CODE OF PRACTICE ON COVERT HUMAN INTELLIGENCE SOURCES 2021

Issued by the Administrator pursuant to section 38 of the Regulation of Investigatory Powers Ordinance 2012 (**a**).

Contents

1.0 Introduction

Definitions

1.1. In this code:

"AGLA" means the Attorney-General and Legal Adviser;
"CHIS" means a covert human intelligence source;

(**a**) Ordinance 26/2012

"controller" means the person referred to in section 21(3)(b) of RIPO;
"ECHR" means the European Convention for the Protection of Human Rights and Fundamental Freedoms;
"handler" means the person referred to in section 21(3)(a) of RIPO;
"imprisonable crime" has the meaning given in section 3(1) of RIPO;
"investigating authority" means the SBA Customs & Immigration Service or the SBA Police Service;
"IPC" means the Investigatory Powers Commissioner;
"LP authorisation" has the meaning given in section 12 of RIPO;
"matters subject to legal privilege" has the meaning given in section 13 of RIPO;
"RIPO" means the Regulation of Investigatory Powers Ordinance 2012;
"serious crime" has the meaning given in section 3(1) of RIPO.

Background

1.2. This code of practice provides guidance on the authorisation of a covert human intelligence source (a "CHIS") by investigating authorities in accordance with RIPO.

1.3 This code is a revised version of the code issued on 31 October 2012**a** pursuant to section 38 of RIPO, which provides that the Administrator may issue one or more codes of practice in relation to the powers and duties in RIPO. It replaces, in its entirety, the code issued on 31 October 2012.

1.4. This code is publicly available and should be readily accessible by members of any investigating authority seeking to use RIPO to authorise activity by a CHIS.

Effect of code

1.5. RIPO provides that all codes of practice relating to it are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant to any court or tribunal considering any such proceedings, it must be taken into account. Investigating authorities may also be required to justify, with regard to this code, the use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

1.6. Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are not provisions of the code, but 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, authorising officers 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.

Scope of CHIS activity to which this code applies

1.7. RIPO provides for the authorisation for the use or conduct of a CHIS by an investigating authority:

---

a P.I. 28/2012

- for the purpose of preventing or detecting serious or imprisonable crime or of preventing disorder;
- in the interests of public safety; or
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to the Crown.

1.8. However, an LP authorisation may be granted only for the purpose of preventing or detecting serious crime: see paragraphs 4.4 and 4.5.

1.9. Not all human sources of information will fall within the definition of a CHIS and an authorisation under RIPO will not therefore always be appropriate.

1.10. Neither RIPO nor this code is intended to affect the existing practices and procedures surrounding criminal participation of a CHIS.

1.11. Chapter 2 provides a fuller description of a CHIS, along with definitions of terms, exceptions and examples.

2.0 Covert human intelligence sources - definitions and examples

Definition of a CHIS

2.1. Under RIPO, a person is a CHIS if:

- he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the next two bullet points;
- he covertly uses such a relationship to obtain information or to provide access to any information to a third person; or
- he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

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

2.3. A relationship is used covertly, and information obtained is disclosed covertly, 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.

Scope of 'use' or 'conduct' authorisations

2.4. Subject to the procedures outlined in Chapter 3, an authorisation may be obtained under RIPO for the use or conduct of a CHIS.

2.5. The use of a CHIS involves any action on behalf of an investigating 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. In general, therefore, an authorisation for the use of a CHIS will be necessary to authorise steps taken by an investigating authority in relation to a CHIS.

2.6. 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 an investigating authority.

2.7. Most CHIS authorisations will be for both use and conduct. This is because investigating 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 investigating authority, such as responding to particular tasking.

2.8. 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 investigating authorities. Such authorisations should not conflict.

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

2.9. Investigating authorities are not required by RIPO to seek or obtain an authorisation just because one is available. 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. This will include ensuring 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 ECHR, particularly Article 8 and Article 6.

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

2.11. It is therefore strongly recommended that an investigating 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 investigating authority.

Establishing, maintaining and using a relationship

2.12. 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 an investigating 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 regard to the requirements of RIPO that an investigating authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to obtaining a covert 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 investigating 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.*

Human source activity falling outside CHIS definition

2.13. Not all human source activity will meet the definition of a CHIS. For example, a source may be a volunteer who discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of a relationship.

Volunteers

2.14. In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that is within their personal knowledge, without being induced, asked or tasked by an investigating authority. This means that the source is not a CHIS for the purposes of RIPO and no authorisation under RIPO is required.

