Covert Human Intelligence Sources

Draft Revised Code of Practice

December 2021

This publication is available at [www.gov.uk/government/publications]

Any enquiries regarding this publication should be sent to us at RIPA@homeoffice.gov.uk.

Contents

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 Section 29 of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"), and on the use of Criminal Conduct Authorisations under Section 29B of the 2000 Act. The Code also provides guidance on the handling of any information obtained by authorisation 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 exercise and performance of the powers and duties in Part II of the 2000 Act.

1.3 In accordance with Section 72 of the 2000 Act, any public authority exercising or performing power and duties under Part II to which this Code refers is under a duty to have regard to the provisions of the Code. For the avoidance of doubt, the duty to have regard to the Code exists regardless of any contrary content of a public authority's internal advice or guidance.

1.4 This Code replaces the previous Covert Human Intelligence Sources Code of Practice (dated August 2018). This version of the Code reflects changes to the authorisation of CHIS made by the CHIS (Criminal Conduct) Act 2021.

1.5 This Code 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 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 CHIS.

1.6 The 2000 Act provides that all codes of practice issued under the Act are admissible as evidence in criminal and civil proceedings. Any court or tribunal considering any such proceedings, the Investigatory Powers Tribunal, or the Investigatory Powers Commissioner responsible for overseeing the relevant powers and functions may take the provisions of this Code 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.

1.7 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.

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

1.8 Part II of the 2000 Act provides for the authorisation of the use or conduct of a CHIS and for the authorisation of criminal conduct in the course of or otherwise in connection with the conduct of a 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.

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 section 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.[1]

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.[2]

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.[3]

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 (here).

Scope of authorisations

2.6 Subject to the procedures outlined in chapter 3 and chapter 5 of this Code, an authorisation may be obtained under Part II of the 2000 Act for the use or conduct of CHIS. Subject to the procedures outlined in chapter 3 and chapter 6 of this Code, an authorisation may also, where appropriate, be obtained by certain public authorities for criminal conduct by or in relation to CHIS.

2.7 The use of a CHIS consists of 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

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

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

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

means of the conduct of a CHIS.[4] 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.[5]

2.9 The criminal conduct that may be authorised under a Criminal Conduct Authorisation is any criminal conduct in the course of, or otherwise in connection with, the conduct of a CHIS. As such, a Criminal Conduct Authorisation will always be linked to a Section 29 authorisation which authorises the conduct of the CHIS to whom the Criminal Conduct Authorisation relates. Guidance specific to Criminal Conduct Authorisations is set out in chapter 6 of this Code.

2.10 Unless otherwise stated, any references in this Code to a "CHIS authorisation" also includes reference to any section 29B Criminal Conduct Authorisation that has been authorised alongside any section 29 authorisation.

2.11 Most Section 29 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.

2.12 A Section 29 authorisation for the conduct and/or the use of a CHIS cannot itself authorise any criminal conduct. All criminal conduct that it is envisaged may form part of the conduct of a CHIS should be authorised by means of a separate but linked Section 29B Criminal Conduct Authorisation.[6]

2.13 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 section 29 authorisations obtained by one or more public authorities. Such authorisations should not conflict.

2.14 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 CHIS authorisation was granted, but which is incidental to authorised conduct. Such conduct is excluded from civil liability as a result of section 27(2) but may still attract criminal liability. However, where it is necessary for a CHIS to engage in criminal conduct which was not envisaged at the time the authorisation was granted, there may be other defences in law available to the CHIS.

---

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

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

[6] There was previously an ability to authorise very limited criminal conduct by or in relation to a covert human intelligence source under section 29 of the 2000 Act, but the Covert Human Intelligence Sources (Criminal Conduct) Act 2021removed this capability. Criminal conduct by a CHIS should now be authorised using a Criminal Conduct Authorisation issued under section 29B of the 2021 Act rather than under section 29.

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

2.15 The availability of a CHIS authorisation does not mean that it is unlawful not to seek or obtain one. 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, or where it is believed an individual is acting in that capacity and it is intended to obtain information from them accordingly. Public authorities must ensure that all CHIS use or conduct that is authorised is:

- necessary on grounds falling within section 29(3);
- proportionate to what is sought to be achieved by that conduct or use; and
- in compliance with relevant Articles of the European Convention on Human Rights, particularly Article 6 and Article 8.

2.16 Unlike directed surveillance, which interferes with Article 8 on the basis that it is likely to result in obtaining information relating to a person's private or family life. CHIS relationships may amount to an interference regardless of whether such private information is obtained. This is on the basis that Article 8 protects the right to establish and develop relationships (both personal and professional). Authorisations for the use or conduct of a CHIS do not relate specifically to private information; covert manipulation of a relationship by a public authority (e.g. where one party has a covert purpose and is acting on behalf of a public authority) may therefore engage Article 8, regardless of whether private information is obtained.

Establishing, maintaining, and using a relationship

2.17 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 that contact.

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 to make a purchase of alcohol.* On the basis that the exchange between a buyer and seller will be simply transactional, it is unlikely a relationship would be formed in these circumstances, and therefore it is unlikely that the juvenile would be considered a CHIS according to the definition in section 26(8) of the 2000 Act. A CHIS authorisation would not therefore be appropriate. *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 if it is likely to result in the obtaining of private information.*

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 and pass back information to the public authority on the shopkeeper's activities. In these circumstances a relationship has*

been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

Legend building

2.18 When a Relevant Source (detailed at paragraph 2.4) is deployed to establish their "legend"/ build up their cover profile, a CHIS authorisation should be considered if the activity will interfere with an individual's Article 8 rights. This will include circumstances where it is not clear to the individual with whom the source establishes or maintains a relationship that the Relevant Source is not who he or she claims to be. Interference with any individual's Article 8 rights may require a CHIS authorisation, irrespective of whether that individual is the subject of a current or future investigation. Where a CHIS 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

2.19 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 who 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

2.20 In many cases involving human sources, the source will not have established or maintained a relationship for a covert purpose. Many sources provide information that they have observed or acquired other than through a relationship. This means that the source is not a CHIS for the purposes of the 2000 Act and no CHIS authorisation 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 is not a CHIS. They are not passing information obtained 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.*

[7] See Chapter 3 of this Code for further guidance on types of source activity to which a CHIS authorisation may or may not apply.

Professional or statutory duty

2.21 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.

2.22 Any such professional or statutory disclosures should not usually 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 obtaining or disclosing such information.

Tasking not involving relationships

2.23 Tasking a person to obtain information covertly may result in a CHIS authorisation 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 2000 Act, for example, a directed surveillance authorisation, may need to be considered where the activity is likely to result in the public authority obtaining information relating to a person's private or family life.*

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 or considering whether it would be appropriate to do so.

> ***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 or 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.

2.26 It is possible that a person may become engaged in the conduct of a CHIS without a public authority inducing, asking, or assisting the person to engage in that conduct. However, a CHIS authorisation should be considered, for example, where a public authority is aware that an individual 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 CHIS authorisations

Authorising Officer

3.1 Responsibility for giving the CHIS authorisation will depend on which public authority is seeking to authorise the CHIS. For the purposes of this Code, the person in a public authority responsible for granting a CHIS authorisation will be referred to as the "Authorising Officer". The relevant public authorities are listed in Schedule 1 of the 2000 Act, as amended by the Covert Human Intelligence Sources (Criminal Conduct) Act 2021. The relevant authorising officers are listed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 CHIS Order").[8]

Necessity and Proportionality – section 29 use or conduct authorisations

3.2 The 2000 Act requires that the person granting a section 29 authorisation believes that the use or conduct to be authorised is necessary on one or more of the statutory grounds listed in section 29(3) of the 2000 Act.

