, any possible mitigation steps should be considered by the authorising officer and, if none is available, consideration should be given to whether special handling arrangements are required within the relevant public authority.

8.34 Material which has been identified as confidential personal or constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there should be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised purposes set out at 8.4 above.

8.35 Where confidential personal or constituent information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser to the relevant public authority before any further dissemination of the material takes place.

8.36 Any case where confidential personal or constituent information is retained, other than for the purpose of destruction, should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and any material which has been retained should be made available to the Investigatory Powers Commissioner on request so that the Investigatory Powers Commissioner can consider whether the correct procedures and considerations have been applied.

Applications to acquire material relating to confidential journalistic material and journalists sources

8.37 There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.

8.38 For the purpose of this code, confidential journalistic material is:

- In the case of material contained in a communication, journalistic material which the sender of the communication
  - Holds in confidence, or

- Intends the recipient, or intended recipient, of the communication to hold in confidence;
- In any other case, journalistic material which a person holds in confidence

8.39 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.

8.40 A person holds material in confidence if they hold the material subject to an express or implied undertaking to hold it in confidence, or they hold the material subject to a restriction on disclosure or an obligation of secrecy contained in an enactment. Confidentiality can continue to attach to confidential journalistic material when it is sent to or held by a person who is neither the journalist nor the source (for example, a news editor who has been sent some notes by a journalist).

8.41 When a public authority applies for an authorisation where the purpose, or one of the purposes, of the authorisation is to authorise the acquisition of material that the authority believes will be confidential journalistic material, the application for an authorisation must contain a statement that the purpose is to acquire material which the public authority believes will contain confidential journalistic material. The person to whom the application is made may issue the authorisation only if they consider that appropriate safeguards relating to the handling, retention use and disclosure of the material are in place.

8.42 A source of journalistic information is an individual who provides material intending the recipient to use it for the purpose of journalism or knowing that it is likely to be so used. Any reference to sources in this code should be understood to include any person acting as an intermediary between a journalist and a source.

8.43 When a public authority applies for an authorisation where the purpose, or one of the purposes is to identify or confirm a source of journalistic information, the application must contain a statement confirming that this is the purpose (or one of the purposes) for the application. The person to whom the application is made may issue the authorisation only if they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place.

8.44 An assessment of whether someone is a journalist (for the purpose of this code) should be made on all the facts and circumstances available at the time. Consideration should be given, in particular, to the frequency of the individual's relevant activities, the level of personal rigour they seek to apply to their work, the type of information that they collect, the means by which they disseminate that information and whether they receive remuneration for their work. This approach will take into account the purpose of the safeguards in this code, which is to protect the proper exercise of free speech, and reflect the role that journalists play in protecting the public interest. The fact that a person uses social media tools to communicate does not, in itself, indicate that that person is a journalist or that he or she is likely to be holding confidential journalistic material.

8.45 The acquisition of material through use or conduct of a CHIS will be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of

the ECHR only if the conduct being authorised is necessary, proportionate and in accordance with law.

8.46 Where material is created or acquired with the intention of furthering a criminal purpose, the material is not to be regarded as having been created or acquired for the purpose of journalism. For example, if a terrorist organisation is creating videos for the promotion or glorification of terrorism according to the UK legal standard, the material cannot be regarded as journalistic material for the purposes of this code and will not attract the safeguards set out in this code. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material.

8.47 Where confidential journalistic material, or that which identifies the source of journalistic information, is retained and disseminated to an outside body, reasonable steps should be taken to mark the disseminated information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of such information, advice should be sought from a legal adviser to the relevant public authority before any further dissemination of the content takes place.

8.48 Where confidential journalistic material, or that which identifies a source of journalistic information, has been obtained or retained, other than for the purposes of destruction, the matter should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable.

Matters subject to Legal Privilege - Introduction

8.49 Section 98 of the 1997 Act defines those matters that are subject to legal privilege.[20] In Scotland, the law relating to legal privilege rests on common law principles. In general, communications between professional legal advisers and their clients will be subject to legal privilege unless they are intended for the purposes of furthering a criminal act. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to. These definitions should be used to determine how to classify material obtained through use or conduct of a CHIS authorised under the 2000 Act. As discussed in further detail below, special safeguards apply to matters subject to legal privilege.

