Covert Human Intelligence Sources

Code of Practice

Issued on 11 December 2017

Scottish Government
Riaghaltas na h-Alba
gov.scot

Covert Human Intelligence Sources Code of Practice[1]

Pursuant to Section 24 of the Regulation of Investigatory Powers (Scotland) Act 2000

Contents

[1] SG/2017/283

1. Introduction

Definitions

1.1. In this code:

- "RIP(S)A" means the Regulation of Investigatory Powers (Scotland) Act 2000;
- "1997 Act" means the Police Act 1997;
- "RIPA" means the Regulation of Investigatory Powers Act 2000;
- "IPA" means the Investigatory Powers Act 2016;
- "2010 Order" means the Regulation of Investigatory Powers (Prescription of Offices, etc. and Specification of Public Authorities) (Scotland) Order 2010[2];
- "2014 Order" means The Regulation of Investigatory Powers (Authorisation of Covert Human Intelligence Sources) (Scotland) Order 2014; and
- "CHIS" means covert human intelligence source.

Background

1.2. This code of practice provides guidance on the authorisation of the use or conduct of a CHIS by public authorities under RIP(S)A.

1.3. This code is issued pursuant to Section 24 of RIP(S)A, which stipulates that the Scottish Ministers shall issue one or more codes of practice in relation to the powers and duties in RIP(S)A. This code replaces the previous code of practice issued in 2014. This version of the code reflects changes to the oversight of investigatory powers made under the IPA, including oversight by the Investigatory Powers Commissioner (IPC). The previous arrangements, set out in the code of practice issued in December 2014 should be applied, until the relevant provisions of the 2016 Act have been commenced.

1.4. This code of practice is primarily intended for use by the public authorities able to authorise activity under RIP(S)A. It will also allow other interested persons to understand the procedures to be followed by those public authorities. This code is publicly available and should be readily accessible by members of any relevant public authority seeking to use RIP(S)A to authorise the use or conduct of CHIS.[3]

Effect of code

1.5. RIP(S)A provides that all codes of practice relating to RIP(S)A are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal, including the Investigatory Powers Tribunal, established under RIPA, considering any such proceedings, or to the IPC or one of the Judicial Commissioners responsible for overseeing the powers conferred by RIP(S)A, it must be taken into account. Public authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

[2] As amended by SSI 2013/119 and the 2014 Order.
[3] Being those listed in section 8(3) of RIP(S)A.

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

1.7. For the avoidance of doubt, the duty to have regard to the code when exercising functions to which the code relates exists regardless of any contrary content of a public authority's internal advice or guidance.

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

1.8. RIP(S)A provides for the authorisation of the use or conduct of CHIS. The definitions of these terms are laid out in section 1 of RIP(S)A and Chapter 2 of this code.

1.9. Not all human sources of information will fall within these definitions and an authorisation under RIP(S)A will therefore not always be appropriate.

1.10. Neither RIP(S)A nor this code of practice is intended to affect the existing practices and procedures surrounding criminal participation of CHIS.

Personal data

1.11. Personal data is data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. It is likely that much of the private information obtained by the methods described in this code will be personal data if it is recorded by the relevant agency. Where this is the case, data protection law will apply to the processing of that personal data until it is securely destroyed.

2. Covert human intelligence sources: definitions and examples

Definition of a CHIS

2.1. Under RIP(S)A, a person is a CHIS if:

a) he or she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

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

c) he or she covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.[4]

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 or more of the parties to the relationship is unaware of the purpose.[5]

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.[6]

2.4. The 2014 Order defines a 'relevant source' as being an individual who holds an office, rank or position with the Police Service of Scotland, a police force in England or Wales, the Metropolitan Police, the City of London police force, the Police Service of Northern Ireland, the National Crime Agency, the Ministry of Defence Police, the British Transport Police, the Royal Navy Police or the Royal Military Police. Enhanced authorisation arrangements are in place for this type of source as detailed in this code. Such sources will be referred to as 'relevant sources' throughout this code.

2.5. Any Police Scotland Officer deployed as a 'relevant source' in Scotland will be required to comply with and uphold the principles and standards of professional behaviour set out in Police Scotland's Code of Ethics. Officers deployed as relevant sources from other law enforcement bodies will be required to uphold the principles and standards of professional behaviour set out in the College of Policing Code of Ethics.

Scope of 'use' or 'conduct' authorisations

2.6. Subject to the procedures outlined in Chapter 3 of this code, an authorisation may be obtained under RIP(S)A for the use or conduct of a CHIS.

2.7. For authorisation purposes, the use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.[7] In general, therefore, an authorisation for use of a CHIS will be necessary for any steps taken by a public authority in relation to a CHIS.

[4] See section 1(7) of RIP(S)A.
[5] See section 1(8)(a) of RIP(S)A for full definition.
[6] See section 1(8)(c) of RIP(S)A for full definition.
[7] See section 1(6)(b) of RIP(S)A.

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.[8]

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

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

2.11. The reactive nature of the work of a CHIS, and the need for a CHIS to maintain cover, may make it necessary for a CHIS to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct. Such incidental conduct is regarded as properly authorised by virtue of sections 1(6)(a), 5 and 7(5) of RIP(S)A, even though it was not specified in the initial authorisation. This is likely to occur only in exceptional circumstances, such as where the incidental conduct is necessary to protect life and limb, including in relation to the CHIS, in circumstances that were not envisaged at the time the authorisation was granted.

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

2.12. Public authorities are not required by RIP(S)A to seek or obtain an authorisation just because one is available (see section 30 of RIP(S)A). The use or conduct of a CHIS, however, can be a particularly intrusive and high risk covert technique, requiring dedicated and sufficient resources, oversight and management. Authorisation is therefore advisable where a public authority intends to task someone to act as a CHIS. Public authorities must ensure that all use or conduct is:

- necessary and proportionate to the intelligence dividend that it seeks to achieve; and
- in compliance with relevant Articles of the European Convention on Human Rights (ECHR), particularly Articles 6 (right to a fair trial) and 8 (right to respect for private and family life).