Example 3: *A member of the public volunteers a piece of information to a member of an investigating 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 4*: A caller to a confidential hotline reveals that he knows of criminal or terrorist 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, an authorisation for the use or conduct of a CHIS may be appropriate.*

Professional or statutory duty

2.15. Certain individuals will be required to provide information to investigating authorities or designated bodies out of a professional or statutory duty. 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.

2.16. Furthermore, this reporting is undertaken “in accordance with the law” for the purposes of Article 8(2) of the ECHR.

2.17. This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which he acquires as a result of an existing professional or business relationship with the subject but that person is under

no obligation to pass it on. For example, a travel agent who is asked by the police to find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances, a CHIS authorisation may be appropriate.

Tasking not involving relationships

2.18. Tasking a person to obtain information covertly may result in authorisation under RIPO being required. 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 5: *A member of the public is asked by a member of an investigating 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 RIPO, such as for covert surveillance, may need to be considered where there is an interference with the Article 8 rights of an individual.*

Identifying when a human source becomes a CHIS

2.19. Individuals or members of organisations (e.g. travel agents 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. Such individuals need to be managed appropriately. Investigating 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.

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

Example 6: *Mr Y volunteers information to a member of an investigating 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 investigating 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 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.*

2.21. 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 RIPO, whether or not that CHIS is asked to do so by an investigating authority. It is possible therefore that a person will become engaged in the conduct of a CHIS without an investigating authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where an investigating authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the investigating authority intends to make use of that material for its own investigative purposes.

3.0 General rules on authorisations

Authorising officer

3.1. Responsibility for granting the authorisation will depend on which investigating authority is responsible for the CHIS. For the purposes of this and future chapters, the person in an investigating authority responsible for granting an authorisation will be referred to as the "authorising officer". The investigating authorities and authorising officers are specified in RIPO.

Necessity and proportionality

3.2. RIPO stipulates that the authorising officer must be satisfied that an authorisation for the use or conduct of a CHIS is necessary in the circumstances of the particular case on one or more of the statutory grounds listed in section 21 of RIPO.

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

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

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

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of RIPO and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- providing evidence, as far as reasonably practicable, of what other methods have been considered and why they were not implemented;
-

- whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation; and

- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

Extent of authorisations

3.6. An authorisation under RIPO for the use or conduct of a CHIS will provide lawful authority for any activity that:

- involves the use or conduct of a CHIS as is specified 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 specified in the authorisation.

3.7. 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

3.8. Before authorising the use or conduct of a CHIS, the authorising officer should take into account the risk of interference with the private and 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.

3.9. Measures should be taken, wherever practicable, to avoid or minimise interference with the private and 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.

3.10. 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.

3.11. 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 and 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 7**: An individual is tasked to obtain information about the activities of a suspected criminal gang under CHIS authorisation. It is assessed that the individual will in the course of this deployment obtain private information about other persons who are not involved in criminal activities and are of no interest to the investigation. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation.*

***Example 8:** The police seek to establish the whereabouts of Mr W in the interests of public safety. In order to do so, a CHIS is tasked to seek to obtain this information from Mr P, an associate of Mr W who is not of direct 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

3.12. 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.

3.13. The authorising officer will stipulate the frequency of formal reviews, and the controller (see paragraph 6.8) 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.

3.14. 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.

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

Example 9: *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 and family life of "Mr X and his associates, including Mr A" and that such an interference is in accordance with the original authorisation.*

3.16. 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.

Local considerations and community impact assessments

3.17. 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 investigating 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.

3.18. It is therefore recommended that, where an authorising officer from an investigating authority other than the SBA Police considers that conflicts might arise, he should, where possible, consult a senior officer within the SBA Police before the CHIS is deployed. All investigating authorities, where possible, should consider consulting with other relevant investigating authorities to gauge community impact.

Combined authorisations

3.19. A single authorisation may combine two or more different authorisations under RIPO. For example, a single authorisation may combine authorisations for covert 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.

3.20. The above does not preclude investigating authorities from obtaining separate authorisations.

Operations involving multiple CHIS

3.21. A single authorisation under RIPO may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the

conduct of several 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 CHIS.