8.50 As defined, legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by a member of the legal profession, such as advocates, barristers, solicitors or Chartered Legal Executives.

[20] Also see definition in Paragraph 2 of the 2010 Legal Privilege Order for matters to which the Order applies.

8.51 For the purposes of this code, any communication or items held between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the communication or item does not form part of a professional consultation of the lawyer, or there is clear evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the material is subject to legal privilege or over whether material is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser to the relevant public authority.

8.52 The acquisition of matters subject to legal privilege is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR, as well as engaging Article 8. The acquisition of matters subject to legal privilege (whether deliberate or otherwise) is therefore subject to additional safeguards. These safeguards provide for three different circumstances where legally privileged items will or may be obtained. They are:

- where privileged material is intentionally sought;
- where privileged material is likely to be obtained; and
- where the purpose or one of the purposes is to obtain items that, if they were not made or held with the intention of furthering a criminal purpose, would be subject to privilege.

Further guidance is set out in paragraphs 8.54 to 8.61 below as to what should be done in each of those cases.

8.53 Where there is a renewal application in respect of a warrant or authorisation which has resulted in the obtaining of legally privileged items, that fact should be highlighted in the renewal application.

Authorisations for the use or conduct of a CHIS intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege

8.54 If a public authority seeks to grant or renew an authorisation for the use or conduct of a CHIS, in circumstances where it is intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the 2010 Legal Privilege Order will apply. The 2010 Legal Privilege Order creates an enhanced regime of prior notification and approval for such authorisations, providing that before an authorising officer grants or renews an authorisation to which the Order applies, they must give notice to and seek approval from the relevant "approving officer". The relevant approving officer will be the Secretary of State in the case of a member of the intelligence services, an official of the Ministry of Defence, or an individual holding an office, rank or position in Her Majesty's Prison Service or the Northern Ireland Prison Service. In all other cases, the relevant approving officer will be a Judicial Commissioner.

8.55 The approving officer must be satisfied that the authorisation is necessary on grounds that it is in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom (see paragraph 6 of the 2010 Legal Privilege Order). The authorising officer

is prohibited from granting or renewing an authorisation, to which the 2010 Legal Privilege Order applies, until they have received confirmation in writing that the approving officer has approved the application. If the approving officer does not approve the application, the authorising officer may still grant an authorisation in respect of the use or conduct of the CHIS in question, but may not authorise the use or conduct of the CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege.

8.56 Where a public authority is seeking an authorisation in these circumstances, the application for an authorisation must contain a statement that the purpose, or one of the purposes, of the authorisation is to obtain legally privileged material (in addition to the other notification requirements provided for in paragraph 5 of the 2010 Legal Privilege Order). An authorisation for these purposes should only be sought where there are exceptional and compelling circumstances that make the authorisation necessary, and the approving officer approves that decision. Circumstances which can be regarded as "exceptional and compelling" will only arise in a very restricted range of cases, where there is a threat to life or limb or in the interests of national security. The exceptional and compelling test can only be met when the public interest in obtaining the information sought outweighs the public interest in maintaining the confidentiality of legally privileged material, and when there are no other reasonable means of obtaining the required information. The authorised use or conduct of a CHIS must be reasonably regarded as likely to yield the intelligence necessary to counter the threat.

Example: A public authority may need to deliberately target legally privileged communications where the legal consultation might yield intelligence that could prevent harm to a potential victim or victims, in addition to the privileged material. For example, if they have intelligence to suggest that an individual is about to conduct a terrorist attack and the consultation may reveal information that could assist in averting the attack (e.g. by revealing details about the location and movements of the individual) then they might want to target the legally privileged communications.

8.57 Further, in considering any such application, the approving officer must be satisfied that the proposed use or conduct of a CHIS is proportionate to what is sought to be achieved and must have regard to the public interest in the confidentiality of items subject to privilege. They will wish to consider carefully whether the activity or threat being investigated is of a sufficiently serious nature to override the public interest in preserving the confidentiality of privileged communications, and the likelihood that the information sought will have a positive impact on the investigation.