2.13. Unlike directed surveillance (which relates specifically to private information), authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert forming and/or maintaining of a relationship to gain any information. ECHR case law makes it clear that Article 8 includes the right to establish and develop relationships. Accordingly, any forming and/or maintaining of a relationship by a public authority e.g. one party having a covert purpose on behalf of a public authority, is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.

[8] See section 1(6)(a) of RIP(S)A.

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

Establishing, maintaining and using a relationship

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

> **Example 1**: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of RIP(S)A that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, or the test purchase is being monitored for corroborative purposes by a third party, consideration should be given to granting a directed surveillance authorisation.
>
> **Example 2**: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing he has 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 his trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

Legend building

2.16. When a relevant source is deployed to establish their 'legend'/build up their cover profile, an authorisation must be considered under RIP(S)A if the activity will interfere with an individual's Article 8 rights. This will include circumstances where it is not clear to the individual that the relevant source is not who he or she claims to be. The individual does not have to be the subject of any current or future investigation. Interference with any individual's article 8 rights requires authorisation under RIP(S)A. The decision whether or not to authorise rests with the Authorising Officer, who should document their rationale accordingly. A decision not to authorise should be reviewed on a suitably regular basis.

Human source activity falling outside CHIS definition

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

Public volunteers

2.18. In many cases involving sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that they have observed or acquired other than through a personal relationship, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of RIP(S)A and no authorisation under RIP(S)A is required.[9]

> **Example 1**: A member of the public volunteers a piece of information to a member of a public authority regarding something he has witnessed in his neighbourhood. The member of the public would not be regarded as a CHIS. He is not passing information as a result of a relationship which has been established or maintained for a covert purpose.
>
> **Example 2**: A caller to a confidential hotline (such as Crimestoppers) reveals that he knows of criminal activity. Even if the caller is involved in the activities on which he is 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 his relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so) an authorisation for the use or conduct of a CHIS may be appropriate.

Professional or statutory duty

2.19. Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 are required to report suspicious transactions.

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

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

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

[9] See Chapter 2 of this code for further guidance on types of source activity to which authorisations under RIP(S)A may or may not apply.

Tasking not involving relationships

2.23. Tasking a person to obtain information covertly may result in authorisation under RIP(S)A 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 RIP(S)A e.g. for directed surveillance may need to be considered where there is a possible interference with the Article 8 rights of an individual.

Identifying when a human source becomes a CHIS

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

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

> **Example**: Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private and family life of Mr Y's work colleague.

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

3. General rules on authorisations

Authorising officer

3.1. Responsibility for giving the authorisation will depend on which public authority is responsible for the CHIS. For the purposes of this code, the person in a public authority responsible for granting an authorisation will be referred to as the "authorising officer". The relevant public authorities and authorising officers are listed in the 2010 Order, as amended by the 2014 Order.

Necessity and proportionality

3.2. RIP(S)A stipulates that the authorising officer must believe that an authorisation for the use or conduct of a CHIS is necessary in the circumstances of the particular case for one or more of the statutory grounds listed in section 7(3) of RIP(S)A.

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

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

3.5. The following elements of proportionality should therefore be considered:

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

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

Extent of authorisations

3.7. An authorisation under RIP(S)A for the use or conduct of a CHIS will provide lawful authority for any such activity that:

- involves the use or conduct of a CHIS as is specified or described in the authorisation;
- is carried out by or in relation to the person to whose actions as a CHIS the authorisation relates; and
- is carried out for the purposes of, or in connection with, the investigation or operation so described[10].

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

Collateral intrusion

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

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

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

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

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

[10] See section 7(5) of RIP(S)A

Example 2: The police seek to establish the whereabouts of Mr W in the interests of preventing and detecting crime. 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 criminal interest. An application for a CHIS authorisation is made to authorise the deployment. The authorising officer will need to consider the necessity and proportionality of the operation against Mr P and Mr W, who will be the direct subjects of the intrusion. The authorising officer will also need to consider the proportionality of any collateral intrusion that will arise if there is any additional interference with the private and family life of other individuals of no interest to the investigation.

Reviewing and renewing authorisations

3.13. Where possible, the authorising officer who grants an authorisation should be responsible for considering subsequent renewals of that authorisation and any related security and welfare issues, except where approval for a long term authorisation is required for a relevant source as set out in the 2014 Order.

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

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

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

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

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

Local considerations and community impact assessments

3.18. Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS.

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

Combined authorisations

3.20. A single authorisation may combine two or more different authorisations under RIP(S)A.[11] 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 police superintendent or above can authorise the conduct of a CHIS (so long as the CHIS isn't a relevant source), but an authorisation for intrusive surveillance needs the separate authorisation of the Chief Constable or a designated senior officer (and the prior approval of a Judicial Commissioner, except in cases of urgency).

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

Operations involving multiple CHIS

3.22. A single authorisation under RIP(S)A may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several relevant sources acting as CHIS in situations where the activities to be authorised, the subjects of the operation, the interference with private and family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each relevant source. If an authorisation includes more than one relevant source, each relevant source must be clearly identifiable within the documentation. In these circumstances adequate records must be kept of the length of deployment of each relevant source to ensure the enhanced authorisation process set out in the 2014 Order can be adhered to.

Covert surveillance of a CHIS

3.23. It may be necessary to deploy covert surveillance against a potential or authorised 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. It is possible that covert surveillance in such circumstances may not be capable of authorisation as it may not be necessary on one of the statutory grounds on which directed surveillance authorisations can be granted. This will depend on the facts of the case. Where the use of surveillance against a CHIS cannot be authorised under RIP(S)A, it will still require to be justifiable under Article 8(2) of the ECHR.