Covert surveillance of a potential CHIS

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

Use of CHIS with technical equipment

3.23. A CHIS wearing or carrying a surveillance device does not need a separate covert surveillance authorisation, provided the device will only be used in the presence of the CHIS. This is the case even if the CHIS is recording activity taking place in residential premises or a private vehicle that takes place in the CHIS's presence. Similarly, a separate covert surveillance authorisation is not needed where the CHIS records telephone conversations or other forms of communication (other than by interception) that take place in the CHIS's presence.

3.24. However, if a surveillance device is to be used other than in the presence of the CHIS, a covert surveillance authorisation should be obtained where appropriate, together with an authorisation for entry on or interference with property, if applicable. (See the Code of Practice on Covert Surveillance and Property Interference.) An authorisation for covert surveillance may not be granted in relation to anything taking place on residential premises or in a private vehicle if a surveillance device is present on the premises or in the vehicle.

4.0 Special considerations for authorisations

Matters subject to legal privilege and other confidential information

4.1. RIPO does not provide any special protection for "confidential information", with the exception of matters subject to legal privilege (see below). 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. Apart from matters subject to legal privilege, confidential information consists of confidential personal information and confidential journalistic material, both of which are defined in RIPO. 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 wherever matters of medical or journalistic confidentiality may be involved.

Matters subject to legal privilege - introduction

4.2. Section 13 of RIPO defines "matters subject to legal privilege". Legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence.

4.3. Investigating authorities may, however, obtain knowledge of matters subject to legal privilege via CHIS in three scenarios: (1) where the investigating authority responsible for the CHIS deliberately authorises the use or conduct of the CHIS in order to obtain knowledge of matters subject to legal privilege; (2) where the CHIS obtains knowledge of matters subject to legal privilege through conduct incidental (as referred to in section 9(2)(a)) to his conduct as a CHIS; and (3) where a CHIS obtains knowledge of matters subject to legal privilege in circumstances 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 to obtain, provide access to or disclose knowledge of matters subject to legal privilege – LP authorisations

4.4. An authorisation for the use or conduct of a CHIS in order to obtain, provide access to or to disclose knowledge of matters subject to legal privilege is an "LP authorisation" (section 12 of RIPO). An LP authorisation may be granted only for the purpose of preventing or detecting serious crime, must be notified to the IPC and takes effect only once the authorising officer has been notified that the IPC has approved the authorisation. The duration of an LP authorisation is 3 months from the time of grant or renewal (instead of 12 months). If the IPC does not approve the authorisation, 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.

4.5. The IPC may only approve, and authorising officers may only authorise, LP authorisations if they are satisfied that there are exceptional and compelling circumstances that make the authorisations necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb, and the use or conduct of a CHIS to require knowledge of matters subject to legal privilege is reasonably regarded as likely to yield intelligence necessary to counter the threat.

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

4.6. 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 9(2), 19 and 21(4) of RIPO, even though it was not specified in the initial authorisation.

4.7. 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.

4.8. If any of these situations arises, the investigating authority should draw it to the attention of the IPC during the next inspection (at which the material should be made available if requested). In addition, the investigating 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.

4.9. 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 LP authorisation, approved by the IPC, at the earliest reasonable opportunity.

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

4.10. Investigating authorities should make every effort to avoid their CHIS unintentionally obtaining, providing access to or disclosing knowledge of matters subject to legal privilege. If an investigating authority assesses that a CHIS may be exposed to such knowledge unintentionally, the investigating authority should task the CHIS in such a way that this possibility is reduced as far as possible. When debriefing the CHIS, the investigating 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 investigating 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 investigating authority, the investigating 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 an investigating authority, together with a description of all steps taken in relation to that material, should be drawn to the attention of the IPC during the next inspection (at which the material should be made available if requested).

The use and handling of material subject to legal privilege

4.11. 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.

4.12. Where investigating 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, investigating authorities should ensure that knowledge of matters subject to legal privilege is kept separate from law enforcement investigations or criminal prosecutions.

4.13. In cases likely to result in the obtaining by an investigating authority of knowledge of matters subject to legal privilege, the authorising officer or IPC 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 IPC during the next inspection (at which the material should be made available if requested).

4.14. 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 IPC during the next inspection and made available on request.

4.15. Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from AGLA's Office before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception (see paragraph 4.2). The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates. Any dissemination of legally privileged material to an outside body should be notified to the IPC during the next inspection.

Other confidential information

4.16. Similar consideration should also be given to authorisations for use or conduct that are likely to result in the obtaining of confidential personal information and confidential journalistic material. Where such material has been acquired and retained, the matter should be reported to the IPC during the next inspection and the material be made available if requested.