8.58 The approving officer will take into account both the public interest in preserving the confidentiality of those particular items and the broader public interest in maintaining the confidentiality of items subject to legal privilege more generally. In addition to considering that there are exceptional and compelling circumstances that make it necessary to grant the authorisation (as detailed above), the approving officer must be satisfied that there are appropriate arrangements in place for the handling, retention, use and destruction of privileged items. In such circumstances, the approving officer will be able to impose additional requirements such as regular reporting arrangements, so as to keep the authorisation under review more effectively.

8.59 The duration for which an authorisation may be granted is reduced where the 2010 Legal Privilege Order is applicable. The usual 12 month duration is reduced to six

months in the case of an intelligence service authorisation, and three months for authorisation by any other public authority.

Authorisations for the use or conduct of a CHIS likely to obtain, provide access to or disclose knowledge of matters subject to legal privilege

8.60 If the use or conduct is not intended to result in the acquisition of knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should include, in addition to the reasons why the use or conduct is considered necessary, an assessment of how likely it is that information which is subject to legal privilege will be obtained. The public authority should also confirm that any inadvertently obtained material that is subject to legal privilege will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the material that is subject to legal privilege. In cases where the use or conduct of a CHIS is likely to result in the acquisition of knowledge of matters subject to legal privilege, the activity must be authorised at a more senior level within each public authority. Annex A to this code lists the enhanced authorisation levels relevant to these circumstances.

Authorisations for the use or conduct of a CHIS intended to result in the acquisition of knowledge of matters that would be subject to legal privilege if they were not created or held with the intention of furthering a criminal purpose

8.61 Where an application for an authorisation is made where the purpose or one of the purposes is to obtain items that, if they were not created or held with the intention of furthering a criminal purpose, would be subject to privilege and where the public authority considers that the items are likely to be created or held to further a criminal purpose, the application must include a statement to that effect and the reasons for believing that the items are likely to be created or held to further a criminal purpose. This includes applications to which the 2010 Legal Privilege Order would otherwise apply (see 2(2)(b) of the Order). For example, if the public authority had reliable intelligence that a criminal fugitive was seeking advice from a lawyer in order to obtain a false alibi or to assist them in evading arrest, then this may provide grounds for an assessment that the communications with the lawyer will not be privileged, notwithstanding the fugitive appeared to be seeking advice from a lawyer in a professional capacity, and this information should be set out in the application. The requirement to ensure the case for an authorisation is presented in the application in a fair and balanced way, including information which weakens the case for the warrant or authorisation (as set out in paragraph 5.14) applies in these circumstances as it does elsewhere. For example, information which may undermine the assessment that material is likely to be created or held to further a criminal purpose must also be included in the application to ensure the authorising officer can make an informed assessment about the nature of the material. The authorisation can only be approved where the authorising officer considers that the items are likely to be created or held with the intention of furthering a criminal purpose.

Unintentional obtaining of knowledge of matters subject to legal privilege by a CHIS

8.62 Public authorities should make every effort to avoid their CHIS unintentionally obtaining, providing access to or disclosing knowledge of matters subject to legal privilege. If a public authority assesses that a CHIS may be exposed to such knowledge unintentionally, the public authority should task the CHIS in such a way that this possibility is reduced as far as possible.

8.63 The reactive nature of the work of a CHIS, and the need for a CHIS to maintain cover, may make it necessary for a CHIS to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct, and may lead them to be exposed to matters subject to legal privilege. Such incidental conduct is regarded as properly authorised by virtue of sections 26(7)(a), 27 and 29(4) of the 2000 Act, even though it was not specified in the initial authorisation. This is likely to occur only in exceptional circumstances, such as where the obtaining of such knowledge is necessary to protect life and limb, including in relation to the CHIS, or national security, in circumstances that were not envisaged at the time the authorisation was granted.