3.3 If the use or conduct is deemed necessary on one or more of the statutory grounds, the person granting the authorisation must also believe that the use or conduct to be authorised is proportionate to what is sought to be achieved by it.

3.4 The degree of intrusiveness of the actions tasked or undertaken by a CHIS will vary from case to case, and therefore proportionality must be assessed on a case-by-case basis. This involves balancing the seriousness of the intrusion into the private or family life of the subject of the operation (and any other person who may be affected) against what is sought to be achieved by the proposed activity in investigative and operational terms.

3.5 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 any activity under investigation may involve serious offences will not alone render the use or conduct of a CHIS proportionate. Similarly, the activity under investigation may involve an offence so minor that any use or conduct 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.

3.6 The following elements of proportionality should therefore be considered:

[8] As amended by the 2013 Relevant Sources Order and the Regulation of Investigatory Powers (Criminal Conduct Authorisations) (Amendment) Order 2021. Note that the original 2010 CHIS Order has subsequently been amended (including by the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 No.2788 and the Regulation of Investigatory Powers (Criminal Conduct Authorisations) (Amendment) Order 2021), so care must be taken to refer to the most up-to-date version.

- 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 private and family life 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.

3.7 The fact that a section 29 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. Public authorities are permitted, for example, to apply for a section 29 authorisation in respect of members or officials of a trade union who are considered to be a legitimate intelligence target where it is necessary for one or more of the statutory purposes and proportionate to what is sought to be achieved.

Necessity and Proportionality – Criminal Conduct Authorisations

3.8 Public authorities must ensure that any criminal conduct to be authorised is:

- necessary on grounds falling within section 29B(5) of the 2000 Act;
- proportionate to what is sought to be achieved by the conduct to be authorised; and
- in compliance with relevant Articles of the European Convention on Human Rights.

3.9 The 2000 Act[9] requires that the person granting a Criminal Conduct Authorisation believes that the criminal conduct to be authorised is necessary on one or more of the statutory grounds listed in section 29B (5) of the 2000 Act[10].

3.10 If the criminal conduct is believed to be necessary on one or more of the relevant grounds, the person granting the authorisation must also believe that the criminal conduct to be authorised is proportionate to what is sought to be achieved by that it.

3.11 The person granting the authorisation must hold a reasonable belief that the authorisation is necessary and proportionate.

---

[9] As amended by the CHIS (Criminal Conduct) Act 2021

[10] A Criminal Conduct Authorisation is necessary on grounds falling within Section 29B if it is necessary—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder; or

(c) in the interests of the economic well-being of the United Kingdom.

3.12 The person granting the authorisation is best placed to assess necessity and any assessment of reasonableness must be by reference to the circumstances which existed at the time of the authorisation.

3.13 The criminal conduct to be authorised will not be proportionate if it is excessive in the overall circumstances of the case. Any criminal conduct authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that the activity under investigation may involve serious offences will not alone render the criminal conduct of a CHIS proportionate. Similarly, the activity under investigation may involve an offence so minor that any criminal conduct by a CHIS would be disproportionate.

3.14 The following elements of proportionality should therefore be considered before granting a Criminal Conduct Authorisation:

- whether what is sought to be achieved by the criminal conduct could reasonably be achieved by other conduct which would not constitute crime;
- whether the criminal conduct to be authorised is part of efforts to prevent or detect more serious criminality;
- whether the potential harm to the public interest from the criminal conduct would be outweighed by the potential benefit to the public interest and that the potential benefit would be proportionate to the criminal conduct in question.

Extent of CHIS authorisations

3.15 A CHIS authorisation may authorise conduct that:

- involves the use or conduct of a CHIS, including criminal conduct by or in relation to that CHIS, as is specified or described in the authorisation;
- is carried out by or in relation to the person to whom the authorisation relates; and
- is carried out for the purposes of, or in connection with, the investigation or operation so described.[11]

3.16 In the above context, it is important that those involved in the use of a CHIS are aware of the extent and limits of the authorisation in question and that the CHIS is made aware of the extent and limits of any conduct authorised (including criminal conduct)..

Collateral Intrusion

3.17 Before granting a CHIS authorisation the Authorising Officer should take into account the risk of any impact on persons who are not the intended subjects of the CHIS activity (collateral intrusion, as opposed to intended intrusion). Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where communications between a member of a relevant legislature and another person on constituency business may be involved (see chapter 8).

3.18 Measures should be taken, wherever practicable, to avoid or minimise the impact on those who are not the intended subjects of the CHIS activity. Where such collateral

[11] See section 29(4) and 29B(6)(c) of the 2000 Act.

intrusion is unavoidable, the authorisation may still be granted 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.

3.19 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 use or conduct of the CHIS.

3.20 Where CHIS activity is deliberately proposed in relation to individuals who are not suspected of direct or culpable involvement in the activity being investigated, the impact on such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such interference should be carefully considered against the necessity and proportionality criteria as described above.

Example 1: *A Relevant Source[12] 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 not the intended subjects of the authorisation. 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 both be the subjects of intended intrusion. The Authorising Officer will also need to consider the proportionality of any collateral intrusion that will arise if there is any impact on individuals who are not the intended subjects of the authorisation.*

Reviewing and renewing authorisations

3.21 The Authorising Officer who grants a CHIS authorisation should, where possible, be responsible for considering subsequent renewals of that authorisation and any related security and welfare issues, where enhanced arrangements under the 2013 Relevant Sources Order apply (see paragraph 2.4 above).

3.22 The Authorising Officer will stipulate the frequency of formal reviews and the controller (see paragraph 6.33 below) should maintain an audit of case work sufficient to ensure that the use or conduct of the CHIS, including criminal conduct by or in relation to 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.

3.23 Where the nature or extent of the impact of an authorisation 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).

[12] As to the meaning of "Relevant Source" see paragraph 2.4 above.

3.24 Where an 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 that interference with the private or family life of such individuals was within the scope of the original authorisation .

Example: *A CHIS 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.*

3.25 Any proposed changes to the nature of the CHIS deployment (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 additional impact or collateral intrusion), before approving or rejecting them with their documented rationale. Any such changes should be highlighted at the next renewal (if applicable).

Local considerations and community impact assessments

3.26 Any person applying for or granting a CHIS authorisation will also need to be aware of any particular sensitivities in the local community where the CHIS is being used 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 deployment of a CHIS (including any criminal conduct) or use of information obtained from that CHIS.

3.27 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

3.28 A single authorisation may combine two or more different authorisations under Part II of the 2000 Act.[13] 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).

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

3.29 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.

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

Operations involving multiple CHIS

3.31 A single CHIS authorisation may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the deployment of several undercover operatives acting as CHISs in situations where the activities to be authorised, the subjects of the operation, the impact of the activity including the interference with private or family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each operative. If a CHIS 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 each Relevant Source to ensure the enhanced authorisation process set out in the 2013 Relevant Sources Order (see paragraph 2.4 above)and Annex B of this Code can be adhered to (see also paragraph 4.16)

3.32 Where there is a Section 29 authorisation in place that itself relates to multiple CHIS, a single Criminal Conduct Authorisation could similarly cover all of those CHIS, provided that the circumstances are such that the CHIS are connected by a single investigation or operation and the criminal conduct to be authorised is the same. If a CHIS authorisation includes more than one CHIS, each CHIS must be clearly identifiable within the documentation.

3.33 Where a Section 29 authorisation ceases to have effect, the related Criminal Conduct Authorisation will cease to have effect in so far as it relates to that Section 29 authorisation (and the CHIS to whom that Section 29 authorisation relates) but will continue to have effect in so far as it relates to any other Section 29 authorisation(s).