[11] See section 19(2) of RIP(S)A.

Use of equipment by a CHIS

3.24. 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.

3.25. 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 his presence. This also applies to the recording of telephone conversations or other forms of communication, other than by interception, which takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way.

3.26. If a CHIS is acting on behalf of one of the bodies to which the equipment interference provisions of the IPA apply, and is required as part of his 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.

Oversight of use of CHIS by local authorities

3.27. Elected members of a local authority should review the authority's use of RIP(S)A and set the policy at least once a year. They should also consider internal reports on use of RIP(S)A on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations. In regard to the matters mentioned in this paragraph, local authorities may wish to consider ensuring that their elected members have undergone sufficient training in order to fulfil these requirements.

4. Special considerations for authorisations

Vulnerable individuals

4.1. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases, Annex A lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a CHIS.

Juvenile sources

4.2. Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) (Scotland) Order 2002; SSI No. 206 are satisfied. Authorisations for juvenile sources should be granted by those listed in the table at Annex A. The duration of such an authorisation is one month from the time of grant or renewal (instead of 12 months). For these purposes, the age test is applied at the time of the grant or renewal of the authorisation.

Relationship with the Regulation of Investigatory Powers Act 2000 (RIPA)

4.3. RIPA is the appropriate legislation for authorisation of a source whose use or conduct:

- will mainly take place outwith Scotland;
- will start outwith Scotland; or
- is for reserved purposes such as national security or economic well-being.

4.4. Where the conduct authorised is likely to take place in Scotland, authorisation should be granted under RIP(S)A, unless the authorisation is being obtained by certain public authorities (see section 46 of RIPA and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2009; SI No. 3403). RIP(S)A is the appropriate legislation and should be used by Scottish public authorities for all other use or conduct of covert human intelligence sources.

4.5. RIPA contains provisions to allow cross border operations. An authorisation under RIP(S)A will allow Scottish public authorities to use or conduct a source anywhere in the UK for a period of up to three weeks at a time (see section 76(2) of RIPA). This three-week period will restart each time the border is crossed by the source, provided it remains within the original validity period of the authorisation.

4.6. RIPA authorises the conduct or use of a source in Scotland by public authorities (listed in Schedule 1 of RIPA) other than those specified in section 8(3) of RIP(S)A.

Online covert activity

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

4.8. Where someone, such as an employee or member of the public, is tasked by a public authority to establish or maintain a covert relationship with an individual or group online, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

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

4.9. A CHIS authorisation will not always be required for online investigation or research. Some websites require a user to register by 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, although, 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.

4.10. 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” in order 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 gestures may lead to further interaction with other users. A CHIS authorisation should be obtained if it is intended to engage in such interaction to obtain, provide access to or disclose information.

> **Example**: 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.

[12] As an official rather than private individual.

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

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

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

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

4.14. Where it is intended that more than one officer will share the same online persona, each officer should be authorised separately. Clear information should be provided in the application about the conduct required of each officer and individual risk assessments should be undertaken.

5. Authorisation procedures for covert human intelligence sources

Authorisation criteria

5.1. Under section 7 of RIP(S)A an authorisation for the use or conduct of a CHIS may be granted by the authorising officer where he believes that the authorisation is necessary:

- for the purpose of preventing or detecting[13] crime or of preventing disorder;
- in the interests of public safety; or
- for the purpose of protecting public health[14.]

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

Relevant public authorities

5.3. The public authorities entitled to authorise the use or conduct of a CHIS are laid out in the 2010 Order.[15]

Authorisation procedures

5.4. Responsibility for authorising the use or conduct of a CHIS rests with the authorising officer and all authorisations require the personal authority of the authorising officer. The 2010 Order[16] designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases.

5.5. The authorising officer must give authorisations in writing, except in urgent cases, where they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant (or the person with whom the authorising officer spoke) as a priority. This statement need not contain the full detail of the application, which should however subsequently be recorded in writing when reasonably practicable (generally the next working day).

5.6. Other officers entitled to act in urgent cases may only give authorisation in writing.

5.7. A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not generally 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.

---

[13] Detecting crime is defined in section 31(8) of RIP(S)A. Preventing and detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

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

[15] For Food Standards Scotland, see Regulation of Investigatory Powers (Prescription of Ranks and Positions) (Scotland) Order 2016/56 (Scottish SI).

[16] As above.

5.8. Authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the CHIS, the handler of the CHIS, or the controller. Furthermore, authorising officers should, where possible, be independent of the investigation. However, it is recognised that this is not always possible, especially in the cases of small organisations, or where it is necessary to act urgently or for security reasons. However, where possible, clear separation should be maintained between those responsible for the investigation and those managing the CHIS to ensure that the welfare and safety of the CHIS are always given due consideration. Where an authorising officer authorises his own activity, the central record of authorisations should highlight this and it should be brought to the attention of a Judicial Commissioner or Inspector during his next inspection. Where a relevant source is deployed on more than one occasion, 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. All Police Service authorisations of relevant sources should be notified to the IPC when granted by the authorising officer, save where there is a requirement to seek prior approval. The authorisation should be notified to a Judicial Commissioner within seven days. 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. The Police Service should provide the IPC with the authorisation and associated risk assessment for each relevant source.

Information to be provided in applications for authorisation

5.10. 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 7(3) of RIP(S)A (e.g. for the purpose of preventing or detecting crime);
- the purpose for which the CHIS will be tasked or deployed (e.g. in relation to drug supply, stolen property, a series of racially motivated crimes etc);
- where a specific investigation or operation is involved, the nature of that investigation or operation;
- the nature of what the CHIS conduct will be;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any material subject to legal privilege or other confidential information that may be obtained as a consequence of the authorisation;[17]
- 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; and
- the level of authorisation required (or recommended, where that is different).