8.64 When debriefing the CHIS, the public authority should make every effort to ensure that any knowledge of matters subject to legal privilege which the CHIS may have obtained is not disclosed to the public authority, unless there are exceptional and compelling circumstances that make such disclosure necessary. If, despite these steps, knowledge of matters subject to legal privilege is unintentionally disclosed to the public authority, the public authority in question should ensure that it is not used in law enforcement investigations or criminal prosecutions. Any unintentional obtaining of knowledge of matters subject to legal privilege by a public authority, together with a description of all steps taken in relation to that material, should be drawn to the attention of the Investigatory Powers Commissioner or inspectors supporting the work of the Commissioner during the next inspection (at which the material should be made available if requested).

8.65 If it becomes apparent that it will be necessary for the CHIS to continue to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the initial authorisation should be replaced by an authorisation that has been subject to the prior approval procedure, set out in the 2010 Legal Privilege Order and in paragraphs 8.54 to 8.59 above, at the earliest reasonable opportunity. This is because it is now intended to obtain LPP material, so the nature of the operation has changed and the enhanced safeguards are applicable.

Lawyers' material

8.66 Where a lawyer, acting in this professional capacity, is the subject of a CHIS operation, it is possible that a substantial proportion of the material which will be acquired will be subject to legal privilege. Therefore, in any case where the subject of a CHIS operation is known to be a lawyer acting in that professional capacity the application should be made on the basis that it is likely or intended to acquire communications or items subject to legal privilege and the provisions in paragraphs 8.54 or 8.60 will apply, as relevant.

8.67 The public authority will need to consider which of the three circumstances apply, when items subject to legal privilege will or may be obtained is relevant, and what processes should therefore be followed. In other words, they will need to consider whether items subject to legal privilege are likely to be obtained; whether items subject to legal privilege are intentionally sought; or whether the purpose or one of the purposes is to obtain material that, if it was not created or held with the intention of furthering a criminal purpose, would be subject to privilege. This paragraph does not prevent an application being made on the grounds that the lawyer is under investigation for serious criminal offences, in which case, the application or notification must be made on the basis that it is likely to acquire items subject to legal privilege and the additional considerations set out at paragraph 8.60 will apply. The provisions of the 2010 Legal Privilege Order will therefore apply where a lawyer is the subject of a CHIS operation and it is intended to acquire material subject to legal privilege.

8.68 Any such case should also be notified to the Investigatory Powers Commissioner during his or her next inspection and any material which has been retained should be made available to the Commissioner on request.

The handling, retention and deletion of material subject to legal privilege

8.69 In addition to safeguards governing the handling and retention of material as provided for in paragraphs 8.12 to 8.20 of this code, authorised persons who analyse material obtained by use or conduct of a CHIS should be alert to any communications or items which may be subject to legal privilege.

8.70 A legal adviser to the public authority must be consulted when it is believed that material which attracts privilege is obtained. The legal adviser is responsible for determining that material is privileged, rather than an officer who is involved in an investigation. In cases where there is doubt as to whether material is privileged or not, the public authority may seek advice from the Investigatory Powers Commissioner. Where it is discovered that privileged material has been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain it for one or more of the authorised purposes. If not, the material should not be retained, other than for the purpose of its destruction or in accordance with other statutory requirements.

8.71 Material which has been identified as legally privileged (and is being retained for purposes other than its destruction) should be clearly marked as subject to legal privilege and the Investigatory Powers Commissioner must be notified of the retention of the items as soon as reasonably practicable. Paragraph 8.72 to 8.75 below provide more detail on reporting privileged items to the Commissioner. Such material should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes. Privileged items must be securely destroyed when their retention is no longer needed for those purposes. If such material is retained, there must be adequate information management systems in place to ensure that continued retention, for purposes other than their destruction, remains necessary and proportionate for the authorised statutory purposes.

Reporting to the Commissioner

8.72 In those cases where items identified by a legal adviser to the public authority as being legally privileged have been acquired, the matter should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable.

8.73 The Commissioner must order the destruction of the item or impose conditions on its use or retention unless the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. Even if retention is necessary and the public interest in its retention outweighs the public interest in the confidentiality of items subject to legal privilege, the Commissioner may still impose conditions as he considers necessary to protect the public interest in the confidentiality of items subject to privilege.