Covert surveillance of a CHIS

3.34 It may be necessary to deploy covert surveillance against a CHIS or potential CHIS, other than those acting in the capacity of a Relevant Source, 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 European Convention on Human Rights.

Use of equipment by a CHIS

3.35 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.

3.36 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 CHIS's presence. Authorisation for the use or conduct of the CHIS may be obtained in the usual way.

3.37 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

3.38 The use section 29 authorisations by local authorities in England and Wales is subject to judicial approval. Local authorities do not have the power to grant Criminal Conduct Authorisations.

3.39 The Protection of Freedoms Act 2012 amended the 2000 Act to make the use of section 29 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 section 29 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 or conduct 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. This amendment also means that local authorities are no longer able to grant a section 29 authorisation orally. Further detail on these changes is set out in separate guidance for local authorities and the judiciary, available on the gov.uk website.[14]

3.40 In Northern Ireland the requirement introduced by the Protection of Freedoms Act applies only to local authority use of section 29 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.

3.41 In Scotland, CHIS authorisations are governed by the Regulation of Investigatory Powers (Scotland) Act 2000 and a separate Code of Practice applies.

3.42 Elected members of a local authority should review the authority's use of Part II 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.

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

4 Special considerations for certain authorisations

4.1 The Investigatory Powers Commissioner must be informed within seven working days of a CHIS authorisation of a vulnerable adult or a juvenile source. The Investigatory Powers Commissioner intends to keep such authorisations under close review and will report any relevant findings in his Annual Report.

Vulnerable individuals

4.2 Special safeguards apply to the authorisation of a vulnerable individual as a CHIS. 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 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

4.3 Special safeguards also apply to the authorisation of a juvenile source as a CHIS. A juvenile source is a source who us under 18 years old. In respect of section 29 authorisations, safeguards are set out in the Regulation of Investigatory Powers (Juveniles) Order 2000 ("the Juveniles Order"), and in this Code; in respect of Criminal Conduct Authorisations, safeguards are set out in section 29C of the 2000 Act and this Code, These safeguards recognise that juvenile CHIS are likely to be more vulnerable than adult CHIS due to their age and level of maturity, and that enhanced protections are appropriate to ensure their safety and welfare.

4.4 Juvenile sources should only be authorised to act as a CHIS in exceptional circumstances. The need to safeguard and promote the best interests of the juvenile is a primary consideration in all juvenile CHIS deployments, both when deciding whether to grant the authorisation and during the conduct of any subsequent operation. Each public authority that authorises juvenile CHIS should have its own guidance, policies and procedures in place to safeguard and promote the best interests of a juvenile CHIS. This guidance should be considered before an authorisation is granted.

4.5 In accordance with paragraph 5.8 of this Code, clear separation should be maintained between those responsible for the investigation and those authorising and managing the juvenile CHIS. This is to ensure that the safety and welfare of the juvenile CHIS are always given due consideration.

4.6 On no occasion should a juvenile CHIS who is under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, such authorisations should not be granted unless the special provisions, contained within the Juveniles Order are satisfied. A juvenile CHIS who is aged 16 or 17 years old should only be deployed to gather information against their parents or any person who has parental responsibility for them where careful

consideration has been given to whether the authorisation is justified in light of that fact. In such instances the rationale must be documented by the public authority.

4.7 Authorisations for juvenile CHIS should be granted by those listed in the attached table at Annex A, which sets out enhanced authorisation levels for such purposes. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these provisions, the age test is applied at the time of the grant or renewal of the authorisation.

4.8 Public authorities must ensure that an appropriate adult is present at any meetings with a juvenile CHIS who is under 16 years of age when the meeting takes place. The need for an appropriate adult to be present at meetings where the juvenile CHIS is 16 or 17 years of age when the meeting takes place should be considered on a case-by-case basis following an assessment of the maturity of the juvenile and their ability to give informed consent. The rationale for any decision not to have an appropriate adult present should be documented by the Authorising Officer.

4.9 The appropriate adult should normally be the parent or guardian of the juvenile CHIS, unless they are unavailable or there are specific reasons for excluding them, such as their involvement in the matters being reported upon, or where the CHIS provides a clear reason for their unsuitability. In these circumstances another suitably qualified person should act as appropriate adult, e.g. someone who has personal links to the CHIS or who has professional qualifications that enable them to carry out the role (such as a social worker). The appropriate adult should be independent of the investigatory authority.

4.10 Any deployment of a juvenile CHIS should be subject to the enhanced risk assessment process set out in the Juveniles Order, and the rationale recorded in writing. Where appropriate, external advice should be sought when undertaking the enhanced risk assessment for a juvenile CHIS, for example from someone with relevant professional qualifications such as a social worker or an appropriately trained health professional. Where a juvenile CHIS's parent or guardian will not be informed of the tasking as a result of decisions taken in accordance with paragraphs 4.4, 4.6, 4.8 or 4.9 above, the impact this will have on the juvenile CHIS should be considered as part of the enhanced risk assessment.

Juvenile sources – Criminal Conduct Authorisations

4.11 Additional safeguards apply when a juvenile source is being tasked to participate in criminal conduct. A Criminal Conduct Authorisation can only be granted in relation to a juvenile source in exceptional circumstances. The meaning of exceptional circumstances in this context is set out in section 29C of the 2000 Act. In the context of participation in criminal conduct, such exceptional circumstances will only exist where there is no reasonably foreseeable harm to the juvenile as a result of the authorisation, and where the authorisation is believed to be compatible with the best interests of the juvenile.

4.12 Public authorities must ensure that an appropriate adult is present at all meetings with a juvenile CHIS who is under 16 years of age when the meeting takes place. An appropriate adult must also be present at any meetings where the juvenile CHIS is 16 or 17 years of age when the meeting takes place, unless there are circumstances

which justify the absence of an appropriate adult. In such cases, a record must be kept explaining why there are circumstances that justify the absence of an appropriate adult.

Scotland – section 29 use or conduct authorisations

4.13 Where all the conduct authorised is likely to take place in Scotland, authorisations should be granted under the Regulation of Investigatory Powers (Scotland) Act 2000, 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 2007;
- the authorisation is to be granted or renewed by or authorises conduct by a person holding any office, rank or position with, any such listed 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.

4.14 This Code is extended to Scotland in relation to CHIS 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 the Regulation of Investigatory Powers (Scotland) Act 2000.

Scotland – Criminal Conduct Authorisations

4.15 A Criminal Conduct Authorisation under section 29B(5)(b) of the 2000 Act may not be granted where all or some of the conduct to be authorised is likely to take place in Scotland, unless the authorisation is for a purpose relating to a reserved matter (within the meaning of the Scotland Act 1998).

4.16 Authorisations that are necessary in the interests of national security or the economic well-being of the United Kingdom can still be granted even where all of the conduct to be authorised is likely to take place in Scotland, as these are by definition reserved.

4.17 Authorisations that are necessary for preventing or detecting crime, and where some or all of the activity is likely to take place in Scotland, may only be authorised where the purpose of the authorisation relates to a reserved matter as defined by the Scotland Act 1998.

4.18 There may be circumstances where CHIS operations are carried out not for the purpose of preventing or detecting crime or preventing disorder generally, but for the purpose of preventing or detecting a particular category of crime as part of a special statutory regime governing a particular (reserved) area. The crime prevention activities are not a separate matter but an integral part of the application of the legislation/framework concerned and therefore if a particular matter is reserved, the activities for the prevention of crime in relation to that matter, and the use of the CHIS in particular, are to be treated as relating to a reserved matter.