[17] See Chapter 4 for 'Special considerations for authorisations'.

5.11. A subsequent record of whether authorisation was given or refused, by whom and the time and date should also be recorded.

5.12. Additionally, in urgent cases, the authorisation should record (as the case may be) the following information in writing as soon as is reasonably practicable:

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

5.13. When completing an application, a member of a public authority must follow the "duty of candour" principle and ensure that the Authorising Officer and Judicial Commissioner (as the case may be) is provided with all relevant information upon which they should be asked to reach their decision.

Duration of authorisations

5.14. A written authorisation will, unless renewed or cancelled, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect, except in the case of juvenile CHIS or in the case of matters pertaining to the 2014 Order.

5.15. Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

Reviews

5.16. Regular reviews of authorisations should be undertaken by the authorising officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified.

Renewals

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

5.18. If, before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of 12 months. Renewals may also be granted orally in urgent cases and in this case, can last for a period of 72 hours.

5.19. 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.

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

5.21. Any person who would be entitled to grant a new authorisation can renew an authorisation. However, where possible the authorising officer who granted the original authorisation should consider the renewal.

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

5.23. Applications by the Police Service for renewal to extend an authorisation of a relevant source beyond 12 months must be approved by a Judicial Commissioner before authorisation by the appropriate authorising officer. The 2014 Order creates an enhanced regime of prior approval for such authorisations. Before an authorising officer grants or renews an authorisation to which the 2014 Order applies, he must give notice to the relevant approving officer. The relevant approving officer will be a Judicial Commissioner.

5.24. The 2014 Order provides that a long term authorisation is one where there is either a period totalling 12 months under a single authorisation; or an accumulation of all authorisations granted in relation to the same relevant source deployed on the same investigation or operation. If a relevant source has not been authorised on the same investigation or operation for at least three years, any previous authorisations will be disregarded for the purposes of calculating the 12 months.

5.25. When deciding if the relevant source is authorised as part of the 'same investigation or operation' in calculating the period of deployment, consideration should be given to the target of the investigation or operation; the legend used by the relevant source; relationships established in previous investigation or operations; and if the activity could be considered legend building. In addition, in the spirit of the legislation, the perception that the relevant source is being authorised in the same investigation or operation should also be considered.

5.26. Where a generic authorisation has been provided as a framework for investigators to establish an online presence intended to provide a basis for future enforcement activity, this should be treated as part of the same investigation or operation for renewal purposes. However, where this generic activity leads to a new operation against targets identified through the online presence, a fresh authorisation may be appropriate. Where the same relevant source is to be deployed in the fresh operation, the extent of any prior engagement on line between the relevant source and those subjects now being looked at as part of that separate, more targeted operation, will be a determinant factor.

5.27. The Police Service should notify the IPC at the nine month point of any authorisation that may require renewal beyond 12 months (as calculated in paragraph 5.25).

Example 1: An authorisation has been granted for a relevant source against a subject for the purposes of buying drugs. The subject disappears for one year and there is insufficient evidence obtained at that time to prosecute. The authorisation is cancelled, having been in place for six months. The subject then returns to deal drugs in the area again and the police service wishes to authorise another relevant source against the subject. If the same relevant source is used, authorisation by an Assistant Chief Constable will last for a maximum of six months before requiring to be renewed. If the Police Service decides to use a different relevant source against the subject it is treated as a new 12 month authority, provided the relevant source has not been authorised previously in respect of the same investigation or operation.

Example 2: An authority for a relevant source is initially granted by an Assistant Chief Constable. This lasts for a period of three months before being cancelled. During the operation it was apparent that legally and privileged material was likely to be accessed. Prior approval by the IPC was granted and the deployment authorised by the Chief Constable for three months (as required by the 2014 Order). After this period it was agreed that the relevant source would no longer be likely to access any legally privileged material. Further deployment could be authorised by the Assistant Chief Constable. This could remain in place for six months before requiring to be renewed or cancelled. The entire period of deployment, including the three months authorised at the higher level for access to legally privileged material, would count toward the 12 month period. Who authorised the relevant source and what they have had access to is irrelevant for the purposes of calculating the 12 month period.

5.28. 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

5.29. The authorising officer who granted or renewed the authorisation must cancel it if he is 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 in section 7 of RIP(S)A. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer.

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

5.31. If a Judicial Commissioner does not conclude that a long term authorisation should be granted by the Deputy Chief Constable, the Police Service may appeal against the decision to the IPC, within seven days.

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

6. Management of covert human intelligence sources

Tasking

6.1. Tasking is the assignment given to the CHIS by the persons defined at sections 7(6)(a) and (b) of RIP(S)A, asking them to obtain, provide access to or disclose information. Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

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

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

6.4. Similarly, where it is intended to task a CHIS in a significantly greater or different way than previously identified, the persons defined at section 7(6)(a) or (b) of RIP(S)A must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Handlers and controllers

6.5. Public authorities should ensure that arrangements are in place for the proper oversight and management of a CHIS, including appointing individual officers as defined in section 7(6)(a) and (b) of RIP(S)A for each CHIS.

6.6. Oversight and management arrangements for relevant sources, while following the principles of the RIP(S)A, will differ, in order to reflect the specific role of such individuals as members of public authorities.

6.7. The person referred to in section 7(6)(a) of RIP(S)A (the "handler") will have day to day responsibility for:

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

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

6.9. The person referred to in section 7(6)(b) of RIP(S)A (the “controller”) will normally be responsible for the management and supervision of the “handler” and general oversight of the use of the CHIS.