8.74 It may be the case, in some circumstances, that privileged items can be retained when their retention does not outweigh the public interest in the confidentiality of items subject to privilege. This includes, for example, where it is not possible to separate privileged items from those that are not privileged and of intelligence value and where the retention is necessary and proportionate for one of more of the authorised purposes or in accordance with statutory requirements. In these circumstances, the Commissioner must impose conditions on the use or retention of the item.

8.75 The Investigatory Powers Commissioner will make an assessment of whether the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege, and of whether retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. If both of those conditions are met, then the Commissioner may impose conditions as to the use or retention of the items, but the Commissioner is not obliged to do so. If those conditions are not met, the Commissioner must direct that the item is destroyed, or must impose one or more conditions as to the use or retention of the items. The Commissioner must have regard to any representations made by the public authority about the proposed retention of privileged items or conditions that may be imposed.

Dissemination

8.76 In the course of an investigation, a public authority must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained, except in urgent circumstances. Where there is an urgent need to take action and it is not reasonably practicable to inform the Investigatory Powers Commissioner that the material has been obtained before taking action, the public authority may take action before informing the Investigatory Powers Commissioner. In such cases, the public authority should, wherever possible consult a legal adviser. A public authority must not disseminate privileged items if doing so would be contrary to a condition imposed by the Investigatory Powers Commissioner in relation to those items.

8.77 The dissemination of legally privileged material to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available,

or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard, civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any legally privileged material, held by the relevant public authority, with any possible connection to the proceedings. In respect of civil proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on legally privileged material in order to gain a litigation advantage over another party in legal proceedings.

8.78 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that lawyers or other officials with conduct of legal proceedings should not see legally privileged material relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such material could yield a litigation advantage, the direction of the Court must be sought.

9 Senior responsible officers and oversight by the Commissioner

The senior responsible officer

9.1 Within every relevant public authority a senior responsible officer[21] must be appointed with responsibility for:

- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with this code;
- oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner's inspectors when they conduct their inspections, where applicable;
- where necessary, oversight of the implementation of post-inspection action plans approved by the Investigatory Powers Commissioner; and
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

Oversight by the Commissioner

9.2 The Investigatory Powers Act provides for an Investigatory Powers Commissioner ("the Commissioner"), whose remit includes providing comprehensive oversight of the use of the powers to which this code applies, and adherence to the practices and processes described in it. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of Her Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts, qualified to assist the Commissioner in his or her work. The Commissioner will also be advised by the 'Technology Advisory Panel'.

9.3 The Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Investigatory Powers Commissioner may undertake these inspections, as far as they relate to the Investigatory Powers Commissioner's statutory functions, entirely on his or her own initiative or the Commissioner may be asked to investigate a specific issue by the Prime Minister. Section 236 of the 2016 Act also provides for the Intelligence and Security Committee of Parliament to refer a matter to the Investigatory Powers Commissioner with a view to carrying out an investigation, inspection or audit.

[21] Within local authorities, the senior responsible officer should be a member of the corporate leadership team

9.4 The Commissioner will have unfettered access to all locations, documentation and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the Investigatory Powers Commissioner must not act in a way which is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (section 229(6) of the 2016 Act). A Commissioner must in particular not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, nor unduly impede the operational effectiveness of an intelligence service, a police force, a government department, or Her Majesty's Forces (see section 229(7) of the 2016 Act).

9.5 All relevant persons using investigatory powers must provide all necessary assistance to the Commissioner and anyone who is acting on behalf of the Commissioner. Here, a relevant person includes, amongst others, any person who holds, or has held, an office, rank or position within a public authority (see section 235(7) of the 2016 Act).

9.6 Anyone, including anyone working for a public authority, who has concerns about the way that investigatory powers are being used may report their concerns to the Commissioner. In particular, any person who exercises the powers described in the Act or this code must, in accordance with the procedure set out in chapter 7 of this code, report to the Commissioner any relevant error of which it is aware. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority.