4.19 For example, the subject matter of the Misuse of Drugs Act 1971 is reserved. The 1971 Act includes powers to search and to obtain evidence, as well as provisions concerning the prosecution and punishment of offences. Where a UK-wide body is conducting CHIS operations in respect of offences under the 1971 Act, as the specific statutory

regime is reserved, then the activities conducted in such investigations are to be treated as relating to that reserved matter.

4.20 This does not affect authorisations for use or conduct where the conduct is likely to take place in Scotland, which will be subject to the process set out in paragraphs 4.13 to 4.14.

International

4.21 CHIS Authorisations can be granted for 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.

4.22 Public authorities are therefore advised to seek authorisations where available under Part II of 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. This is subject to the provision in section 80 of the 2000 Act, which provides that authorisations may not be required where there is another legal basis for the activity concerned. For example, where a deployment overseas has been authorised under the Intelligence Services Act 1994, an authorisation under Part II of the 2000 Act need not be considered unless there are specific reasons to anticipate that part of the activity will take place in the British Islands and would not be covered by the authorisation under the Intelligence Services Act 1994.

4.23 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 Part II of 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.

4.24 To the extent that the obligations under the European Convention on Human Rights apply to overseas territories and to overseas facilities that are within the legal jurisdiction of the UK, authorisations under Part II of the 2000 Act may be appropriate for overseas covert operations. For example, an authorisation may be appropriate in respect of overseas covert operations occurring in UK Embassies, military bases, detention facilities, etc.[15]

4.25 Members of foreign law enforcement or other agencies or CHIS of those agencies may be authorised under Part II of 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 (see paragraph 2.4 above).

[15] See *Al-Skeini and Others v UK* [2007] UKHL 26. If conduct is to take place overseas the NPCC Covert Legislation and Guidance Working Group may be able to offer additional advice.

Online Covert Activity

4.26 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 in circumstances where the other parties could not reasonably be expected to know their true identity[16], should consider whether the activity requires a CHIS authorisation. This applies whether the interaction involves publicly open websites such as an online news and social networking service, or more private exchanges such as messaging sites. Where the activity is likely to result in obtaining private information but does not amount to establishing or maintaining a CHIS relationship, consideration should be given to the need for a directed surveillance authorisation.

4.27 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 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.

4.28 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. However, 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 authorisation 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.*

[16] As an official rather than private individual.

4.29 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 there is an intention 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: *An officer who has maintained a false persona uses that persona to send 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 likely to be appropriate in respect of the proposed covert monitoring of the site if the activity is likely to result in obtaining private information. Once accepted into the group it becomes apparent that further interaction is necessary: this should be authorised by means of a CHIS authorisation.*

4.30 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 a CHIS authorisation. Full consideration should be given to the potential risks posed by that activity.

4.31 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with paragraph 7.15 to 7.21 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.

4.32 Where it is intended that more than one person will share the same online persona, each individual should be clearly identifiable within the overarching authorisation for that operation. The authorisation should provide clear information about the conduct required of – and the risk assessments in relation to – each individual involved. (See also paragraph 3.31.

5 Authorisation procedures for use or conduct of a 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;[17]
- for the purpose of preventing or detecting crime[18] 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;[19]
- 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.[20]

5.2 The Authorising Officer must also believe that the use or conduct of the 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. Part A1 sets out those public authorities that are relevant authorities for the purposes of both section 29 authorisations and Criminal Conduct Authorisations. Part 1 sets out those public authorities that are relevant authorities in respect of section 29 authorisations only.

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 authorisation of the Authorising

---

[17] 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, except another intelligence service, should not issue an authorisation under Part II of the 2000 Act where the investigation or operation 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.

[18] 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.

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

[20] This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the European Convention on Human Rights.

Officer. The 2010 CHIS Order (see paragraph 3.1 above) sets out the seniority of prescribed office, rank and or position that an authorising officer must hold for each different public authority, and the same in respect of those 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 grant authorisations in writing, except in urgent cases, where they may be granted 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, but the full detail should subsequently be recorded in writing by the applicant when reasonably practicable (generally the next working day).

5.6 Officers entitled to act only in urgent cases are empowered to grant authorisation in writing only e.g. written authorisation for use or conduct of a Relevant Source[21] granted 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 investigation or operation for which the authorisation was being granted. 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. 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 it is 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 drawn 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 under the 2013 Relevant Sources Order (see paragraph 2.4 above) should be notified to the Investigatory Powers Commissioner within 7 days when granted by the Authorising Officer, save

[21] As to the meaning of which see paragraph 2.4 above.

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 acting under 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 investigating 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 granted 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 granted; or
- the reasons why the officer entitled to act only 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 granted at 09.00 on 12 February will expire on 11 February. Authorisations (except those granted in urgent cases – see paragraph 5.18 below) will cease at 23.59 on the last day, with any subsequent renewal commencing at 00.00 hours the following day.

5.16 The duration of an authorisation for the use or conduct of a juvenile CHIS, or for criminal conduct where the CHIS to whom the authorisation relates is a juvenile, is four months from the date the authorisation is granted (see paragraph 4.7 above for further detail).

5.17 The duration of an authorisation intended to obtain, provide access to or disclose knowledge of matters subject to legal privilege is reduced from the usual twelve months to 6 months (in the case of an intelligence service authorisation), or 3 months (for any other public authority). Paragraphs 9.30 to 9.31 provide more detail on authorisations where the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 is applicable.

5.18 Urgent oral authorisations or authorisations granted or renewed by an officer who is empowered 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 orally to authorise the use or conduct of CHIS (see paragraph 3.38 above), but arrangements should be in place with Her Majesty's Court Service to enable judicial approval of out of hours applications.

5.19 In certain circumstances, the duration of an authorisation for a particular Relevant Source may need to be adjusted from the statutory twelve-month duration to take into account the cumulative time they have been deployed on a given investigation or operation. Examples provided after paragraph 5.30 below demonstrate where this may be appropriate.

Reviews

5.20 Regular reviews of authorisations should be undertaken by the Authorising Officer to assess whether use or conduct of the CHIS remains necessary and proportionate and whether the authorisation remains justified. (See paragraphs 9.9 to 9.12 below)

Renewals

5.21 Before an Authorising Officer renews an authorisation, they must be satisfied that a review has been carried out of the use made of the CHIS since the last grant or renewal, and of the tasks given and information obtained during that period, and have considered the results of that review.

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

5.23 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.

5.24 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 twelve months should be carried out by a Chief Constable or equivalent and pre-approved by a Judicial Commissioner.

5.25 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 five years (see chapter 8).

5.26 All applications by public authorities under 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.

5.27 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.

5.28 When deciding if the Relevant Source is authorised as part of the "same investigation or operation" for the purpose of 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 the current investigation is a development or recommencement of 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;
- the career history of the Relevant Source.

Fresh authorisation or renewal: online operations

5.29 Sometimes an over-arching operation may be set up as a framework to enable authorised operatives to establish an online presence intended to provide a basis for future enforcement activity, for example within the context of long-term monitoring/investigation of matters such as child sexual abuse or terrorism. Once subjects of interest are identified and this generic, over-arching activity leads to a separate, clearly defined operation against specific subjects, a fresh authorisation is normally appropriate, and any previous relationships that have been formed with the

subjects should be taken into account when calculating the duration of the authorisation. A decision should be taken on a case-by-case basis by reference to the factors listed in paragraph 5.28 above.