Joint working

6.10. There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. Such cases may include the prevention or detection of criminal matters affecting 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, or in a joint police/local authority anti-social behaviour operation on a housing estate.

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

Security and welfare

6.12. Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset and reviewed throughout the period of authorised activity by that CHIS. Consideration should also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of a CHIS. For example, this could be by means of disclosure to a court, or tribunal, or any other circumstances where disclosure of information may be required, and strategies for minimising the risks to the CHIS or others should be put in place. Additional guidance about protecting the identity of the CHIS is provided at paragraphs 8.26 and 8.27.

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

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

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

7. Keeping of records

Centrally retrievable record of authorisations

7.1. A centrally retrievable record of all authorisations should be held by each public authority. These records need only contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed or cancelled and an indication as to whether the activities were self-authorised. These records should be updated whenever an authorisation is granted, renewed or cancelled and should be made available to the IPC or Inspector upon request. These records should be used when calculating the period of deployment for the purposes of the 2014 Order. These records should be retained for a period of at least three years from the ending of the authorisations to which they relate.

7.2. While retaining such records for the time stipulated, public authorities must take into consideration the duty of care to the CHIS, the likelihood of future criminal or civil proceedings relating to information supplied by the CHIS or activities undertaken, and specific rules relating to data retention, review and deletion under data protection law and, where applicable, any relevant codes of practice produced by individual authorities in the handling and storage of material.

7.3. Records must be retained to allow the Investigatory Powers Tribunal (IPT), established under Part IV of RIPA, to carry out its functions. The IPT 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 RIPA), particularly where continuing conduct is alleged. It is thus desirable, if possible, to retain records for up to five years.

Individual records of authorisation and use of CHIS

7.4. Detailed records must be kept of the authorisation and use made of a CHIS. Section 7(6) of RIP(S)A provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless he believes 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) (Scotland) Regulations 2002; SSI No: 205 details the particulars that must be included in these records.

7.5. Public authorities are encouraged to maintain auditable records for individuals providing intelligence who do not meet the definition of a CHIS. This will assist authorities to monitor the status of an individual 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 the public authorities.

Further documentation

7.6. In addition, records or copies of the following, as appropriate, should be kept by the relevant authority for at least three 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;
- the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease; and
- a copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months.

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

8. Safeguards (including privileged or confidential information)

Introduction

8.1. This chapter provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through use or conduct of a CHIS. It also details the procedures and safeguards to be applied where authorisations are likely to result in the acquisition of material subject to legal privilege, or other confidential material including journalistic material and the constituency business of a member of a relevant legislature[18].

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

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

8.4. Dissemination, copying and retention of material obtained through use or conduct of a CHIS must be limited to the minimum necessary for the authorised purposes. Dissemination, copying and retention 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 RIP(S)A;
- is necessary for facilitating the carrying out of the functions under RIP(S)A of the public authority ;
- is necessary for facilitating the carrying out of any functions of the IPC or the IPT;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

Retention and destruction of material

8.5. Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use or conduct of a CHIS. Authorising officers must ensure compliance with the appropriate data protection

[18] 'A member of a relevant legislature' means a member of the Scottish Parliament, a member of either Houses of Parliament, a member of the National Assembly for Wales, a member of the Northern Ireland Assembly, or a member of the European Parliament elected for the United Kingdom.

requirements under the data protection law and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

8.6. Where the product of the use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with applicable disclosure requirements.

8.7. Subject to the provisions in Chapter 4, there is nothing in RIP(S)A or this code which prevents material obtained from authorisations for the use or conduct of a CHIS for a particular purpose from being used to further other purposes.

Law enforcement agencies

8.8. In the cases of the law enforcement agencies, particular attention is drawn to the requirements of Part 6 of the Criminal Justice and Licensing (Scotland) Act 2010. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be provided to the prosecutor.

Use of material as evidence

8.9. Subject to the provisions in this chapter, material obtained from a CHIS may be used as evidence in criminal proceedings. The admissibility of evidence is governed by the common law and impacted by the Human Rights Act 1998. While this code does not affect the application of those rules, obtaining appropriate authorisations should help ensure the admissibility of evidence derived from CHIS.

8.10. Product obtained by a CHIS is subject to the ordinary rules for retention and disclosure of material.

8.11. Any decisions by a Judicial Commissioner in respect of granting prior approval for use or conduct of a CHIS shall not be subject to appeal or be liable to be questioned in any court.[19]

8.12. Ensuring the continuity and integrity of evidence is critical to every prosecution. These considerations will apply to any material acquired through use or conduct of a CHIS that is used in evidence. When information obtained through use or conduct of a CHIS is used evidentially, the public authority should be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

8.13. Where material acquired through use or conduct of a CHIS could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements.

Reviewing authorisations

8.14. Regular reviews of all authorisations should be undertaken during their lifetime to assess the necessity and proportionality of the conduct. 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 particularly sensitive information is likely to be obtained. At the point the public authority is considering applying for an authorisation, they must have regard to whether the level of protection to be applied

[19] See section 91(10) of the 1997 Act

in relation to information obtained under the authorisation is higher because of the particular sensitivity of that information.

8.15. In each case, unless specified by a Judicial Commissioner, the frequency of reviews should be determined by the public authority that made the application. This should be as frequently as is considered necessary and proportionate.

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

Handling material

8.17. Paragraphs 8.20 to 8.25 provide guidance as to the safeguards which govern the dissemination, copying, storage and destruction of material obtained through use or conduct of a CHIS. Each public authority must ensure that there are internal arrangements in force for securing that the requirements of these safeguards are satisfied in relation to such material. Authorising officers, through their relevant Data Protection Officer, must ensure compliance with all data protection requirements under data protection law including any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

8.18. The heads of law enforcement agencies are also under a duty to ensure that arrangements are in force to secure that: (i) no information is obtained except so far as necessary for the proper discharge of their functions; and (ii) no information is disclosed except so far as is necessary for those functions, for the purpose of any criminal proceedings.