4.17. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, 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. Examples might include consultations between a health professional and a patient, or information from a patient's medical records. (Spiritual counselling means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith.)

4.18. 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.

4.19. Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from AGLA's Office, before any further dissemination of the material takes place. Any dissemination of confidential material to an outside body should be notified to the IPC during the next inspection.

Vulnerable individuals

4.20. 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.

Juveniles

4.21. Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as a CHIS: see Schedule 1 to RIPO. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. The duration of an authorisation for a CHIS under 18 years old is 1 month from the time of grant or renewal (instead of 12 months). The age test is applied at the time of the grant or renewal of the authorisation.

4.22. Investigating authorities must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent or guardian of the CHIS, unless they are unavailable or there are specific reasons for excluding them, such as their involvement in the matters being reported upon, or where the CHIS provides a clear reason for their unsuitability. In these circumstances another suitably qualified person should act as appropriate adult, e.g. someone who has personal links to the CHIS or who has professional qualifications that enable them to carry out the role (such as a social worker). Any deployment of a juvenile CHIS should be subject to a risk assessment and the rationale recorded in writing.

Outside the Areas

4.23. Authorisations under RIPO can be given for the use or conduct of CHIS both inside and outside the Areas. However, authorisations for actions outside the Areas can usually only validate them for the purpose of the law of the Areas. Although RIPO and the Human Rights Ordinance 2004 apply only in the Areas, the provisions of RIPO should be applied to the conduct or use of CHIS outside the Areas. This is particularly important when judicial proceedings in the Areas are likely.

Online Covert Activity

4.24. Any member of an investigating 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 (as an official rather than a private individual), should consider whether the activity requires a CHIS authorisation.

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

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

4.26. A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of an investigating authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS

authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example 10: *A customs officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.*

Example 11: *An investigating authority task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.*

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

Example 12**:** *The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.*

4.27. When engaging in conduct as a CHIS, a member of an investigating 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.

4.28. Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.11 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.

4.29. Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved. (See also paragraph 3.21)

5.0 Authorisation procedures for CHIS

Authorisation criteria

5.1. Under RIPO an authorisation for the use or conduct of a CHIS may be granted by the authorising officer where he is satisfied that the authorisation is necessary:

- for the purpose of preventing or detecting serious or imprisonable crime or of preventing disorder;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to the Crown.

5.2. However, an LP authorisation may be granted only for the purpose of preventing or detecting serious crime: see paragraphs 4.4 and 4.5.

5.3. The authorising officer must also be satisfied both that the authorised use or conduct of a CHIS is proportionate to what is sought to be achieved by that use or conduct and that the required arrangements are in place (see section 21(3) of RIPO).

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. RIPO designates the authorising officer for the SBA Police as being the Chief Constable or Deputy Chief Constable (or other officer nominated under section 7 of the Police Ordinance 2007 to exercise the Chief Constable's functions) and for the SBA Customs & Immigration Service as being the Fiscal Officer or a designated deputy. In urgent cases, where an application is made by a police officer, an officer of at least Chief Superintendent rank may authorise the conduct or use of a CHIS. RIPO makes no provision for applications by customs officers to be authorised on an urgent basis by officers other than the Fiscal Officer or a designated deputy.

5.5. The authorising officer must grant authorisations in writing, except in urgent cases, where they may be granted orally by the authorising officer or in writing by the officer entitled to act only in urgent cases. Where authorisations are granted orally, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant 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. There is no provision for urgent applications in the case of LP authorisations.

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

urgent where the need for an authorisation has been neglected or the urgency is of the applicant's or authorising officer's own making.

5.8. Authorising officers should not be responsible for authorising their own activities, e.g., those in which they themselves are to act as the CHIS or as the handler of the CHIS. 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. Where an authorising officer authorises his own activity, the central record of authorisations should highlight this.

5.9. Authorising officers within the SBA Police may grant authorisations only on application by a member of (including those formally seconded to) the SBA Police. Customs officers within SBA Customs & Immigration will grant authorisations on application by a customs officer.

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 necessary grounds (e.g., for the purpose of preventing or detecting imprisonable 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, nature of that investigation or operation; • the nature of what the CHIS will be tasked to do;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the level of authorisation required; and
- a subsequent record of whether authorisation was granted or refused, by whom and the time and date.