9.7 Should the Commissioner uncover, or be made aware of, what they consider to be a serious error relating to a person who has been subject to an investigatory power then, if it is in the public interest to do so, the Commissioner is under a duty to inform the person affected. Further information on errors can be found in chapter 8 of this code. The public authority who has made the error will be able to make representations to the Commissioner before the Commissioner decides it is in the public interest for the person to be informed. Section 231(6) of the 2016 Act states that the Commissioner must also inform the affected person of their right to apply to the Investigatory Powers Tribunal (see chapter 10 of this code for more information on how this can be done).

9.8 The Commissioner must report annually on the findings of their audits, inspections and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Only the Prime Minister will be able to make redactions to the Commissioner's report.

9.9 The Commissioner may also report, at any time, on any of their investigations and findings as they see fit. Public authorities may seek general advice from the Commissioner on any issue which falls within the Commissioner's statutory remit. The Commissioner may also produce whatever guidance they deem appropriate for public authorities on how to apply and use investigatory powers.

9.10 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: [insert website]

9.11 Oversight of public authorities in Northern Ireland, whose powers have been conferred by Order of the Northern Ireland Assembly, is a devolved matter.

10 Complaints

10.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against public authority use of investigatory powers, including those covered by this code, and is the only appropriate tribunal for human rights claims against the intelligence services. Any complaints about the use of powers as described in this code should be directed to the IPT.

10.2 The IPT is entirely independent from Her Majesty's Government and the public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for these purposes includes an organisation, an association, or combination of persons (see section 81(1) of RIPA 2000), as well as an individual.

10.3 This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com. Alternatively information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

10.4 If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

11 ANNEX A

Enhanced authorisation levels when knowledge of privileged or confidential information may be acquired or when a vulnerable individual or juvenile is to be used as a source.

Relevant Public Authority	Authorisation level for when confidential information is likely to be acquired	Authorisation level for when a vulnerable individual or juvenile is to be used as a source
Police Forces Any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London)	Chief Constable	Assistant Chief Constable
Police Service of Scotland	Chief Constable	Assistant Chief Constable
Metropolitan Police Force	Assistant Commissioner	Commander
City of London Police Force	Commissioner	Commander
Police Service of Northern Ireland	Deputy Chief Constable	Assistant Chief Constable
Ministry of Defence Police	Chief Constable	Asssitant Chief Constable
Royal Navy Police	Provost Marshal	Provost Marshal
Royal Military Police	Provost Marshal	Provost Marshal
Royal Air Force Police	Provost Marshal	Provost Marshal
National Crime Agency	Deputy Director General	Deputy Director
Serious Fraud Office	A member of the Senior Civil Service, or Head of Domain	A member of the Senior Civil Service, or Head of Domain
The Intelligence Services	Deputy Director General	Deputy Director General

The Security Service		
The Secret Intelligence Service	A Director of the Secret Intelligence Service	A member of the Intelligence Service not below the equivalent rank to that of a Grade 5 in the Home Civil Service
The Government Communications Headquarters (GCHQ)	A Director of GCHQ	A Director of GCHQ
HM Forces		
The Royal Navy	Rear Admiral	Rear Admiral
The Army	Major General	Major General
The Royal Air Force	Air-Vice Marshal	Air-Vice Marshal
The Commissioners for HM Revenue and Customs	Director Investigation, or Regional Heads of Investigation	Grade 7 (Intel)
Department for the Environment, Food and Rural Affairs		
DEFRA Investigation Services	Head of DEFRA Investigation Service	Head of DEFRA Investigation Service
Marine and Fisheries Agency	Head of Better Regulation	----------
Centre for Environment, Fisheries and Aquacutlure Science	Head of Better Regulation	Head of Better Regulation
Department of Health		
The Medicines and Healthcare Products Regulatory Agency	Chief Executive	Head of Division for Inspection and Enforcement
Home Office	Senior Civil Servant pay band 1 with responsibility for criminal investigations in relation to immigration and border security	Grade 6 with responsibility for criminal investigations in relation to immigration and border security