8.19. Public authorities' internal arrangements should be made available to the IPC. The arrangements should ensure that the disclosure, copying and retention of material obtained through use or conduct of a CHIS is limited to the minimum necessary for the authorised purposes. Breaches of these handling arrangements should be reported to the IPC.

Dissemination of material

8.20. Material acquired through use or conduct of a CHIS may need to be disseminated both within and between agencies, as well as to consumers of intelligence (which includes oversight bodies 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 classed 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. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside an agency. It may be enforced, where appropriate, by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle in accordance with section 7(6)(e) of RIP(S)A: this requires that records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons. For example, if a summary of the material will suffice, no more than that should be disclosed.

8.21. The obligations apply not just to the original public authority, but also to anyone to whom the material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the original public authority's permission before disclosing the material further. In others, explicit safeguards should be applied to secondary recipients. The above is not intended to affect arrangements for sharing actionable intelligence in accordance with the statutory functions and procedures of public authorities, particularly where that information has been prepared to ensure that it does not disclose the identity of the CHIS or sensitive working processes.

Copying

8.22. Material obtained through use or conduct of a CHIS may only be copied to the extent necessary for the authorised purpose. Copies include not only direct copies of the whole of the material, but also extracts and summaries and any other records which contain material obtained through use or conduct of a CHIS. The making, distribution and destruction of any such copies, extracts and summaries should be recorded in order to ensure that material is not being copied more widely than is necessary.

Storage

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

8.24. 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;
- ICT security to minimise the risk of unauthorised access to ICT systems; and
- an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

8.25. Material obtained through use or conduct of a CHIS, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose. 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. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

Protection of the identity of a CHIS

8.26. 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 investigations and law enforcement work. All organisations have a responsibility to protect

the identity of individuals working as a CHIS, and others who may be affected by the disclosure of the operative's identity. Any corrosion of the belief that organisations will attempt to protect the identities of CHIS by all lawful means possible and where appropriate by neither confirming nor denying the existence of a deployment or the identity of the CHIS, would in turn lead to the position where organisations could no longer credibly encourage people to undertake this difficult work, on the basis that their identities and roles would be protected.

8.27. In all cases it should be borne in mind that the risk to the CHIS may not disappear or deplete 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 which 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 information

8.28. RIP(S)A does not provide any special protection for 'confidential information'. Nevertheless, particular care should be taken in cases where the subject of the intrusion might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information includes 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 the use or conduct of a CHIS, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or between a member of a relevant legislature and a constituent relating to private constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved.

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

8.30. In cases where through the use or conduct of a CHIS it is likely that confidential information will be acquired, the deployment of the CHIS is subject to a higher level of authorisation. The 2010 Order lists the authorising officer for each public authority permitted to authorise use or conduct of a CHIS[20]. In addition, the 2014 Order puts in place further arrangements that must be adhered to for CHIS authorisations where there is a likelihood of obtaining legally privileged material.

8.31. There may be circumstances when a relevant source, as set out in the 2014 Order, will have access to legally privileged or confidential information. In such circumstances the authorisation process set out in the 2014 Order should be adhered to. The authorisation levels for access to confidential material are set out at Annex A.

[20] For Food Standards Scotland, see Regulation of Investigatory Powers (Prescription of Ranks and Positions) (Scotland) Order 2016/56 (Scottish SI)

Confidential personal information and communications of a member of a relevant legislature

8.32. 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 or her 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 an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

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

8.34. Communications of a member of a relevant legislature includes communications sent by, or intended for, a person who is an elected representative, a member of a relevant legislature's private information and communication between a member of a relevant legislature and a constituent in respect of constituency business.

8.35. Where the intention is to acquire confidential personal information, or communications of a member of a relevant legislature, 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 acquisition of confidential personal or elected representative information is likely but not intended, any possible mitigation steps should be considered by the authorising officer and, if none is available, consideration should be given to whether special handling arrangements are required within the relevant public authority.

8.36. Material which has been identified as confidential personal or member of a relevant legislature 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 purpose.

8.37. Where confidential personal or member of a relevant legislature 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 within the relevant public authority before any further dissemination of the material takes place.

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

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

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

8.40. The acquisition of material through use or conduct of a CHIS will be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of the ECHR, only if the conduct being authorised is necessary, proportionate and in accordance with law.

8.41. 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;
- intends the recipient, or intended recipient, of the communication to hold in confidence; or
- in any other case, journalistic material which a person holds in confidence.

8.42. 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.

8.43. 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).

8.44. When a public authority applies for an authorisation where the purpose, or one of the purposes, of the authorisation is to authorise the acquisition of material that the authority believes will be confidential journalistic material, the authorisation 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.

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

8.46. When a public authority applies for an authorisation where the purpose, or one of the purposes is to identify or confirm a source of journalistic information, the application must contain a statement confirming that this is the purpose (or one of the purposes) for the application. The person to whom the application is made may issue the authorisation

only if they consider that appropriate safeguards relating to the handling, retention, use and disclosure of the material are in place.

8.47. 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.

8.48. The acquisition of material through use or conduct of a CHIS will be a justifiable interference with an individual's human rights under Articles 8 (right to respect for private and family life) and, in certain circumstances, 10 (freedom of expression) of the ECHR only if the conduct being authorised is necessary, proportionate and in accordance with law.

8.49. 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. Once material has been broadcast, no confidentiality can attach to the material so it is not confidential journalistic material. The fact that a person uses social media tools to communicate does not, in itself, indicate that that person is a journalist or that he or she is likely to be holding confidential journalistic material.

8.50. 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.