5.30 In relation to a continuation of the same operatives on a longer term operation, there should be a presumption towards renewal over a fresh authorisation, even though the individuals targeted may change from time to time. This will ensure that the continuing deployment of the same operatives on that type of online activity over a lengthy period is taken into consideration at the point of renewal. Under the 2013 Relevant Source Order, this will be considered by a Chief Constable or equivalent (and in line with paragraph 5.24 above). Such a renewal for Relevant Sources requires the prior approval of a Judicial Commissioner. It will be open to the Senior Authorising Officer (a Chief Constable or equivalent) to decide that a cancellation and fresh authorisation of the operative(s) may be appropriate, but they should document their rationale for having reached this decision, and specifically their considerations in relation to the points listed in paragraph 5.28 above. Similarly, they should document their conclusions as to the risk to the Relevant Source as per paragraphs 4.31, 4.32 and 7.16 to 7.21. This documented rationale should be recorded within the RIPA documentation and made available on request to the Investigatory Powers Commissioner's Office during its inspections, or at any other time.

Example: *Relevant Sources have been authorised to engage online with groups known or suspected to be sharing indecent images of children on an international scale, under Operation Detect. When specific subjects of interest have been identified to the point at which further, enhanced engagement is required, the Authorising Officer (Assistant Chief Constable or equivalent) will consider whether they wish to authorise this as part of the ongoing conduct of the operatives as part of Operation Detect, or to authorise those operatives, or different ones, under a fresh operation, Operation Detain. Regardless of which decision has been made once subjects have been identified for further approaches (whether online or in the real world), if Operation Detect is to continue beyond twelve months using the same operatives (who will at that point become "long-term" Relevant Sources), then the decision whether to cancel and start under a fresh operation name and directives, or continue to renewal, must be taken by the Chief Constable or equivalent, factoring in the points bulleted in paragraph 5.28.*

5.31 Public authorities acting under the 2013 Relevant Sources Order should notify the Investigatory Powers Commissioner at the 9-month point of any authorisation that may require renewal beyond twelve 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 authorisation 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 a 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, as required by Article 3(4) of the 2013 Relevant Sources Order. If the police force decides to use different Relevant Sources against the subject, an Assistant Chief Constable can grant the authorisation for twelve months and it is treated as a new authorisation, 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 three months, as provided for by the 2010 Legal Privilege Order. 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, in line with the requirements of Article 3 of the 2013 Relevant Sources Order, as the entire period of deployment, including the 3 months at the higher level for access to legally privileged material, would count toward the twelve-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 twelve-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.*

5.32 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

5.33 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.

5.34 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 7.16 to 7.21 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

5.35 If a Judicial Commissioner does not approve the grant of a long-term authorisation of a Relevant Source by the Chief Constable (or equivalent), the relevant public authority may appeal against the decision to the Investigatory Powers Commissioner within 7 days.

5.36 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 CHIS Criminal Conduct Authorisations

Authorisation Criteria

6.1 Under section 29B (5) of the 2000 Act, an authorisation for the criminal 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[22];
- for the purpose of preventing or detecting crime or of preventing disorder[23]; or
- in the interests of the economic well-being of the United Kingdom.

6.2 The other grounds on which the use or conduct of a CHIS can be authorised are not available for a Criminal Conduct Authorisation.

6.3 The Authorising Officer must also believe that the criminal conduct to be authorised is proportionate to what is sought to be achieved by that it (see paragraphs 3.11 to 3.14 of this Code).

6.4 The person granting the authorisation must hold a reasonable belief that the authorisation is necessary and proportionate.

6.5 The person granting the authorisation is best placed to assess necessity and any assessment of reasonableness must be by reference to the circumstances which existed at the time of the authorisation.

6.6 Authorisation is strongly advised where a public authority intends to task a CHIS and the activity tasked is expected to amount to participation in criminal conduct. Where there is any doubt or ambiguity around whether the proposed conduct or use of the CHIS would, or would not, involve a crime, Authorising Officers should consider whether a Criminal Conduct Authorisation is appropriate.

6.7 A Criminal Conduct Authorisation cannot be lawfully authorised in circumstances where the Authorising Officer does not consider that the conduct would be criminal, because the necessity test would not be satisfied. In order for a Criminal Conduct Authority to be granted, the Authorising Officer should believe that there is a risk that the conduct to be authorised amounts to a criminal offence.

---

[22] 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, except another intelligence service, should not issue an authorisation under Part II of the 2000 Act where the investigation or operation 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.

[23] 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.

6.8 However, an authorisation may be granted where there is uncertainty as to whether the conduct will amount to a criminal offence - for example, where facts could materialise which mean that the conduct is not in fact criminal. The Criminal Conduct Authority will have effect to the extent that the authorised conduct would constitute crime. The grant of a Criminal Conduct Authorisation does not indicate that the authorised conduct would otherwise constitute crime.

Relevant public authorities

6.9 A limited number of public authorities are entitled to authorise the criminal conduct of a CHIS. The number of public authorities entitled to authorise criminal conduct is far fewer than those entitled to authorise the use or conduct of a CHIS.

6.10 The public authorities entitled to authorise criminal conduct by or in relation to a CHIS are laid out in Part A1 of Schedule 1 to the 2000 Act, which was inserted by the Covert Human Intelligence Sources (Criminal Conduct) Act 2021.

Authorisation procedures

6.11 Responsibility for authorising criminal conduct rests with the Authorising Officer and all authorisations require the personal authorisation of the Authorising Officer. The 2010 CHIS Order (see paragraph 3.1 above) sets out the seniority of prescribed office, rank and or position that an authorising officer must hold for each different public authority, and the same in respect of those officers entitled to act only in urgent cases.

6.12 The Authorising Officer must grant authorisations in writing, except in urgent cases, where they may be granted 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, but the full detail should subsequently be recorded in writing by the applicant when reasonably practicable (generally the next working day).

6.13 Officers entitled to act only in urgent cases are empowered to give authorisation in writing only . Such officers may only grant an authorisation where it is not reasonably practicable, having regard to the urgency of the case, for the application for an authorisation to be considered by the appropriate Authorising Officer.

6.14 A case is not normally to be regarded as urgent unless the time that would elapse before the Authorising Officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being granted. 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.

6.15 As for use or conduct authorisations (see paragraph 5.8) an Authorising Officer must not authorise their own activities, including criminal conduct. They should also where possible be independent of the investigation.

Notification to Judicial Commissioners – Criminal Conduct Authorisations

6.16 The Investigatory Powers Commissioner is required by statute to, in particular, keep under review the exercise of the power to grant Criminal Conduct Authorisations.

6.17 Where a person grants, renews or cancels a Criminal Conduct Authorisation under Section 29B of the 2000 Act, they must give notice to a Judicial Commissioner at the Investigatory Powers Commissioner's Office.

6.18 The notice must be given as soon as reasonably practicable and within 7 days of the authorisation being granted, renewed, or cancelled.

6.19 The notice must set out the grounds on which the person giving the notice believes the authorisation to be necessary and proportionate and must specify what conduct is authorised.

6.20 In respect of the grant of an authorisation, the conduct that has been authorised can begin as soon as the authorisation has been granted by the Authorising Officer; there is no requirement to wait for comments from a Judicial Commissioner before commencing the activity.

6.21 Where a Judicial Commissioner makes observations in relation to a notification, it is for the Authorising Officer to determine what action should be taken. Having consulted with a more senior officer, they must, as soon as reasonably practicable, notify the Investigatory Powers Commissioner's Office of the intended action, or where action has been taken (for example in urgent cases) of the action.

Information to be provided in applications for authorisation of criminal conduct

6.22 An application for the authorisation of participation in criminal conduct by a CHIS should be in writing and record:

- the section 29 authorisation to which it relates;
- the reasons why the authorisation is necessary in the particular case and on which of the grounds listed in Section 29B(5) of the 2000 Act;
- the purpose for which the CHIS will be tasked to participate in criminal conduct;
- the nature of what the criminal conduct will be;
- the reasons why the criminal conduct is considered proportionate to what it seeks to achieve;
- 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 level of authorisation required;
- a subsequent record of whether authorisation was given or refused, by whom and the time and date.