Ministry of Justice	Chief Executive of the National Offender Management Service	A member of the senior Civil Service in the National Offender Management Service not below the equivalent rank of a Grade 5 in the Home Civil Service
Northern Ireland Office		
Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service	Director or Deputy Director Operations in the Northern Ireland Prison Service
Department of Business, Innovation and Skills	The Director of Legal Services A	The Director of Legal Services A
The Welsh Assembly Government		
	Head of Department for Health and Social Services Head of Rural Payments Division Regional Director or equivalent grade n the Care and Social Service Inspectorate for Wales	Head of Department for Health and Social Services Head of Rural Payments Division Regional Director or equivalent grade n the Care and Social Service Inspectorate for Wales
Any county council or district council in England, a London borough, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, and any ciounty council or borough council in Wales	Head of Paid Service, or (in his absence) The person acting as the Head of Paid Service	Head of Paid Service, or (in his absence) The person acting as the Head of Paid Service
Environment Agency	Chief Executive of the Environment Agency	Executive Manager in the Environment Agency
The Prudential Regulation Authority	Chief Executive of the Prudential Regulation Authority	Chief Executive of the Prudential Regulation Authority
Competition and Markets Authority	Chair of the Competition and Markets Authority	Chair of the Competition and Markets Authority
Financial Conduct Authority	Chairman of the Financial Conduct Authroity	Chairman of the Financial Conduct Authority

Food Standards Agency	Head of Group, or Deputy Chief Executive, or Chief Executive of the Food Standards Agency	Head of Group, or Deputy Chief Executive, or Chief Executive of the Food Standards Agency
The Gambling Commission	----------	Chief Executive
Health and Safety Executive	Director of Field Operations, or Director of Hazardous Installations Directorate	Director of Field Operations, or Director of Hazardous Installations Directorate

12 ANNEX B

Authorisation levels for the enhanced arrangements set out in the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
A police force maintained under section 2 of the Police Act 1996	**Relevant Source Authorisation** Assistant Chief Constable **Long Term Authorisation** Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The City of London Police Force	**Relevant Source Authorisation** Commander **Long Term Authorisation** Commissioner	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The Metropolitan Police Force	**Relevant Source Authorisation** Commander **Long Term Authorisation** Assistant Commissioner	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The Police Service of Northern Ireland	**Relevant Source Authorisation** Assistant Chief Constable **Long Term Authorisation** Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The Police Service of Scotland	**Relevant Source Authorisation** Assistant Chief Constable **Long Term Authorisation** Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)

The Ministry of Defence Police	**Relevant Source Authorisation** Assistant Chief Constable **Long Term Authorisation** Chief Constable	Superintendent	Paragraphs (a), (b) and (c)
The Royal Navy Police	**Relevant Source Authorisation** Commander **Long Term Authorisation** Provost Marshal (Navy)	Lieutenant Commander	Paragraphs (a), (b) and (c)
The Royal Military Police	**Relevant Source Authorisation** Colonel **Long Term Authorisation** Provost Marshal (Army)	Major	Paragraphs (a), (b) and (c)
The Royal Air Force Police	**Relevant Source Authorisation** Wing Commander **Long Term Authorisation** Provost Marshal (Royal Air Force)	Squadron Leader	Paragraphs (a), (b) and (c)
The British Transport Police	**Relevant Source Authorisation** Assistant Chief Constable **Long Term Authorisation** Chief Constable	Superintendent	Paragraphs (a), (b), (c), (d) and (e)
The National Crime Agency	**Relevant Source Authorisation** Deputy Director **Long Term Authorisation** Deputy Director General	Grade 2 Senior Manager	Paragraph (b)
Her Majesty's Revenue and Customs	**Relevant Source Authorisation** Assistant Director **Long Term Authorisation** Director Criminal Investigation	Senior Officer	Paragraphs (a), (b), (d), (e) and (f)
The Home Office	**Relevant Source Authorisation**	Grade 6 with responsibility for	Paragraphs (b), (c) and (d)"

Senior Civil Service pay band 1 with responsibility for criminal investigations in relation to immigration and border security	criminal investigations in relation to immigration and border security
Long Term Authorisation	
Director General with responsibility for criminal investigations in relation to immigration and border security	