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

- the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was granted; or
- where the officer entitled to act only in urgent cases has granted written authority, the reasons for the urgency and why it was not reasonably practicable for the application to be considered by the authorising officer whose entitlement to act is not so confined.

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

5.13. When completing an application, the investigating authority must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which weakens the case for the authorisation.

Duration of authorisations

5.13. A written authorisation will, unless renewed, 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 a juvenile CHIS or an LP authorisation. See Chapter 4.

5.14 An authorisation for the use or conduct of a juvenile CHIS is one month from the date the authorisation is given.

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 took effect.

Reviews

5.16. Regular reviews of authorisations should be undertaken to assess the need for the use of a CHIS to continue and that the authorisation remains justified. The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS. The results of a review should be retained for at least 3 years. Particular attention is drawn to the need to review authorisations frequently where the use of a CHIS provides access to confidential information or involves significant collateral intrusion.

5.17. In each case the authorising officer within each investigating authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable, but should not prevent reviews being conducted in response to changing circumstances. See Chapter 3.

Renewals

5.18. 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.

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

5.20. A renewal takes effect at the time at which, or day on 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.

5.21. Any person who would be entitled to grant a new authorisation can renew an authorisation. However, where possible, the same authorising officer that 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 3 years (see Chapter 7).

5.23. 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

5.24. 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 satisfactory arrangements for the CHIS's case no longer exist. 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.

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

6.0 Management of CHIS

Tasking

6.1. Tasking is the assignment given to the CHIS, by the person referred to in section 21(3)(a) of RIPO (the "handler") asking him to obtain information, to provide access to or to 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. It is not the intention that authorisations 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 CHIS's task. If the nature of the task changes significantly or matters affect personal risk, then a new authorisation may need to be sought.

> ***Example 13:*** *A person is authorised for use as a CHIS to obtain information relating to volume crime being committed by a particular group of individuals and their associates or being committed in a specific geographical area. The CHIS is authorised for conduct, which amounts to maintaining a relationship with the individuals concerned through their recognised social or business activity and to pass any information to the police. Specific tasking will be given, based on any information received. Where a CHIS so authorised indicates that he now can access individuals involved in serious organised crime or has been asked to take part in criminal activity, a review of the authorisation will be necessary.*

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 handler or the person referred to in section 21(3)(b) of RIPO (the "controller") must refer the proposed tasking to the authorising officer, who should consider whether the existing authorisation is sufficient or requires review and amendment. 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. The investigating authority should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing handlers and controllers for each CHIS.

6.6. The handler will have day-to-day responsibility for:

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

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

6.8. The controller will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS. For the SBA Police, this role will be conducted by an officer of at least the rank of Inspector. For the SBA Customs & Immigration Service, the role will be conducted by the Deputy Fiscal Officer.

Joint working

6.9. In cases where the authorisation is for the use or conduct of a CHIS whose activities benefit more than one investigating 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 controller and handler of a CHIS need not be from the same investigating authority.

6.10. There are many cases where the activities of a CHIS may provide benefit to more than a single authority. In such situations, however, the authorities involved must set out in writing their agreed oversight arrangements.

Security and welfare

6.11. The investigating 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. Also consideration should be given to the management of any requirement to disclose information tending to reveal the existence of identity of a CHIS to, or in, court.

6.12. 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.

6.13. 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.

7.0 Record keeping

Centrally retrievable record of authorisations

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

7.2. While retaining such records for the time stipulated, investigating authorities must take into consideration the duty of care to the CHIS, the likelihood of future criminal or civil proceedings relating to information supplied by the CHIS or activities undertaken, and specific rules relating to data retention, review and deletion under the Data Protection Ordinance 2020.

Individual records of authorisation and use of CHIS

7.3. Proper records must be kept of the authorisation and use made of a CHIS. 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 records must contain particulars of the matters set out in paragraph 2 of Schedule 1 to RIPO.

7.5. The investigating authorities are encouraged to consider maintaining such records also for human sources who do not meet the definition of a CHIS. This may assist authorities to monitor the status of a human source and identify whether that source becomes a CHIS.

Further documentation

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

- a copy of the authorisation together with any supplementary documentation and notification of the approval granted by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent; • any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;

- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation; and
- the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.

7.7. The records kept by investigating authorities should be maintained in such a way as to preserve the confidentiality of the CHIS and the information provided by that CHIS.