6.23 The authorisation should have clear parameters set out for the CHIS to ensure they are clear about the criminal conduct in which they are being authorised to participate.

6.24 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 granted; or
- the reasons why the officer entitled to act only 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.

6.25 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).

6.26 When completing an application, the applicant 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.

6.27 The criminal conduct that may be authorised is not limited to criminal conduct by a CHIS: a Criminal Conduct Authorisation may authorise conduct by someone else "in relation to" a CHIS, namely those within a public authority that are involved in or affected by the authorisation.

Duration of authorisations

6.28 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.

6.29 A Criminal Conduct Authorisation can last no longer than the related section 29 authorisation and will cease to have effect if the related section 29 authorisation is cancelled or expires.

6.30 An authorisation should be cancelled as soon as reasonably practicable after the authorised conduct has been undertaken or if the conduct is no longer necessary or proportionate. The CHIS should be notified that their conduct is no longer authorised, and a full record should be kept of anything said to / by the CHIS on that issue.

Reviews

6.31 Criminal conduct will often take place and be completed shortly after the conduct has been authorised. In such circumstances the authorisation is no longer needed, and the authorisation must be cancelled and there would be no need to conduct a review.

6.32 However, where this is not the case, regular reviews of an authorisation should be undertaken by the Authorising Officer to assess whether the criminal conduct remains necessary and proportionate and whether the authorisation remains justified.

6.33 The Authorising Officer will stipulate the frequency of formal reviews and the controller should maintain an audit of casework sufficient to ensure that the criminal conduct of the CHIS remains within the parameters of the extant authorisation. This

will not prevent additional reviews being carried out by the Authorising Officer in response to changing circumstances.

6.34 In undertaking reviews, the Authorising Officer should ensure that the authorisation is relied upon for as short a duration as possible.

6.35 As far as possible, the Criminal Conduct Authorisation should be reviewed to the same schedule as the related Section 29 authorisation.

6.36 Any proposed changes to the nature of the criminal participation should be brought to the attention of the Authorising Officer who should consider whether the proposed changes are within the scope of the existing Criminal Conduct Authorisation and whether they remain necessary and proportionate, before approving or rejecting them by way of a review.

6.37 In the event that there are any significant and substantive changes to the nature of the conduct during the course of the authorisation, the Authorising Officer should consider whether it is necessary to apply for a new authorisation and to cancel the existing authorisation. Such changes which mean that it is necessary to apply for a new authorisation may relate to the scale or nature of the criminal conduct authorised – for instance, the involvement of the CHIS in conduct not included in the extant authorisation.

Renewals

6.38 Before an Authorising Officer renews an authorisation, they must be satisfied that a review has been carried out of the use made of a the CHIS since the last grant or renewal, and of the tasks given and information obtained during that period, and have considered the results of the review.

6.39 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.

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

6.41 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.

6.42 Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation.

6.43 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 and proportionate for the authorisation to continue;
- the criminal conduct undertaken by 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 including any information obtained from the criminal conduct of the CHIS; and
- the results of regular reviews of the criminal conduct undertaken by the CHIS.

Cancellations

6.44 The Authorising Officer who granted or renewed the authorisation must cancel it, as soon as is reasonably practicable, if the Criminal Conduct Authorisation no longer satisfies the criteria for authorisation. For example, if the conduct of the CHIS is no longer likely to involve the criminal conduct authorised. Where the Authorising Officer is no longer available, this duty will fall to the person who has taken over the role of the Authorising Officer or the person who is acting as Authorising Officer.

Unauthorised CHIS criminality

6.45 Where a purported Criminal Conduct Authorisation does not meet the requirements of the Part II of the 2000 Act, the conduct will not be rendered lawful by it.

6.46 Conduct that goes beyond what is authorised by a Criminal Conduct Authorisation will also not be rendered lawful by it.

6.47 The responsibility for considering whether unauthorised criminal conduct by a CHIS should be reported to the appropriate authority rests with the relevant public authority. This could include instances where the criminal conduct of a CHIS goes beyond what is specified in the authorisation, or where an invalid authorisation means that the conduct potentially remains criminal.

6.48 Public authorities are expected to have policies in place governing the reporting of unauthorised criminal conduct by a CHIS.

6.49 In addition to any report to an appropriate authority that may be made, the relevant public authority must report relevant errors (for example where a CHIS is tasked to engage in criminal conduct without a Criminal Conduct Authorisation in place) to the Investigatory Powers Commissioner (see paragraphs 8.8 to 8.18).

7 Management of CHIS

Tasking – use or conduct

7.1 Tasking is the assignment given to the CHIS by the persons defined at subsection (5)(a) ("the Handler") and (5)(b) ("the Controller") of section 29 of the 2000 Act, asking the CHIS to obtain, provide access to or disclose information or undertake any necessary criminal conduct as part of the CHIS authorisation. 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.

7.2 Authorisations for the use or conduct of a CHIS under section 29 of the 2000 Act 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 change in the nature of the task that significantly alters the deployment, then a new authorisation may need to be sought. If in doubt, advice should be sought from the Investigatory Powers Commissioner.

7.3 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 operation. 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, followed by an assessment as to whether the existing authorisation covers the unforeseen action or undertaking. Where initial assessment indicates the existing authorisation may be insufficient, a review should be submitted so that the Authorising Officer can decide whether the existing authorisation is sufficient or whether a new authorisation is required.

7.4 Similarly, where it is intended to task a CHIS in a significantly greater or different way than previously identified, the CHIS's handler or controller 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 keep the number of authorisations per CHIS to the minimum and necessary in order to avoid generating excessive paperwork.

Tasking – criminal conduct

7.5 A CHIS may also be tasked to participate in criminal conduct. A Criminal Conduct Authorisation will therefore be required prior to any tasking where it is expected that the CHIS will need to participate in criminal conduct.

7.6 Criminal Conduct Authorisations should be specific in nature and should contain clear parameters. The public authority must ensure that the CHIS is clear about the criminal conduct in which they are being tasked to participate.

Handlers and controllers

7.7 Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers acting as handler and as controller for each CHIS (see subsection (5)(a) and (5)(b) of section 29 and, in the case of a source of a "relevant collaborative unit", subsection (4A)(a) and (4A)(b) of section 29). As in paragraph 5.8 above, the Authorising Officer must also be a different person to the CHIS, the handler and the controller.

7.8 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.

7.9 The handler of a CHIS will usually be of a rank or position below that of the Authorising Officer.

7.10 The controller will normally be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

7.11 Oversight and management arrangements for undercover operatives, while following the requirements 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

7.12 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.

7.13 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.

7.14 Management responsibility for the use and conduct of CHIS, and relevant roles, may also be divided between different police forces or 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.[24]

Security and welfare

7.15 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.

7.16 Before granting a CHIS authorisation, 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.

7.17 The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should be considered at the outset and reviewed throughout the period of authorised activity by that CHIS.

7.18 Consideration should 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.

7.19 Additional guidance about protecting the identity of the CHIS is provided at paragraphs 9.25 to 9.28 below.

7.20 The handler is responsible for bringing to the attention of the 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.

7.21 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.

[24] For statutory provisions on “relevant collaborative units” see section 29A of the 2000 Act.

8 Record keeping and error reporting

Centrally retrievable record of CHIS authorisations

8.1 A centrally retrievable record of all CHIS authorisations should be held by each public authority. These records need only contain the name, code name, or unique identifying reference of the CHIS, and the date the authorisation was granted, renewed or cancelled. 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 (see paragraph 2.4 above). These records should be retained for a period of at least five years from the ending of the authorisations to which they relate.

8.2 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 2018 and, where applicable, the code of practice on the Management of Police Information.