Reporting to the IPC

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

Matters subject to legal privilege - Introduction

8.52. 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.

8.53. For the purpose of this code, any communications 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 and compelling evidence that the 'furthering of 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 material privilege due to the 'in furtherance of criminal purpose' exception, advice should be sought from a legal adviser within the relevant public authority.

8.54. Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if, for example, the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

8.55. Public authorities may obtain knowledge of matters subject to legal privilege via a CHIS in three scenarios: first, where the public authority responsible for the CHIS deliberately authorised the use or conduct of the CHIS in order to obtain knowledge of matters subject to legal privilege; second, where the CHIS obtains knowledge of matters subject to legal privilege through conduct incidental (within the meaning of section 1(6)(a) of RIP(S)A) to his conduct as a CHIS; and, third, where a CHIS obtains knowledge of matters subject to legal privilege where his conduct cannot properly be regarded as incidental to his conduct as a CHIS. Separate guidance is relevant to each scenario.

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

8.56. The 2014 Order creates an enhanced regime of prior approval for such authorisations. It provides that before an authorising officer grants or renews an authorisation to which the Order applies, he or she must give notice to the relevant approving officer. The relevant approving officer will be a Judicial Commissioner. The authorising officer is prohibited from granting or renewing an authorisation to which the 2014 Order applies until he or she has received confirmation in writing that a Judicial Commissioner has approved the application. If a Judicial Commissioner does not approve the application, the authorising officer may still grant an authorisation in respect of the use or conduct of the CHIS in question, but may not authorise the use or conduct of the CHIS to obtain, provide access to, or disclose knowledge of, matters subject to legal privilege.

8.57. Where the intention is to acquire items subject to legal privilege, the authorisation application must contain a statement that the purpose, or one of the purposes, of the authorisation is to obtain legally privileged material. An authorisation should only be issued where there are exceptional and compelling circumstances that make the authorisation necessary, and a Judicial Commissioner approves that decision. Circumstances cannot be exceptional and compelling unless certain conditions are met. Exceptional and compelling circumstances will arise only in a very restricted range of cases, where there is a threat to life or limb or in the interests of national security. The exceptional and compelling test can only be met when the public interest in obtaining the information sought outweighs the public interest in maintaining the confidentiality of legally privileged material, and when there are no other reasonable means of obtaining the required information. The authorised use or conduct 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. For example, if they have intelligence to suggest that an individual is about to commit an act likely to result in serious harm and the consultation may reveal information that could assist in averting the attack (e.g. by

revealing details about the location and movements of the individual) then they might want to target the legally privileged communications.

8.58. Further, in considering any such application, the authorising officer or Judicial Commissioner must be satisfied that the proposed use or conduct 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. The authorising officer or Judicial Commissioner 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. The authorising officer and Judicial Commissioner must consider that there are exceptional and compelling circumstances (see example above) that make it necessary to issue the authorisation and must be satisfied that there are appropriate arrangements in place for the handling, retention, use and destruction of privileged items, and the Judicial Commissioner must approve the issuing authority's decision. In such circumstances, the authorising officer and Judicial Commissioner will be able to impose additional requirements such as regular reporting arrangements, so as to keep the authorisation under review more effectively.

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

Circumstances in which the obtaining of knowledge of matters subject to legal privilege by a CHIS or public authority is incidental to the conduct authorised in the authorisation

8.60. The reactive nature of the work of a CHIS, and the need for a CHIS to maintain cover, may make it necessary for a CHIS to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct. Such incidental conduct is regarded as properly authorised by virtue of section 5 of RIP(S)A, even though it was not specified in the initial authorisation.

8.61. This is likely to occur only in exceptional circumstances, such as where the obtaining of such knowledge is necessary to protect life and limb, including in relation to the CHIS, in circumstances that were not envisaged at the time the authorisation was granted.

8.62. If the use or conduct is not intended to result in the acquisition of knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should include, in addition to the reasons why the use or conduct is considered necessary, an assessment of how likely it is that information which is subject to legal privilege will be obtained. The public authority should also confirm that any inadvertently obtained material that is subject to legal privilege will be treated in accordance with the safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the material that is subject to legal privilege.

8.63. If any of these situations arise, the public authority should draw it to the attention of the Judicial Commissioner or Inspector during his next inspection (at which the material should be made available if requested). In addition, the public authority in question should ensure that any knowledge of matters subject to legal privilege obtained through conduct

incidental to the use or conduct of a CHIS specified in the authorisation is not used in law enforcement investigations or criminal prosecutions.

8.64. If it becomes apparent that it will be necessary for the CHIS to continue to obtain, provide access to, or disclose knowledge of, matters subject to legal privilege, the initial authorisation should be replaced by an authorisation that has been subject to the prior approval procedure set out in the 2014 Order at the earliest reasonable opportunity.

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

8.65. Public authorities should make every effort to avoid their CHIS unintentionally obtaining, providing access to, or disclosing knowledge of, matters subject to legal privilege. If a public authority assesses that a CHIS may be exposed to such knowledge unintentionally, the public authority should task the CHIS in such a way that this possibility is reduced as far as possible. When debriefing the CHIS, the public authority should make every effort to ensure that any knowledge of matters subject to legal privilege which the CHIS may have obtained is not disclosed to the public authority, unless there are exceptional and compelling circumstances that make such disclosure necessary. If, despite these steps, knowledge of matters subject to legal privilege is unintentionally disclosed to the public authority, the public authority in question should ensure that it is not used in law enforcement investigations or criminal prosecutions. Any unintentional obtaining of knowledge of matters subject to legal privilege by a public authority, together with a description of all steps taken in relation to that material, should be drawn to the attention of the Judicial Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

Lawyers' material

8.66. Where a lawyer (acting in a 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 a professional capacity and it is intended that a lawyer's material is to be acquired, the application should be made on the basis that it is intended to acquire communications or items subject to legal privilege and the provisions in paragraphs 8.56 to 8.59 will apply, as relevant.