Errors

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

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

7.10. An error must be reported if it is a "relevant error". A relevant error for the purpose of activity covered by this code is any error by an investigating authority in complying with any requirements that are imposed on it by any enactment. This would include compliance by investigating authorities with the RIPO. Examples of relevant errors occurring would include circumstances where:

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

7.11. Errors can have very significant consequences on an affected individual's rights and all relevant errors made by investigating authorities must be reported to the Investigatory Powers Commissioner by the investigating authority that is aware of the error.

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

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

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

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

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

Serious Errors

7.17. The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Ordinance 2006) is not sufficient by itself for an error to be a serious error.

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

- The seriousness of the error and its effect on the person concerned; and
- The extent to which disclosing the error would be contrary to the public interest or prejudicial to the prevention or detection of serious crime.

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

8.0 Safeguards

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.

8.2. Dissemination, copying and retention of material obtained through use or conduct of a CHIS must be limited to the minimum necessary for the authorised purposes. Something is necessary for the authorised purposes if the material is, or is likely to become, necessary for any of the statutory purposes set out in the RIPO in relation to the use or conduct of a CHIS.

Retention and destruction of material - general

8.3. Each investigating 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 appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

8.4. 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 established disclosure requirements for a suitable further period, commensurate to any subsequent review.

8.5. Subject to the provisions of Chapter 4, there is nothing in RIPO which prevents material obtained from authorisations for the use or conduct of a CHIS from being used to further other investigations.

Use of material as evidence

8.6. Subject to the provisions of Chapter 4, material obtained from a CHIS may be used as evidence in criminal proceedings. The admissibility of evidence is governed by the Evidence Ordinance 2010, the Human Rights Ordinance 2004 and other relevant legislation such as the Criminal Procedure Ordinance. Whilst this code does not affect the application of those rules, obtaining appropriate authorisations should help ensure the admissibility of evidence.

8.7. Product obtained by a CHIS is subject to the ordinary rules for retention and disclosure of material, where those rules apply to the law enforcement body in question.

8.8. There are also well-established legal procedures under public interest immunity rules that can be applied when seeking to protect the identity of a CHIS from disclosure in such circumstances. The Criminal Procedure (Disclosure) Ordinance 2007 provides that prosecution material may be withheld from disclosure for numerous reasons: see the factors listed in section 5(2) of that Ordinance.

Reviewing authorisations

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

Dissemination of information

8.10. Material acquired through use or conduct of a CHIS may need to be disseminated both within and between investigating authorities, as well as to consumers of intelligence where necessary in order for action to be taken on it. Material which tends to indicate the presence, activity or identity of a specific CHIS should be classified and handled as highly sensitive material. The number of persons to whom such material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out at 8.6 above. This obligation applies equally to disclosure to additional persons within an investigatory authority, and to disclosure outside an agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the material to carry out those duties. In the same way, only so much of the material may be disclosed as the recipient needs. For example, if a summary of the material will suffice, no more than that should be disclosed.

8.11. The obligations should apply not just to the original investigating 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 investigating authority's permission before disclosing the material further. In others, explicit safeguards should be applied to secondary recipients.

Copying

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

Storage

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

8.14. In particular, each investigating authority must apply the following protective security measures:

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

Destruction

8.15. Material obtained through use or conduct of a CHIS, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purposes. 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.

Protection of the identity of a CHIS

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

9.0 The Senior Responsible Officer and independent oversight

The Senior Responsible Officer

9.1. Within the investigating authority, a senior responsible officer must be appointed and be responsible for:

- the integrity of the process in place within the investigating authority for the management of CHIS;
- compliance with RIPO and with this code;
- oversight of the reporting of errors to the Chief Constable or Fiscal Officer, and by them 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 when inspections are conducted, and
- where necessary, oversight of the implementation of post-inspection action plans or recommendations.

The role of the Investigatory Powers Commissioner

9.2. The IPC's aim is to provide effective and efficient oversight of the conduct of covert surveillance and CHIS and the entry on and interference with property by investigating authorities in accordance with RIPO.

9.3. The IPC has the statutory responsibility for keeping under review investigating authorities' compliance with RIPO and the codes of practice. The IPC has oversight of all authorisations for the entry on or interference with property. Some authorisations require prior approval by the IPC before the activity can take place.

9.4. The IPC should conduct inspections at each investigating authority on a periodic basis.

9.5. It is anticipated that inspections will be requested on a timescale deemed suitable by the Chief Officer, after consulting the IPC.