8.3 Records must be retained to allow the Investigatory Powers Tribunal 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 2000 Act), particularly where continuing conduct is alleged.

Individual records of authorisation and use of CHIS

8.4 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 a section 29 authorisation 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, detail 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.

8.5 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

8.6 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 twelve months (where applicable).

8.7 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

8.8 This section provides information regarding errors. Proper application of the provisions of 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.

8.9 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.

8.10 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.

8.11 A relevant error occurs where both of the following conditions are met:

- There has been an error by a public authority in complying with any requirements imposed by the Act which are subject to review by a Judicial Commissioner, and covert human intelligence source activity has taken place.

8.12 The following provides a non-exhaustive list of possible relevant errors by a public authority that would fall within the definition of a relevant error at paragraph 8.11 above:

- covert human intelligence source activity (including participation in crime) has taken place without lawful authorisation;
- there has been a failure to adhere to the safeguards set out in the relevant statutory provisions or to have regard to this Code.

8.13 Errors can have very significant consequences on an affected individual's rights. 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.

8.14 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.

8.15 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.

8.16 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.

8.17 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 Commissioner.

8.18 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 8.14 apply as they apply to the reporting of a relevant error.

Serious Errors

8.19 Section 231 of the 2016 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.

8.20 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 intelligence services.

8.21 Before making a 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.

8.22 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.

9 Safeguards (including privileged or confidential information)

9.1 This chapter provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through a CHIS authorisation. It also details the procedures and safeguards to be applied where CHIS 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.

9.2 Public authorities should ensure that their actions when handling private information obtained by means of a CHIS authorisation comply with relevant legal frameworks, so that any interference with the right to private and family life is justified in accordance with Article 8(2) of the European Convention on Human Rights. 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.

9.3 All material obtained through a CHIS authorisation 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 personal data breaches should also be reported to the Information Commissioner in accordance with the requirements of the applicable data protection regime. 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.

9.4 Dissemination, copying and retention of material obtained through a CHIS authorisation must be limited to the minimum necessary for the authorised purposes. Dissemination, copying or retention of material 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 authorisation of a CHIS;
- it is necessary to do so for facilitating the carrying out of the functions under the Act of the public authority;
- it is necessary to do so for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal;
- it is necessary to do so for the purposes of legal proceedings; or
- it is necessary to do so for the performance of the functions of any person by or under any enactment.

Use of material as evidence

9.5 Subject to the provisions in this chapter of this Code, material obtained from a CHIS may be used as evidence in criminal proceedings.[25] The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 ("CPIA"), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984[26] and the Human Rights Act 1998. Whilst this Code does not affect the application of those rules and provisions, obtaining appropriate authorisations should help ensure the admissibility of evidence derived from CHIS.

9.6 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 CPIA and these considerations will apply to any material acquired through a CHIS authorisation that is used in evidence. When information obtained through a CHIS authorisation 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.

9.7 Where material acquired through a CHIS authorisation 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 CPA. Particular attention is drawn to the requirements of the Code of Practice issued under CPIA, which requires that the investigator retain all material obtained in an investigation which may be relevant to the investigation.

9.8 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 CHIS authorisations

9.9 Regular reviews of CHIS authorisations should be undertaken by the Authorising Officer. The results of a review should be retained for at least five years (see chapter 8 above).

9.10 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 a CHIS authorisation, they must have regard to 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.

9.11 In each case, unless specified by the Secretary of State or Investigatory Powers Commissioner, the Authorising Officer within each public authority should determine

[25] 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)

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

how often a review should take place. This should be as frequently as is considered necessary and proportionate 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 public authority.

9.12 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

9.13 Paragraphs 9.17 to 9.20 of this Code provide guidance as to the safeguards which govern the dissemination, copying, storage and destruction of material obtained through a CHIS authorisation. 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 2018 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

9.14 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.

9.15 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 a CHIS authorisation 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.

9.16 There is nothing in the 2000 Act which prevents material obtained through A CHIS authorisation from being used to further other investigations where it becomes relevant and in accordance with the safeguards in this chapter.

Dissemination of information

9.17 Material acquired through a CHIS authorisation 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 paragraph 9.4 above. This obligation applies equally to disclosure to additional persons within a public authority, and to disclosure outside an agency.

9.18 This obligation is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle in accordance with subsection (4A)(e) and subsection (5)(e) of section 29of the 2000 Act: 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.

9.19 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.

9.20 The above is not intended to affect arrangements for sharing actionable intelligence in accordance with the statutory functions and procedures of public authorities.

Copying

9.21 Material obtained through a CHIS authorisation may only be copied to the extent necessary for the authorised purpose (set out at paragraph 9.4 above). 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 a CHIS authorisation.

Storage

9.22 Material obtained through a CHIS authorisation 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.

9.23 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

9.24 Material obtained through a CHIS authorisation, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as it is no longer needed for the authorised

purposes set out at paragraph 9.4 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.[27]

Protection of the identity of a CHIS

9.25 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.

9.26 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.

9.27 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.

9.28 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

9.29 Particular consideration should be given in cases where the subject of any intrusion might reasonably assume a high degree of confidentiality, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential constituent information or confidential journalistic material. So, for example, extra care should be taken where, through a CHIS authorisation, 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.

---

[27] 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.

9.30 Annex A of this Code lists the position, rank or office of the authorising officer(s) for each public authority, permitted to authorise the use or conduct, or criminal conduct of a CHIS, in circumstances where it would be possible to acquire knowledge of privileged or confidential information. The authorisation levels are set at a more senior level than that required for other CHIS activity, reflecting the sensitive nature of such information.

9.31 In cases where material subject to legal privilege is obtained, accessed or disclosed as part of the authorised conduct of a CHIS, the 2010 Legal Privilege Order applies (see paragraphs 5.17 and 5.27 above). The 2010 Legal Privilege Order provides that a CHIS authorisation 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. Paragraphs 9.60 to 9.67 below provide further detail on authorisations involving legally privileged material.

9.32 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

9.33 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.

9.34 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.

9.35 Confidential constituent information is information held in confidence relating to communications between a member of a relevant legislature and a constituent in respect of constituency business. 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. In this context, references to a member of a relevant legislative means of members of either House of the UK Parliament, the Scottish Parliament, the National Assembly for Wales, and the Northern Ireland Assembly.

9.36 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.

9.37 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 paragraph 9.4 above.

9.38 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.

9.39 Any case where confidential personal or constituent information is retained, other than for the purpose of destruction, should be notified to the Investigatory Powers Commissioner's Office during their next inspection 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

9.40 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.

9.41 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.

9.42 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.

9.43 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).

9.44 When a public authority applies for a CHIS 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 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.

9.45 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 journalistic sources in this Code should be understood to include any person acting as an intermediary between a journalist and a source.

9.46 When a public authority applies for a CHIS 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.

9.47 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.

9.48 The acquisition of material through a CHIS authorisation will be a justifiable interference with an individual's human rights under Article 8 (right to respect for private and family life) and, in certain circumstances, Article 10 (freedom of expression) of the European Convention on Human Rights only if the conduct being authorised is necessary, proportionate and in accordance with law.

9.49 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.

9.50 Once material has been broadcast, no confidentiality can attach to the material, so it is not confidential journalistic material.

9.51 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.

9.52 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

9.53 As discussed in further detail below, special safeguards apply to matters subject to legal privilege. Section 98 of the Police Act 1997 defines those matters that are subject to legal privilege.[28] 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 a CHIS authorisation.

9.54 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). Legal privilege does not apply to material held with the intention of furthering a criminal purpose (whether the legal adviser is acting unwittingly or culpably). But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.