8.67. The public authority will wish 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 legal 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 paragraphs 8.56 to 8.59 will apply.

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

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

8.69. Legally privileged information is particularly sensitive and any use or conduct of a CHIS which obtains, provides access to or discloses such material may give rise to issues under Article 6 of the ECHR (right to a fair trial) as well as engaging Article 8 (right to respect for private and family life).

8.70. Where public authorities deliberately obtain knowledge of matters subject to legal privilege via the conduct of a CHIS, they may use it to counter the threat which led them to obtain it; but not for other purposes. In particular, public authorities should ensure that knowledge of matters subject to legal privilege is kept separate from law enforcement investigations or criminal prosecutions.

8.71. In cases likely to result in the obtaining by a public authority of knowledge of matters subject to legal privilege, the authorising officer or Judicial Commissioner may require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where knowledge of matters subject to legal privilege has been obtained and retained, the matter should be reported to the authorising officer by means of a review and to the Judicial Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

8.72. A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, in any case where a lawyer is the subject of an investigation or operation, authorising officers should consider whether the special safeguards outlined in this chapter apply. Any material which has been retained from any such investigation or operation should be notified to the Judicial Commissioner or Inspector during his next inspection and made available on request.

8.73. 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 IPC 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.

8.74. 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 IPC must be notified of the retention of the items as soon as reasonably practicable. Paragraph 8.51 provides more detail on reporting privileged items to the IPC. 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.

9. Senior responsible officers and oversight by the IPC

The senior responsible officer

9.1. Within every relevant public authority a senior responsible officer must be responsible for:

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

9.2. Within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the IPC. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

Oversight by the IPC

9.3. The IPA establishes an IPC, 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 IPA requires that the IPC will be, or will have been, a member of the senior judiciary and will be entirely independent of the Scottish and UK Governments or any of the public authorities authorised to use investigatory powers. The IPC will be supported by Judicial Commissioners, Inspectors and others, such as technical experts, qualified to assist the Commissioner in their work (the 'Technology Advisory Panel').

9.4. The IPC, and those that work under the authority of the IPC, will ensure compliance with the law and this code by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The IPC may undertake these inspections, as far as they relate to the IPC's statutory functions, entirely on their own initiative.

9.5. The IPC 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 IPC must not act in a way which is contrary to the public interest or jeopardise operations or investigations. All public authorities using investigatory powers

must, by law, provide all necessary assistance to the IPC and anyone who is acting on behalf of the IPC.

9.6. Anyone working for a public authority who has concerns about the way that investigatory powers are being used may report their concerns to the IPC, who will consider them. In particular, any person who exercises the powers to which this code applies should report to the IPC any action undertaken which they believe to be contrary to the provisions of this code. The IPC may, if they believe it to be unlawful, refer any issue relating to the use of investigatory powers to the IPT.

9.7. The IPC must report annually to the Scottish Ministers in relation to the findings of their inspections and investigations. This report will be laid before the Scottish Parliament and will be made available to the public, subject to any necessary redactions made on the basis the publication would be contrary to the public interest or prejudicial to the prevention or detection of serious crime or the continued discharge of the functions of any public authority whose activities include activities subject to the review of the IPC.

9.8. The IPC may also report, at any time, to the Scottish Ministers on any matter with which they are concerned if a contravention has not already been the subject of a report made to the Scottish Ministers by the IPT. Public authorities may seek general advice from the IPC on any issue which falls within the IPC's statutory remit. The IPC may also produce guidance for public authorities on how to apply and use investigatory powers. Wherever possible, this guidance will be published in the interests of public transparency.

9.9. Further information about the IPC, their office and their work may be found at: ipco.org.uk

10. Complaints

10.1. The IPT has jurisdiction to investigate and determine complaints against public authority use of investigatory powers and human rights claims against the security and intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

10.2. The IPT is entirely independent from the Scottish and UK Governments and all public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. 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.

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

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

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

Annex A

Covert Human Intelligence Sources Code of Practice

Authorisation levels when knowledge of confidential information is likely to be acquired or when a vulnerable individual or juvenile is to be used as a source

Relevant Public Authority	**Authorisation level for when knowledge of confidential information is likely to be acquired**	**Authorisation level for when a vulnerable individual or a juvenile is to be used as a source**
The Police Service of Scotland	Chief Constable[21]	Assistant Chief Constable
The Police Investigations and Review Commissioner	Commissioner	Commissioner
The Scottish Administration		
Marine Scotland	Head of Compliance	
Accountant in Bankruptcy	Accountant in Bankruptcy	
Scottish Prison Service	Chief Executive or Director	Chief Executive or Director
Contracted out prisons	Chief Executive or Director	Chief Executive or Director
Transport Scotland	Chief Executive	
Food Standards Scotland	Chief Executive	Chief Executive
A council constituted under section 2 of the Local Government etc (Scotland) Act 1994	Chief Executive	Chief Executive
The Common Services Agency for the Scottish Health Service	Director of Practitioner and Counter Fraud Services	Director of Practitioner and Counter Fraud Services
The Scottish Environment Protection Agency	Chief Executive	

[21] Reference to the Chief Constable includes any other senior officer of the Police Service of Scotland who is designated by the Chief Constable for this purpose

Annex B

Authorisation levels: use of a relevant source as a covert human intelligence source

Relevant Public Authority	Authorisation level for relevant source	Authorisation level for long term relevant source
The Police Service of Scotland	Assistant Chief Constable	Deputy Chief Constable

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78851-530-6 (web only)

Published by The Scottish Government, December 2017

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS343006 (12/17)