9.55 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. It can also apply in relation to communications not involving a lawyer, where the communication involves a repetition of legal advice that has been provided with the expectation of confidentiality. For example, an individual repeating legal advice to their spouse in confidence.

9.56 Where a public authority is seeking a CHIS authorisation where the purpose (of one of the purposes) of the authorisation is to obtain legally privileged material, the application must also 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 Article 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

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

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 CHIS authorisation 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.*

9.57 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 “furthering a criminal purpose” exception, advice should be sought from a legal adviser to the relevant public authority.

9.58 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 European Convention on Human Rights, 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 the purpose (or one of the purposes) of the authorisation is to obtain privileged material;
- 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 created or held with the intention of furthering a criminal purpose, would be subject to privilege.

Further guidance is set out in paragraphs 9.60 to 9.77 below as to what should be done in each of those cases.

9.59 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.

CHIS authorisations and legal privilege

9.60 If a public authority seeks to grant or renew a CHIS authorisation, in circumstances where the authorised conduct involves obtaining, providing access to or disclosing matters subject to legal privilege, the 2010 Legal Privilege Order will apply.

9.61 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.

9.62 The approving officer must be satisfied that the CHIS 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 Article 6 of the 2010 Legal Privilege Order). An 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 the CHIS authorisation in question, but may not authorise the CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege.

9.63 Further, in considering any such application, the approving officer must be satisfied that the proposed CHIS authorisation 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.

9.64 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.

9.65 If the CHIS authorisation 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 CHIS's deployment, the application should include, in addition to the reasons why the authorisation 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 a CHIS authorisation 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.

9.66 The duration for which a CHIS authorisation may be granted is reduced where the 2010 Legal Privilege Order is applicable. The usual twelve 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.

CHIS authorisations that 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

9.67 Where an application for a CHIS authorisation is made to authorise conduct that involves obtaining 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 Article 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 and paragraph 6.26 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

9.68 Public authorities should make every effort to avoid a 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.

9.69 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.

9.70 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. Where it is believed that knowledge of matters subject to legal professional privilege may have been unintentionally retained, please refer to paragraphs 9.68 – 9.71 of this Code.

9.71 If it becomes apparent during the course of a deployment that it will be necessary for the CHIS to obtain, provide access to or disclose knowledge of matters subject to legal privilege, the initial CHIS authorisation should be cancelled and replaced by an authorisation that has been subject to the prior approval procedure, set out in the 2010 Legal Privilege Order and in paragraphs 9.56 to 9.66 above, at the earliest reasonable opportunity. This is because the nature of the operation has changed, and the enhanced safeguards are applicable.

Lawyers' material

9.72 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 9.53, 9.54 9.55 or 9.58 will apply, as relevant.

9.73 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 9.58 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.

9.74 Any such case should also be notified to the Investigatory Powers Commissioner's Office during their 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

9.75 In addition to safeguards governing the handling and retention of material as provided for in paragraphs 9.13 to 9.24 of this Code, authorised persons who analyse material obtained by a CHIS authorisation should be alert to any communications or items which may be subject to legal privilege. Paragraphs 9.70 to 974 of this Code set out the additional arrangements that apply to legally privileged items where the intention is to retain them for a purpose other than their destruction.

9.76 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 Investigatory Powers Commissioner may be informed, who will be able to give a view. 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.

9.77 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. Paragraphs 9.78 to 9.81 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 Investigatory Powers Commissioner

9.78 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.

9.79 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.

9.80 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 or 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.

9.81 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

9.82 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.

9.83 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.

9.84 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.

10 Oversight

The senior responsible officer

10.1 Within every relevant public authority, a senior responsible officer[29] 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 2000 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 and inspectors who support the Commissioner when they conduct their inspections;
- where necessary, oversight of the implementation of post-inspection action plans recommended or 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 Investigatory Powers Commissioner - CHIS authorisations

10.2 The Investigatory Powers Act 2016 ("the 2016 Act") provides for an Investigatory Powers 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.

10.3 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.

10.4 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

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

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). The 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).

10.5 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).

10.6 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 this Code must, in accordance with the procedure set out in chapter 8 of this Code, report to the Commissioner any relevant error of which they are aware. This may be in addition to the person raising concerns through the internal mechanisms for raising concerns within the public authority.

10.7 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 that has made the error will be able to make representations to the Commissioner before the Commissioner decides if 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 11 of this Code for more information on how this can be done).

10.8 The Commissioner must report annually on the findings of their audits, inspections and investigations. This will include information on the authorisation of the use, conduct, and criminal conduct of CHIS. 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.

10.9 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.

10.10 Further information about the Investigatory Powers Commissioner, their office and their work may be found at: www.ipco.org.uk

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

The Intelligence and Security Committee

10.12 The Intelligence and Security Committee of Parliament ("ISC") is the committee of Parliament that has statutory responsibility for oversight of the UK Intelligence Community.

10.13 In line with its remit under the provisions of the Justice and Security Act 2013 and the Memorandum of Understanding, such information as is requested in order for the ISC to provide effective oversight of these policies, shall be provided to the Committee.

11 Complaints

11.1 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.

11.2 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 the 2000 Act), as well as an individual.

11.3 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

11.4 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.

12 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	Assistant Chief Constable
Royal Navy Police	Provost Marshal	Provost Marshal
Royal Military Police	Provost Marshal	Provost Marshal
Royal Air Force Police	Provost Marshal	Provost Marshal
British Transport Police	Chief Constable	Assistant Chief Constable
National Crime Agency	Director General Operations	Deputy Director
Serious Fraud Office	Designated members of the Senior Civil Service	Designated members of the Senior Civil Service
The Intelligence Services:		
The Security Service	Deputy Director General	Deputy Director General
The Secret Intelligence Service	Director of Service	A member of the Intelligence Service not below the equivalent rank to that of a Grade 5 in the Home Civil Service

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
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 (Fraud Investigation Service) or a nominated Deputy Director & Assistant Director	Grade 7 (Intel)
Department for the Environment, Food and Rural Affairs:		
DEFRA Investigation Services	Head of DEFRA Investigation Service	Head of DEFRA Investigation Service
Centre for Environment, Fisheries and Aquaculture Science	Head of Better Regulation	Head of Better Regulation
Marine Management Organisation	MMO Director (SCS1 equivalent)	MMO Director (SCS1 equivalent)
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 Her Majesty's Prison and Probation Service	A member of the senior Civil Service in Her Majesty's Prison and Probation Service not below the equivalent rank of a Grade 5 in the Home Civil Service

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
Department of Justice Northern Ireland:		
Northern Ireland Prison Service	Director of Reducing Reoffending	Director of Reducing Reoffending
Department for Business, Energy and Industrial Strategy:		
The Insolvency Service	Chief Operating Officer	Chief Operating Officer
Welsh Government	Director General Health & Social Services	Director General Health & Social Services
	Group/Chief Executive NHS Wales	Group/Chief Executive NHS Wales
	Director of Finance Department of Health & Social Services	Director of Department of Health & Social Services
	Head of Rural Payments Division	Head of Rural Payments Division
	Deputy Director, Marine and Fisheries Division	Deputy Director, Marine and Fisheries Division
	Head of Department or equivalent grade in the Care Inspectorate Wales	Head of Department or equivalent grade in the Care Inspectorate 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 county 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

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
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	CEO of the Financial Conduct Authority	CEO 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 Regulation	Director of Regulation

13 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)

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
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)

(1) Relevant public authorities	(2) Prescribed offices etc.	(3) Urgent cases	(4) Grounds set out in section 29(3) of the Act
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** Director General Operations	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** Senior Civil Service pay band 1 with responsibility for 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	Grade 6 with responsibility for criminal investigations in relation to immigration and border security	Paragraphs (b), (c) and (d)"